

Серия ES-3124

Интеллектуальные коммутаторы уровня 2+

Руководство пользователя

Версия 3.80
8/2007
Редакция 1

ПАРАМЕТРЫ ВХОДА ПО УМОЛЧАНИЮ

IP-адрес внутрисетевое управления	http://192.168.1.1
IP-адрес внесетевое управления	http://192.168.0.1
Имя пользователя	admin
Пароль	1234

ZyXEL
www.zyxel.com

Сведения об этом руководстве пользователя

Целевая аудитория

Данное руководство предназначено для пользователей, занимающихся настройкой коммутаторов с использованием Web-конфигуратора. Читатель должен быть знаком как минимум на базовом уровне с основными понятиями и топологией сетей TCP/IP.

Дополнительная документация

- Онлайн-справка Web-конфигуратора
Встроенная Web-справка содержит описания отдельных экранов и дополнительную информацию.
- Справочное руководство по интерфейсу командной строки
В справочном руководстве по интерфейсу командной строки описана настройка коммутатора с использованием этого интерфейса и его команд.



Для настройки коммутатора предпочтительнее использовать Web-конфигуратор.

- Вспомогательный диск
Дополнительную документацию можно найти на прилагаемом компакт-диске.
- Web-сайт ZyXEL
Дополнительную документацию и сертификаты изделий можно найти на сайте www.zyxel.com.

Отзывы по руководству пользователя

Помогая нам, вы помогаете себе. Свои замечания, вопросы или предложения по улучшению любых руководств пользователя просьба направлять по следующему почтовому адресу или адресу электронной почты. Спасибо!

ZyXEL Россия,
117279, Москва,
ул. Островитянова 37а
E-mail: info@zyxel.ru

Условные обозначения

Предупреждения и примечания

Предупреждения и примечания выделяются в данном руководстве пользователя следующим образом.



В предупреждениях приводится информация о ситуациях, которые могут причинить вред пользователю или устройству.



В примечаниях приводится важная информация (например, дополнительные требования по настройке или полезные советы) или рекомендации.

Обозначения

- Коммутаторы ES-3124, ES-3124PWR, ES-3124-4F и ES-3124F могут называться в данном руководстве пользователя как «коммутатор», «устройство», «система» или «продукт». Различия отмечаются в случае необходимости.
- Обозначения продукта, наименования экранов, метки полей и варианты выбора приводятся **полужирным** шрифтом.
- Нажимаемые клавиши заключаются в квадратные скобки и записываются заглавными буквами, например, [ENTER] означает клавишу «Enter» или «возврат каретки» на клавиатуре.
- «Ввести» означает набрать один или несколько символов с последующим нажатием клавиши [ENTER]. «Выбрать» означает, что необходимо выбрать один из предложенных вариантов.
- Правая угловая скобка (>) при перечислении имен экранов обозначает нажатие мыши. Например, **Maintenance > Log > Log Setting** означает, что добраться до соответствующего экрана можно последовательным нажатием на **Maintenance** в навигационной панели, **Log** в подменю и, наконец, на вкладке **Log Setting**.
- В качестве единиц измерения могут использоваться «метрические» значения или «научные» значения. Например, «к» для «кило» может обозначать «1000» или «1024», «М» для «мега» может обозначать «1000000» или «1048576» и т.д.
- Сокращение «т.к.» означает «так как», «т.е.» означает «то есть» или «иными словами».

Значки на рисунках

На рисунках в данном руководстве пользователя могут использоваться следующие общие значки. Значок коммутатора не является точным изображением устройства.

Коммутатор 	Компьютер 	Ноутбук 
Сервер 	DSLAM-мультиплексор 	Межсетевой экран 
Телефон 	Коммутатор 	Маршрутизатор 

Предупреждения по безопасности



В целях вашей безопасности внимательно прочитайте и следуйте всем предупреждениям и указаниям.

- НЕ используйте данный продукт вблизи воды, например, в сыром подвале или неподалеку от плавательного бассейна.
- НЕ подвергайте устройство воздействию сырости, пыли или агрессивных жидкостей.
- НЕ кладите ничего поверх устройства.
- НЕ занимайтесь установкой, обслуживанием и не эксплуатируйте устройство во время грозы. Существует опасность поражения электрическим током в результате удара молнии.
- К устройству разрешается подключать ТОЛЬКО подходящие дополнительные модули.
- НЕ открывайте устройство. В результате вскрытия или снятия защитных кожухов вы подвергаете себя опасности прикосновения к оголенным токоведущим участкам с опасным высоким напряжением и иным рискам. Обслуживать или разбирать данное устройство разрешается ТОЛЬКО квалифицированному сервисному персоналу. Для получения дополнительной информации свяжитесь с поставщиком.
- Убедитесь, что кабели подключены к нужным портам.
- Аккуратно расположите соединительные кабели так, чтобы никто не мог наступить или споткнуться о них.
- Перед обслуживанием или разборкой обязательно отсоедините все кабели от устройства.
- Используйте с устройством ТОЛЬКО подходящий адаптер питания или шнур питания. Подключайте его к источнику питания с требуемым номиналом напряжения (например, 110 В перем. тока в Северной Америке или 230 В перем. тока в Европе).
- Используйте для устройства силовые провода НАДЛЕЖАЩЕГО сечения (подробная информация приводится в [разд. 38.1 на стр. 317](#)). Подключайте устройство к источнику питания с подходящим напряжением (подробная информация приводится в [разд. 38.1 на стр. 317](#)).
- НЕ кладите ничего на адаптер питания или шнур питания и НЕ располагайте продукт в таком месте, где кто-нибудь может наступить на адаптер питания или шнур питания.
- НЕ используйте устройство, если адаптер питания или шнур повреждены, так как в этом случае существует опасность поражения электрическим током.

- Если адаптер питания или шнур питания повреждены, отсоедините их от устройства и от сети питания.
- НЕ пытайтесь отремонтировать адаптер питания или шнур питания. Обратитесь к местному поставщику и закажите новый.
- Не используйте устройство вне помещений; все соединения также должны проходить внутри помещений. Существует опасность поражения электрическим током в результате удара молнии.
- Внимание: В случае установки батареи неправильного типа (на материнской плате) существует опасность взрыва. Соблюдайте указания по утилизации использованных батарей. Сдавайте использованные батареи в пункты утилизации электрических и электронных компонентов. Подробную информацию об утилизации данного изделия можно получить в местном муниципалитете, службе утилизации бытовых отходов или в магазине, где оно было приобретено.
- НЕ заслоняйте вентиляционные отверстия устройства, так как ограниченный приток воздуха может послужить причиной повреждения устройства.
- Устройства, поддерживающие подачу или получение питания по витой паре (PoE), а также подключенные к ним кабели Ethernet должны располагаться целиком внутри помещений.
- Длина зачищенного (оголенного) силового провода не должна превышать 7 мм.

Данное изделие подлежит утилизации. Соблюдайте надлежащие требования по утилизации.



Обзор содержания

Введение	31
Знакомство с коммутатором	33
Аппаратное обеспечение	39
Установка и подключение аппаратного обеспечения	41
Обзор аппаратного обеспечения	45
Web-конфигуратор	53
Web-конфигуратор	55
Пример первичной настройки	67
Состояние системы и статистика портов	71
Основные настройки	77
Виртуальные локальные сети (VLAN)	91
Настройка пересылки на основе статических MAC-адресов	109
Фильтрация	111
Протокол покрывающего дерева	113
Управление пропускной способностью	135
Контроль широковещательных штормов	139
Зеркальное копирование	141
Агрегация каналов	143
Аутентификация портов	151
Средства безопасности портов	157
Классификация	161
Правила политики	167
Метод организации очередей	175
Стекирование VLAN	179
Мультивещание	185
Аутентификация и учет	201
Защита от подмены IP-адресов	215
Защита от образования петель	241
Статические маршруты	245
Дифференцированное обслуживание	247
DHCP	255
Обслуживание	261
Контроль доступа	269
Диагностика	291
Системный журнал Syslog	293

Управление кластерами	297
Таблица MAC-адресов	303
Таблица ARP	305
Настройка клонирования	307
Устранение неполадок и характеристики	311
Устранение неполадок	313
Характеристики продукта	317
Приложения и индекс	325

Содержание

Сведения об этом руководстве пользователя	3
Условные обозначения.....	4
Предупреждения по безопасности	6
Обзор содержания	9
Содержание.....	11
Перечень рисунков.....	21
Перечень таблиц.....	27
Часть I: Введение.....	31
Глава 1	
Знакомство с коммутатором.....	33
1.1 Обзор	33
1.1.1 Применение в магистральной сети	33
1.1.2 Пример мостовой конфигурации	34
1.1.3 Пример высокоскоростной коммутации	35
1.1.4 Примеры применения в сетях VLAN на базе IEEE 802.1Q	35
1.2 Способы управления коммутатором	36
1.3 Полезные советы по управлению коммутатором	37
Часть II: Аппаратное обеспечение	39
Глава 2	
Установка и подключение аппаратного обеспечения.....	41
2.1 Установка на столе	41
2.2 Установка коммутатора в стойку	42
2.2.1 Требования к установке коммутатора в аппаратную стойку	42
2.2.2 Крепление кронштейнов к коммутатору	42
2.2.3 Установка коммутатора в стойку	43

Глава 3	
Обзор аппаратного обеспечения.....	45
3.1 Подключения на передней панели	45
3.1.1 Консольный порт	47
3.1.2 Порты Ethernet	47
3.1.3 Слоты для трансиверов	48
3.2 Задняя панель	50
3.2.1 Разъем питания	50
3.2.2 Разъем для внешнего резервного источника питания	50
3.3 Индикаторы	51
Часть III: Web-конфигуратор	53
Глава 4	
Web-конфигуратор	55
4.1 Введение	55
4.2 Вход в систему	55
4.3 Окно состояния (Status)	56
4.3.1 Изменение пароля	63
4.4 Сохранение конфигурации	63
4.5 Блокировка коммутатора	63
4.6 Сброс коммутатора	64
4.6.1 Загрузка файла конфигурации	64
4.7 Выход из Web-конфигуратора	65
4.8 Помощь	65
Глава 5	
Пример первичной настройки	67
5.1 Обзор	67
5.1.1 Создание виртуальной локальной сети VLAN	67
5.1.2 Назначение идентификатора виртуальной локальной сети VID для порта	69
5.2 Настройка IP-адреса управления коммутатором	69
Глава 6	
Состояние системы и статистика портов	71
6.1 Обзор	71
6.2 Сводная информация о состоянии портов	71
6.2.1 Экран Status: Port Details	72

Глава 7	
Основные настройки	77
7.1 Обзор	77
7.2 Информация о системе	77
7.3 Общие настройки	80
7.4 Введение в виртуальные локальные сети (VLAN)	82
7.5 Экран Switch Setup	83
7.6 Настройки протокола IP	85
7.6.1 IP-интерфейсы	85
7.7 Настройки портов	87
Глава 8	
Виртуальные локальные сети (VLAN)	91
8.1 Введение в виртуальные локальные сети на основе тегов (согласно IEEE 802.1Q)	91
8.1.1 Пересылка кадров с тегами и без тегов	92
8.2 Автоматическая регистрация VLAN	92
8.2.1 Протокол GARP	92
8.2.2 Протокол GVRP	92
8.3 Магистральные порты VLAN	93
8.4 Выбор типа VLAN	94
8.5 Статические VLAN	94
8.5.1 Состояние статической VLAN	94
8.5.2 Подробная информация о статической VLAN	95
8.5.3 Настройка статической VLAN	96
8.5.4 Настройка порта VLAN	97
8.6 VLAN на основе подсетей	99
8.7 Настройка VLAN на основе подсетей	99
8.8 VLAN на основе протоколов	102
8.9 Настройка VLAN на основе протоколов	102
8.10 Пример создания VLAN на основе протокола IP	104
8.11 Настройка VLAN на основе портов	105
8.11.1 Настройка VLAN на основе портов	106
Глава 9	
Настройка пересылки на основе статических MAC-адресов.....	109
9.1 Обзор	109
9.2 Настройка пересылки на основе статических MAC-адресов	109
Глава 10	
Фильтрация	111
10.1 Настройка правила фильтрации	111

Глава 11	
Протокол покрывающего дерева	113
11.1 Обзор протоколов STP/RSTP	113
11.1.1 Терминология STP	114
11.1.2 Как работает протокол STP	114
11.1.3 Состояния портов по протоколу STP	115
11.1.4 Быстрый протокол нескольких экземпляров покрывающего дерева	115
11.1.5 Протокол MSTP	116
11.2 Экран состояния протокола STP	119
11.3 Настройка протокола покрывающего дерева	119
11.4 Настройка быстрого протокола покрывающего дерева	120
11.5 Состояние быстрого протокола покрывающего дерева	123
11.6 Настройка протокола MRSTP	124
11.7 Состояние протокола MRSTP	126
11.8 Настройка протокола MSTP	127
11.9 Состояние протокола MSTP	131
Глава 12	
Управление пропускной способностью	135
12.1 Обзор управления пропускной способностью	135
12.1.1 CIR и PIR	135
12.2 Настройка управления пропускной способностью	136
Глава 13	
Контроль ширококвещательных штормов	139
13.1 Настройка функции контроля ширококвещательных штормов	139
Глава 14	
Зеркальное копирование	141
14.1 Настройка зеркального копирования портов	141
Глава 15	
Агрегация каналов	143
15.1 Обзор агрегации каналов	143
15.2 Динамическая агрегация каналов	143
15.2.1 Идентификатор агрегации каналов	144
15.3 Состояние агрегации каналов	144
15.4 Настройка агрегации каналов	145
15.5 Протокол управления агрегацией каналов LACP	147
15.6 Пример статического группирования портов	148

Глава 16	
Аутентификация портов	151
16.1 Обзор аутентификации портов	151
16.1.1 Аутентификация на основе IEEE 802.1x	152
16.1.2 Аутентификация по MAC-адресам	152
16.2 Настройка аутентификации портов	153
16.2.1 Включение функций безопасности стандарта IEEE 802.1x	153
16.2.2 Включение аутентификации по MAC-адресам	155
Глава 17	
Средства безопасности портов.....	157
17.1 О средствах безопасности портов	157
17.2 Настройка средств безопасности портов	157
Глава 18	
Классификация.....	161
18.1 О классификации и управлении качеством обслуживания	161
18.2 Настройка классификации	161
18.3 Просмотр и редактирование настройки классификации	164
18.4 Пример использования классификации	166
Глава 19	
Правила политики.....	167
19.1 Обзор правил политики	167
19.1.1 Дифференцированное обслуживание	167
19.1.2 Маркер DSCP и обработка на каждом конкретном переходе	167
19.2 Настройка правил политики	168
19.3 Просмотр и редактирование настроек политики	171
19.4 Пример политики	172
Глава 20	
Метод организации очередей	175
20.1 Обзор методов организации очередей	175
20.1.1 Строгая очередь приоритетов (SP)	175
20.1.2 Взвешенная справедливая постановка в очередь (WFQ)	175
20.1.3 Взвешенное циклическое обслуживание (WRR)	176
20.2 Настройка метода организации очередей	176
Глава 21	
Стекирование VLAN.....	179
21.1 Обзор стекирования VLAN	179
21.1.1 Пример стекирования VLAN	179
21.2 Роли портов при стекировании VLAN	180

21.3 Формат тега VLAN	181
21.3.1 Формат кадра	181
21.4 Настройка стекирования VLAN	182
Глава 22	
Мультивещание	185
22.1 Обзор мультивещания	185
22.1.1 IP-адреса мультивещания	185
22.1.2 Фильтрация IGMP	185
22.1.3 Отслеживание многоадресного трафика IGMP	186
22.1.4 Отслеживание многоадресного трафика IGMP и сети VLAN	186
22.2 Состояние мультивещания	186
22.3 Настройка мультивещания	187
22.4 VLAN отслеживания многоадресного трафика IGMP	189
22.5 Профиль фильтрации IGMP	191
22.6 Обзор MVR	193
22.6.1 Типы портов MVR	193
22.6.2 Режимы MVR	193
22.6.3 Как работает механизм MVR	194
22.7 Общая настройка MVR	194
22.8 Настройка группы MVR	197
22.8.1 Пример настройки MVR	198
Глава 23	
Аутентификация и учет.....	201
23.1 Аутентификация, авторизация и учет	201
23.1.1 Локальные учетные записи пользователей	202
23.1.2 RADIUS и TACACS+	202
23.2 Экраны настройки функций аутентификации и учета	202
23.2.1 Настройка сервера RADIUS	203
23.2.2 Настройка сервера TACACS+	204
23.2.3 Настройка аутентификации и учета	206
23.2.4 Специальный атрибут производителя	209
23.3 Поддерживаемые атрибуты RADIUS	211
23.3.1 Атрибуты, используемые для аутентификации	211
23.3.2 Атрибуты, используемые для учета	212
Глава 24	
Защита от подмены IP-адресов	215
24.1 Обзор функции защиты от подмены IP-адресов	215
24.1.1 Обзор отслеживания DHCP	215
24.1.2 Обзор функции инспекции ARP-пакетов	218
24.2 Защита от подмены IP-адресов	219

24.3 Статическая привязка для защиты от подмены IP-адресов	220
24.4 Отслеживание DHCP	222
24.5 Настройка отслеживания DHCP	226
24.5.1 Настройка портов отслеживания DHCP	228
24.5.2 Настройка VLAN отслеживания DHCP	229
24.6 Состояние инспекции ARP-пакетов	231
24.6.1 Состояние сети VLAN для инспекции ARP-пакетов	232
24.6.2 Состояние журнала инспекции ARP-пакетов	233
24.7 Настройка инспекции ARP-пакетов	235
24.7.1 Настройка портов для инспекции ARP-пакетов	236
24.7.2 Настройка сети VLAN для инспекции ARP-пакетов	238
Глава 25	
Защита от образования петель	241
25.1 Обзор функции защиты от образования петель	241
25.2 Настройка защиты от образования петель	243
Глава 26	
Статические маршруты.....	245
26.1 Настройка статических маршрутов	245
Глава 27	
Дифференцированное обслуживание	247
27.1 Обзор механизма DiffServ	247
27.1.1 Маркер DSCP и обработка на каждом конкретном переходе	247
27.1.2 Пример сети с поддержкой DiffServ	248
27.2 Ограничение трафика с использованием маркеров TRTCM	248
27.2.1 TRTCM – режим без учета цвета	249
27.2.2 TRTCM – режим с учетом цвета	250
27.3 Активация механизма DiffServ	250
27.3.1 Настройка маркировки TRTCM	251
27.4 Настройка отображения маркеров DSCP на приоритеты IEEE 802.1p	253
27.4.1 Настройка DSCP	254
Глава 28	
DHCP	255
28.1 Обзор DHCP	255
28.1.1 Режимы DHCP	255
28.1.2 Варианты настройки DHCP	255
28.2 Состояние DHCP	255
28.3 Ретрансляция DHCP	256
28.3.1 Информация агента ретрансляции DHCP	256
28.3.2 Настройка глобальной ретрансляции DHCP	257

28.3.3 Пример настройки глобальной ретрансляции DHCP	258
28.4 Настройка DHCP для конкретных VLAN	258
28.4.1 Пример: Ретрансляция DHCP для двух VLAN	260
Глава 29	
Обслуживание	261
29.1 Экран обслуживания	261
29.2 Загрузка заводских настроек по умолчанию	262
29.3 Сохранение конфигурации	262
29.4 Перезагрузка системы	263
29.5 Обновление встроенного программного обеспечения	263
29.6 Восстановление файла конфигурации	264
29.7 Резервное копирование файла конфигурации	264
29.8 Командная строка FTP	265
29.8.1 Соглашения об именовании файлов	265
29.8.2 Работа с командной строкой FTP	266
29.8.3 FTP-клиенты с графическим пользовательским интерфейсом	267
29.8.4 Ограничения FTP	267
Глава 30	
Контроль доступа	269
30.1 Обзор контроля доступа	269
30.2 Главный экран контроля доступа	269
30.3 Знакомство с протоколом SNMP	270
30.3.1 SNMP v3 и безопасность	271
30.3.2 Поддерживаемые базы MIB	271
30.3.3 Команды Trar протокола SNMP	271
30.3.4 Настройка SNMP	278
30.3.5 Настройка группы «ловушек» SNMP	281
30.3.6 Настройка учетных записей пользователей	282
30.4 Обзор протокола SSH	284
30.5 Как работает протокол SSH	284
30.6 Реализация протокола SSH на коммутаторе	285
30.6.1 Требования к использованию протокола SSH	285
30.7 Знакомство с протоколом HTTPS	285
30.8 Пример подключения по протоколу HTTPS	286
30.8.1 Предупреждения от Internet Explorer	286
30.8.2 Предупреждения от Netscape Navigator	287
30.8.3 Основной экран	288
30.9 Контроль доступа к портам служб	288
30.10 Удаленное управление	289

Глава 31	
Диагностика.....	291
31.1 Экран Diagnostic	291
Глава 32	
Системный журнал Syslog	293
32.1 Обзор Syslog	293
32.2 Настройка Syslog	293
32.3 Настройка сервера Syslog	294
Глава 33	
Управление кластерами.....	297
33.1 Обзор управления кластерами	297
33.2 Состояние управления кластером	298
33.2.1 Управление коммутаторами-членами кластера	299
33.3 Настройка управления кластерами	301
Глава 34	
Таблица MAC-адресов.....	303
34.1 Обзор таблицы MAC-адресов	303
34.2 Просмотр таблицы MAC-адресов	304
Глава 35	
Таблица ARP	305
35.1 Обзор таблицы ARP	305
35.1.1 Как работает протокол ARP	305
35.2 Просмотр таблицы ARP	305
Глава 36	
Настройка клонирования	307
36.1 Настройка клонирования	307
Часть IV: Устранение неполадок и характеристики	311
Глава 37	
Устранение неполадок	313
37.1 Проблемы с питанием, аппаратные подключения и индикаторы	313
37.2 Проблемы с доступом и входом на коммутатор	314

Глава 38	
Характеристики продукта	317
38.1 Общие характеристики коммутатора	317
38.2 Назначение выводов кабеля	322
Часть V: Приложения и индекс	325
Приложение A Настройка IP-адреса компьютера	327
Приложение B Всплывающие окна, JavaScript и разрешения Java.....	349
Приложение C IP-адреса и подсети	357
Приложение D Часто используемые службы.....	369
Приложение E Импорт сертификатов	373
Приложение F Правовая информация.....	379
Приложение G Поддержка пользователей	385
Индекс	387

Перечень рисунков

Рисунок 1 Применение в магистральной сети	34
Рисунок 2 Применение в мостовой конфигурации	34
Рисунок 3 Пример высокоскоростной коммутации	35
Рисунок 4 Применение виртуальной локальной сети на базе тегов	36
Рисунок 5 Пример использования общего сервера в VLAN	36
Рисунок 6 Прикрепление резиновых ножек	41
Рисунок 7 Закрепление кронштейнов	43
Рисунок 8 Установка коммутатора в стойку	43
Рисунок 9 Передняя панель: ES-3124	45
Рисунок 10 Передняя панель: ES-3124-4F	45
Рисунок 11 Передняя панель: ES-3124PWR	46
Рисунок 12 Передняя панель: ES-3124F	46
Рисунок 13 Пример установки трансивера	49
Рисунок 14 Установленный трансивер	49
Рисунок 15 Пример открытия защелки трансивера	49
Рисунок 16 Пример удаления трансивера	49
Рисунок 17 Задняя панель (модели с питанием от переменного тока)	50
Рисунок 18 Задняя панель (модели с питанием от постоянного тока)	50
Рисунок 19 Web-конфигуратор: вход в систему	56
Рисунок 20 Начальная страница Web-конфигуратора (Status)	56
Рисунок 21 Изменение пароля администратора	63
Рисунок 22 Сброс коммутатора: через консольный порт	65
Рисунок 23 Web-конфигуратор: экран выхода	65
Рисунок 24 Пример первичной настройки сети: виртуальная локальная сеть	67
Рисунок 25 Пример первичной настройки сети: идентификатор виртуальной локальной сети для порта	69
Рисунок 26 Пример первичной настройки: IP-адрес управления	70
Рисунок 27 Экран Status	71
Рисунок 28 Экран Status: Port Details	73
Рисунок 29 Экран Basic Setting > System Info	78
Рисунок 30 Экран Basic Setting > General Setup	80
Рисунок 31 Экран Basic Setting > Switch Setup	83
Рисунок 32 Экран Basic Setting > IP Setup	85
Рисунок 33 Экран Basic Setting > Port Setup	88
Рисунок 34 Магистральные порты VLAN	94
Рисунок 35 Экран Switch Setup: выбор типа VLAN	94
Рисунок 36 Экран Advanced Application > VLAN: VLAN Status	94
Рисунок 37 Экран Advanced Application > VLAN > VLAN Detail	95

Рисунок 38 Экран Advanced Application > VLAN > Static VLAN	96
Рисунок 39 Экран Advanced Application > VLAN > VLAN Port Setting	97
Рисунок 40 Пример использования VLAN на основе подсетей	99
Рисунок 41 Экран Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN	100
Рисунок 42 Пример использования VLAN на основе протоколов	102
Рисунок 43 Экран Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN	103
Рисунок 44 Пример настройки VLAN на основе протокола	105
Рисунок 45 Экран Advanced Application > VLAN: Port Based VLAN Setup (All Connected)	106
Рисунок 46 Экран Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)	107
Рисунок 47 Экран Advanced Application > Static MAC Forwarding	110
Рисунок 48 Экран Advanced Application > Filtering	111
Рисунок 49 Пример сети с поддержкой MRSTP	116
Рисунок 50 Пример сети с поддержкой STP/RSTP	117
Рисунок 51 Пример сети с поддержкой MSTP	117
Рисунок 52 Экземпляры MSTI в различных регионах	118
Рисунок 53 Пример сети с использованием MSTP и традиционного протокола RSTP	119
Рисунок 54 Экран Advanced Application > Spanning Tree Protocol	119
Рисунок 55 Экран Advanced Application > Spanning Tree Protocol > Configuration	120
Рисунок 56 Экран Advanced Application > Spanning Tree Protocol > RSTP	121
Рисунок 57 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP	123
Рисунок 58 Экран Advanced Application > Spanning Tree Protocol > MRSTP	124
Рисунок 59 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP	126
Рисунок 60 Экран Advanced Application > Spanning Tree Protocol > MSTP	128
Рисунок 61 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP	132
Рисунок 62 Экран Advanced Application > Bandwidth Control	136
Рисунок 63 Экран Advanced Application > Broadcast Storm Control	140
Рисунок 64 Экран Advanced Application > Mirroring	141
Рисунок 65 Экран Advanced Application > Link Aggregation Status	145
Рисунок 66 Экран Advanced Application > Link Aggregation > Link Aggregation Setting	146
Рисунок 67 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP	147
Рисунок 68 Пример группирования портов – физические подключения	149
Рисунок 69 Пример группирования портов – экран настройки	149
Рисунок 70 Процесс аутентификации на основе IEEE 802.1x	152
Рисунок 71 Процесс аутентификации по MAC-адресу	153
Рисунок 72 Экран Advanced Application > Port Authentication	153
Рисунок 73 Экран Advanced Application > Port Authentication > 802.1x	154
Рисунок 74 Экран Advanced Application > Port Authentication > MAC Authentication	155
Рисунок 75 Экран Advanced Application > Port Security	158
Рисунок 76 Экран Advanced Application > Classifier	162
Рисунок 77 Экран Advanced Application > Classifier: итоговая таблица	164
Рисунок 78 Классификация: пример	166

Рисунок 79 Экран Advanced Application > Policy Rule	169
Рисунок 80 Экран Advanced Application > Policy Rule: итоговая таблица	171
Рисунок 81 Пример политики	173
Рисунок 82 Экран Advanced Application > Queuing Method	177
Рисунок 83 Пример стекирования VLAN	180
Рисунок 84 Экран Advanced Application > VLAN Stacking	182
Рисунок 85 Экран Advanced Application > Multicast	186
Рисунок 86 Экран Advanced Application > Multicast > Multicast Setting	187
Рисунок 87 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN	190
Рисунок 88 Экран Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile	192
Рисунок 89 Пример сети с поддержкой MVR	193
Рисунок 90 Пример с мультивещанием телевидения посредством MVR	194
Рисунок 91 Экран Advanced Application > Multicast > Multicast Setting > MVR	195
Рисунок 92 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration	197
Рисунок 93 Пример настройки MVR	198
Рисунок 94 Пример настройки MVR	199
Рисунок 95 Пример настройки групп MVR	199
Рисунок 96 Пример настройки групп MVR	200
Рисунок 97 Сервер AAA	201
Рисунок 98 Экран Advanced Application > Auth and Acct	202
Рисунок 99 Экран Advanced Application > Auth and Acct > RADIUS Server Setup	203
Рисунок 100 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup	205
Рисунок 101 Экран Advanced Application > Auth and Acct > Auth and Acct Setup	207
Рисунок 102 Формат файла базы данных отслеживания DHCP	217
Рисунок 103 Пример: атака «Man-in-the-middle»	218
Рисунок 104 Экран Advanced Application > IP Source Guard	219
Рисунок 105 Экран Advanced Application > IP Source Guard > Static Binding	221
Рисунок 106 Экран Advanced Application > IP Source Guard > DHCP Snooping	223
Рисунок 107 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure	226
Рисунок 108 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port	228
Рисунок 109 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN	230
Рисунок 110 Экран Advanced Application > IP Source Guard > ARP Inspection	231
Рисунок 111 Экран ARP Inspection VLAN Status	232
Рисунок 112 Экран Advanced Application > IP Source Guard > ARP Inspection > Log Status	233
Рисунок 113 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure	235
Рисунок 114 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > Port	237
Рисунок 115 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN	238

Рисунок 116 Защита от образования петель и STP	241
Рисунок 117 Коммутатор с петлей	242
Рисунок 118 Защита от образования петель – пробный пакет	242
Рисунок 119 Защита от образования петель – петля в сети	243
Рисунок 120 Экран Advanced Application > Loop Guard	243
Рисунок 121 Экран IP Application > Static Routing	245
Рисунок 122 DiffServ: поле Differentiated Service	247
Рисунок 123 Сеть с поддержкой DiffServ	248
Рисунок 124 TRTCM – режим без учета цвета	249
Рисунок 125 TRTCM – режим с учетом цвета	250
Рисунок 126 Экран IP Application > DiffServ	251
Рисунок 127 Экран IP Application > DiffServ > 2-rate 3 Color Marker	252
Рисунок 128 Экран IP Application > DiffServ > DSCP Setting	254
Рисунок 129 Экран IP Application > DHCP Status	256
Рисунок 130 Экран IP Application > DHCP > Global	257
Рисунок 131 Пример сети с глобальной ретрансляцией DHCP	258
Рисунок 132 Пример настройки глобальной ретрансляции DHCP	258
Рисунок 133 Экран IP Application > DHCP > VLAN	259
Рисунок 134 Ретрансляция DHCP для двух VLAN	260
Рисунок 135 Пример настройки ретрансляции DHCP для двух VLAN	260
Рисунок 136 Экран Management > Maintenance	261
Рисунок 137 Загрузка заводских настроек: запуск	262
Рисунок 138 Перезагрузка системы: подтверждение	263
Рисунок 139 Экран Management > Maintenance > Firmware Upgrade	264
Рисунок 140 Экран Management > Maintenance > Restore Configuration	264
Рисунок 141 Экран Management > Maintenance > Backup Configuration	265
Рисунок 142 Экран Management > Access Control	269
Рисунок 143 Модель управления по протоколу SNMP	270
Рисунок 144 Экран Management > Access Control > SNMP	279
Рисунок 145 Экран Management > Access Control > SNMP > Trap Group	281
Рисунок 146 Экран Management > Access Control > Logins	283
Рисунок 147 Пример связи по протоколу SSH	284
Рисунок 148 Как работает протокол SSH	284
Рисунок 149 Реализация протокола HTTPS	286
Рисунок 150 Диалоговое окно Security Alert (Internet Explorer)	287
Рисунок 151 Сертификат безопасности 1 (Netscape)	287
Рисунок 152 Сертификат безопасности 2 (Netscape)	288
Рисунок 153 Пример: значок замка для защищенного соединения	288
Рисунок 154 Экран Management > Access Control > Service Access Control	289
Рисунок 155 Экран Management > Access Control > Remote Management	290
Рисунок 156 Экран Management > Diagnostic	291
Рисунок 157 Экран Management > Syslog	294
Рисунок 158 Экран Management > Syslog > Server Setup	295

Рисунок 159 Пример реализации кластера	298
Рисунок 160 Экран Management > Cluster Management	298
Рисунок 161 Управление кластером: экран Web-конфигуратора члена кластера	299
Рисунок 162 Пример: загрузка встроенного программного обеспечения на коммутатор-член кластера	300
Рисунок 163 Экран Management > Clustering Management > Configuration	301
Рисунок 164 Схема работы таблицы MAC-адресов	304
Рисунок 165 Экран Management > MAC Table	304
Рисунок 166 Экран Management > ARP Table	306
Рисунок 167 Экран Management > Configure Clone	307
Рисунок 168 Назначение выводов консольного порта/порта резервного коммутируемого соединения	322
Рисунок 169 Windows 95/98/Me: окно Network: Configuration	328
Рисунок 170 Windows 95/98/Me: окно TCP/IP Properties: IP Address	329
Рисунок 171 Windows 95/98/Me: окно TCP/IP Properties: DNS Configuration	330
Рисунок 172 Windows XP: меню Start	331
Рисунок 173 Windows XP: окно Control Panel	331
Рисунок 174 Выбор Windows XP: Control Panel: Network Connections: Properties	332
Рисунок 175 Windows XP: окно Local Area Connection Properties	332
Рисунок 176 Windows XP: окно Internet Protocol (TCP/IP) Properties	333
Рисунок 177 Windows XP: окно Advanced TCP/IP Properties	334
Рисунок 178 Windows XP: окно Internet Protocol (TCP/IP) Properties	335
Рисунок 179 Windows Vista: меню Start	336
Рисунок 180 Windows Vista: окно Control Panel	336
Рисунок 181 Windows Vista: окно Network And Internet	336
Рисунок 182 Windows Vista: окно Network and Sharing Center	336
Рисунок 183 Windows Vista: окно Network and Sharing Center	337
Рисунок 184 Windows Vista: окно Local Area Connection Properties	337
Рисунок 185 Windows Vista: окно Internet Protocol Version 4 (TCP/IPv4) Properties	338
Рисунок 186 Windows Vista: окно Advanced TCP/IP Properties	339
Рисунок 187 Windows Vista: окно Internet Protocol Version 4 (TCP/IPv4) Properties	340
Рисунок 188 Macintosh OS 8/9: меню Apple	341
Рисунок 189 Macintosh OS 8/9: окно TCP/IP	341
Рисунок 190 Macintosh OS X: меню Apple	342
Рисунок 191 Macintosh OS X: окно Network	343
Рисунок 192 Red Hat 9.0: среда KDE: окно Network Configuration: Devices	344
Рисунок 193 Red Hat 9.0: среда KDE: окно Ethernet Device: General	345
Рисунок 194 Red Hat 9.0: среда KDE: окно Network Configuration: DNS	345
Рисунок 195 Red Hat 9.0: среда KDE: окно Network Configuration: Activate	346
Рисунок 196 Red Hat 9.0: настройка динамического получения IP-адреса в файле ifconfig-eth0	346
Рисунок 197 Red Hat 9.0: настройка статического IP-адреса в файле ifconfig-eth0	346
Рисунок 198 Red Hat 9.0: настройки DNS в файле resolv.conf	347
Рисунок 199 Red Hat 9.0: перезапуск сетевой карты	347

Рисунок 200 Red Hat 9.0: проверка настроек TCP/IP	347
Рисунок 201 Блокировщик всплывающих окон	349
Рисунок 202 Меню Internet Options: Privacy	350
Рисунок 203 Меню Internet Options: Privacy	351
Рисунок 204 Экран Pop-up Blocker Settings	351
Рисунок 205 Меню Internet Options: Security	352
Рисунок 206 Настройки безопасности – JavaScript	353
Рисунок 207 Настройки безопасности – Java	354
Рисунок 208 Java (Sun)	354
Рисунок 209 Экран Mozilla Firefox: Tools > Options	355
Рисунок 210 Экран Mozilla Firefox Content Security	355
Рисунок 211 Номер сети и идентификатор хоста	358
Рисунок 212 Пример формирования подсетей: до деления на подсети	360
Рисунок 213 Пример формирования подсетей: после деления на подсети	361
Рисунок 214 Пример с конфликтом IP-адресов компьютеров	366
Рисунок 215 Пример с конфликтом IP-адресов маршрутизатора	366
Рисунок 216 Пример с конфликтом IP-адресов компьютера и маршрутизатора	367
Рисунок 217 Сертификат безопасности	373
Рисунок 218 Экран входа в систему	374
Рисунок 219 Общая информация о сертификате, отображаемая перед импортом	374
Рисунок 220 «Мастер» импорта сертификата, шаг 1	375
Рисунок 221 «Мастер» импорта сертификата, шаг 2	375
Рисунок 222 «Мастер» импорта сертификата, шаг 3	376
Рисунок 223 Хранилище корневых сертификатов	376
Рисунок 224 Общая информация о сертификате, отображаемая после импорта	377

Перечень таблиц

Таблица 1 Особенности отдельных моделей	33
Таблица 2 Подключения на передней панели	46
Таблица 3 Индикаторы	51
Таблица 4 Обзор подменю панели навигации	57
Таблица 5 Содержание экранов подменю Web-конфигуратора	58
Таблица 6 Пункты меню навигационной панели	60
Таблица 7 Экран Status	71
Таблица 8 Экран Status > Port Details	73
Таблица 9 Экран Basic Setting > System Info	78
Таблица 10 Экран Basic Setting > General Setup	80
Таблица 11 Экран Basic Setting > Switch Setup	83
Таблица 12 Экран Basic Setting > IP Setup	86
Таблица 13 Экран Basic Setting > Port Setup	88
Таблица 14 Терминология сетей VLAN на основе IEEE 802.1Q	93
Таблица 15 Экран Advanced Application > VLAN: VLAN Status	95
Таблица 16 Экран Advanced Application > VLAN > VLAN Detail	95
Таблица 17 Экран Advanced Application > VLAN > Static VLAN	96
Таблица 18 Экран Advanced Application > VLAN > VLAN Port Setting	98
Таблица 19 Экран Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup	100
Таблица 20 Экран Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup	103
Таблица 21 Экран Advanced Application > VLAN: Port Based VLAN Setup	108
Таблица 22 Экран Advanced Application > Static MAC Forwarding	110
Таблица 23 Экран Advanced Application > Filtering	111
Таблица 24 Стоимость путей протокола STP	114
Таблица 25 Состояния портов по протоколу STP	115
Таблица 26 Экран Advanced Application > Spanning Tree Protocol > Configuration	120
Таблица 27 Экран Advanced Application > Spanning Tree Protocol > RSTP	121
Таблица 28 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP	123
Таблица 29 Экран Advanced Application > Spanning Tree Protocol > MRSTP	124
Таблица 30 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP	127
Таблица 31 Экран Advanced Application > Spanning Tree Protocol > MSTP	129
Таблица 32 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP	132
Таблица 33 Экран Advanced Application > Bandwidth Control	136
Таблица 34 Экран Advanced Application > Broadcast Storm Control	140
Таблица 35 Экран Advanced Application > Mirroring	142
Таблица 36 Идентификатор агрегации каналов: локальный коммутатор	144
Таблица 37 Идентификатор агрегации каналов: коммутатор-партнер	144

Таблица 38 Экран Advanced Application > Link Aggregation Status	145
Таблица 39 Экран Advanced Application > Link Aggregation > Link Aggregation Setting	146
Таблица 40 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP	147
Таблица 41 Экран Advanced Application > Port Authentication > 802.1x	154
Таблица 42 Экран Advanced Application > Port Authentication > MAC Authentication	156
Таблица 43 Экран Advanced Application > Port Security	158
Таблица 44 Экран Advanced Application > Classifier	162
Таблица 45 Экран Classifier: итоговая таблица	164
Таблица 46 Распространенные типы Ethernet и номера протоколов	165
Таблица 47 Распространенные типы протокола IP и номера протоколов	165
Таблица 48 Распространенные номера портов TCP и UDP	165
Таблица 49 Экран Advanced Application > Policy Rule	169
Таблица 50 Политика: итоговая таблица	171
Таблица 51 Экран Advanced Application > Queuing Method	177
Таблица 52 Формат тега VLAN	181
Таблица 53 Формат кадра с одним и двумя тегами 802.11Q	182
Таблица 54 Кадр 802.1Q	182
Таблица 55 Экран Advanced Application > VLAN Stacking	183
Таблица 56 Экран Multicast Status	187
Таблица 57 Экран Advanced Application > Multicast > Multicast Setting	188
Таблица 58 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN	190
Таблица 59 Экран Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile	192
Таблица 60 Экран Advanced Application > Multicast > Multicast Setting > MVR	195
Таблица 61 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration	197
Таблица 62 RADIUS и TACACS+	202
Таблица 63 Экран Advanced Application > Auth and Acct > RADIUS Server Setup	203
Таблица 64 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup	205
Таблица 65 Экран Advanced Application > Auth and Acct > Auth and Acct Setup	207
Таблица 66 Поддерживаемые атрибуты VSA	210
Таблица 67 Поддерживаемые атрибуты протокола туннелирования	211
Таблица 68 Атрибуты RADIUS – события Exec при выполнении команд с консоли	212
Таблица 69 Атрибуты RADIUS – события Exec при выполнении команд через Telnet/SSH	213
Таблица 70 Атрибуты RADIUS – события Exec при выполнении команд с консоли	213
Таблица 71 Экран Advanced Application > IP Source Guard	220
Таблица 72 Экран Advanced Application > IP Source Guard > Static Binding	221
Таблица 73 Экран Advanced Application > IP Source Guard > DHCP Snooping	224
Таблица 74 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure	227
Таблица 75 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port	229

Таблица 76 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN	230
Таблица 77 Экран Advanced Application > IP Source Guard > ARP Inspection	231
Таблица 78 Экран ARP Inspection VLAN Status	232
Таблица 79 Экран Advanced Application > IP Source Guard > ARP Inspection > Log Status	234
Таблица 80 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure	235
Таблица 81 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > Port	237
Таблица 82 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN	238
Таблица 83 Экран Advanced Application > Loop Guard	244
Таблица 84 Экран IP Application > Static Routing	245
Таблица 85 Экран IP Application > DiffServ	251
Таблица 86 Экран IP Application > DiffServ > 2-rate 3 Color Marker	252
Таблица 87 Отображение маркеров DSCP на приоритеты IEEE 802.1p по умолчанию	253
Таблица 88 Экран IP Application > DiffServ > DSCP Setting	254
Таблица 89 Экран IP Application > DHCP Status	256
Таблица 90 Информация агента ретрансляции	257
Таблица 91 Экран IP Application > DHCP > Global	257
Таблица 92 Экран IP Application > DHCP > VLAN	259
Таблица 93 Экран Management > Maintenance	261
Таблица 94 Соглашения об именовании файлов	265
Таблица 95 Общие команды для FTP-клиентов с графическим пользовательским интерфейсом	267
Таблица 96 Обзор контроля доступа	269
Таблица 97 Команды протокола SNMP	270
Таблица 98 Идентификаторы объектов по моделям	272
Таблица 99 Системные команды Trap протокола SNMP (System)	272
Таблица 100 Интерфейсные команды Trap протокола SNMP (Interface)	274
Таблица 101 Команды Trap протокола SNMP для аутентификации, авторизации и учета (AAA)	275
Таблица 102 Команды Trap протокола SNMP для IP	276
Таблица 103 Команды Trap протокола SNMP для коммутатора (Switch)	277
Таблица 104 Экран Management > Access Control > SNMP	279
Таблица 105 Экран Management > Access Control > SNMP > Trap Group	281
Таблица 106 Экран Management > Access Control > Logins	283
Таблица 107 Экран Management > Access Control > Service Access Control	289
Таблица 108 Экран Management > Access Control > Remote Management	290
Таблица 109 Экран Management > Diagnostic	292
Таблица 110 Уровни серьезности Syslog	293
Таблица 111 Экран Management > Syslog	294
Таблица 112 Экран Management > Syslog > Server Setup	295
Таблица 113 Спецификации управления кластерами ZyXEL	297
Таблица 114 Экран Management > Cluster Management	299

Таблица 115 Пример загрузки встроенного программного обеспечения на член кластера посредством FTP	300
Таблица 116 Экран Management > Clustering Management > Configuration	301
Таблица 117 Экран Management > MAC Table	304
Таблица 118 Экран Management > ARP Table	306
Таблица 119 Экран Management > Configure Clone	308
Таблица 120 Характеристики оборудования и параметры окружающей среды	317
Таблица 121 Характеристики функций	319
Таблица 122 Поддерживаемые стандарты	321
Таблица 123 Назначение выводов консольного порта/порта резервного коммутлируемого соединения	323
Таблица 124 Назначение выводов кабеля Ethernet	323
Таблица 125 Пример выделения номера сети и идентификатора хоста в IP-адресе	358
Таблица 126 Маски подсети	359
Таблица 127 Максимально возможное число хостов	359
Таблица 128 Альтернативный формат записи маски подсети	360
Таблица 129 Подсеть 1	362
Таблица 130 Подсеть 2	362
Таблица 131 Подсеть 3	362
Таблица 132 Подсеть 4	362
Таблица 133 Восемь подсетей	363
Таблица 134 Планирование подсетей для сети с 24-битным номером	363
Таблица 135 Планирование подсетей для сети с 16-битным номером	364
Таблица 136 Часто используемые службы	369

ЧАСТЬ I

Введение

Знакомство с коммутатором (33)

Знакомство с коммутатором

В данном руководстве пользователя рассматриваются следующие модели: ES-3124, ES-3124-4F, ES-3124-PWR и ES-3124F. Особенности отдельных моделей описаны в следующей таблице.

Таблица 1 Особенности отдельных моделей

ХАРАКТЕРИСТИКИ	МОДЕЛЬ	ES-3124	ES-3124-4F	ES-3124PWR	ES-3124F
Совмещенные порты		X	X	X	X
2 порта Gigabit Ethernet с разъемами RJ-45 для стекирования		X		X	
2 порта mini-GBIC для стекирования			X		X
24 слота для модулей SFP Fast Ethernet					X
Порты Ethernet с поддержкой питания устройств по витой паре согласно стандарту IEEE 802.3af				X	

Полный перечень общих для всех моделей характеристик можно найти в [гл. 38 на стр. 317](#).

В этой главе описаны основные характеристики и способы применения коммутатора. Кроме того, эта глава знакомит с различными способами управления коммутатором.

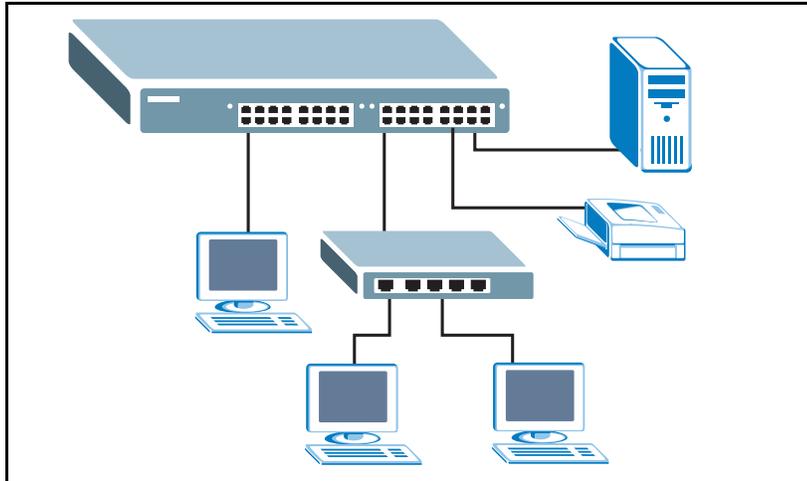
1.1 Обзор

В данном разделе приводится несколько примеров использования коммутатора в различных сетевых конфигурациях.

1.1.1 Применение в магистральной сети

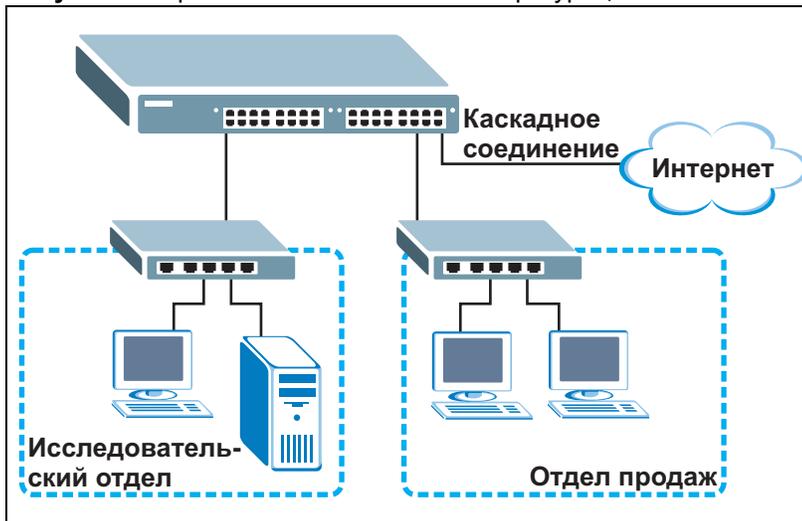
В данной конфигурации коммутатор является идеальным решением для малых сетей, которые ожидают стремительного роста в ближайшем будущем. Данный коммутатор может использоваться автономно для группы активных пользователей. К портам коммутатора можно подключать компьютеры или другие коммутаторы.

В этом примере все компьютеры совместно используют высокоскоростные приложения на сервере. Для расширения сети достаточно просто добавить другие сетевые устройства, например, коммутаторы, маршрутизаторы, компьютеры, принт-серверы и т.д.

Рисунок 1 Применение в магистральной сети

1.1.2 Пример мостовой конфигурации

С помощью коммутатора можно подключить различные отделы компании (**Исследовательский отдел** и **Отдел продаж**) к корпоративной магистральной сети. Это позволяет уменьшить «сосязание» за пропускную способность и устранить «узкие места» в сети и подключении к серверу. Все пользователи, которым требуется большая пропускная способность, могут подключаться к высокоскоростным серверам своих отделов через коммутатор. Использование порта Gigabit Ethernet/mini-GBIC коммутатора позволяет обеспечить высокоскоростной канал для каскадного соединения. Кроме того, коммутатор облегчает задачи контроля и обслуживания, позволяя сетевым администраторам централизованно расположить несколько серверов.

Рисунок 2 Применение в мостовой конфигурации

1.1.3 Пример высокоскоростной коммутации

Данный коммутатор идеально подходит для соединения двух сетей, которым требуется высокая пропускная способность. Переход на высокоскоростные локальные сети, например, работающие по технологии ATM, для большинства пользователей нецелесообразен из-за высокой стоимости замены всех имеющихся Ethernet-кабелей и карт адаптеров, реструктуризации сети и сложности технического обслуживания. Данный коммутатор позволяет добиться такой же пропускной способности, как и в сети ATM, но при существенно меньших затратах и с возможностью использования имеющихся адаптеров и коммутаторов. Более того, сохраняется существующая структура локальной сети, так как все порты могут свободно связываться друг с другом. В приведенном примере для соединения этих двух сетей используется группирование портов на двух коммутаторах.

Рисунок 3 Пример высокоскоростной коммутации



1.1.4 Примеры применения в сетях VLAN на базе IEEE 802.1Q

В данном разделе рассмотрена рабочая группа и сервер общего пользования, работающие в виртуальных локальных сетях VLAN на базе тегов, согласно 802.1Q.

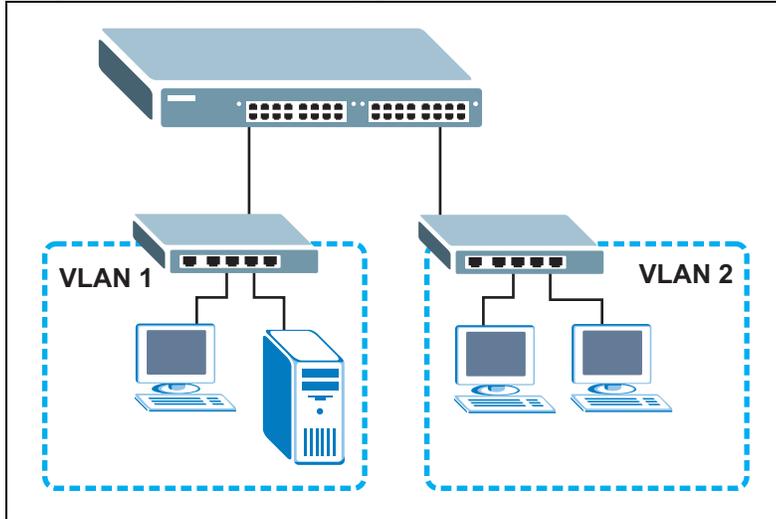
Виртуальные локальные сети (VLAN) позволяют разделить одну физическую сеть на несколько логических. Станции в логической сети принадлежат к одной группе. Станция может принадлежать к нескольким группам. При использовании сетей VLAN станция не может отправлять или принимать данные от станций, не принадлежащих к той же группе (группам); это возможно лишь в том случае, если трафик проходит через маршрутизатор.

Дополнительную информацию о виртуальных локальных сетях можно найти в [гл. 8 на стр. 91](#).

1.1.4.1 Пример виртуальной локальной сети на базе тегов

Порты в одной группе VLAN принадлежат к одному домену широковещательной передачи кадров. Это позволяет повысить производительность сети за счет уменьшения широковещательного трафика. Группы VLAN можно изменять в любой момент, добавляя, перемещая или изменяя порты без переподключения кабелей.

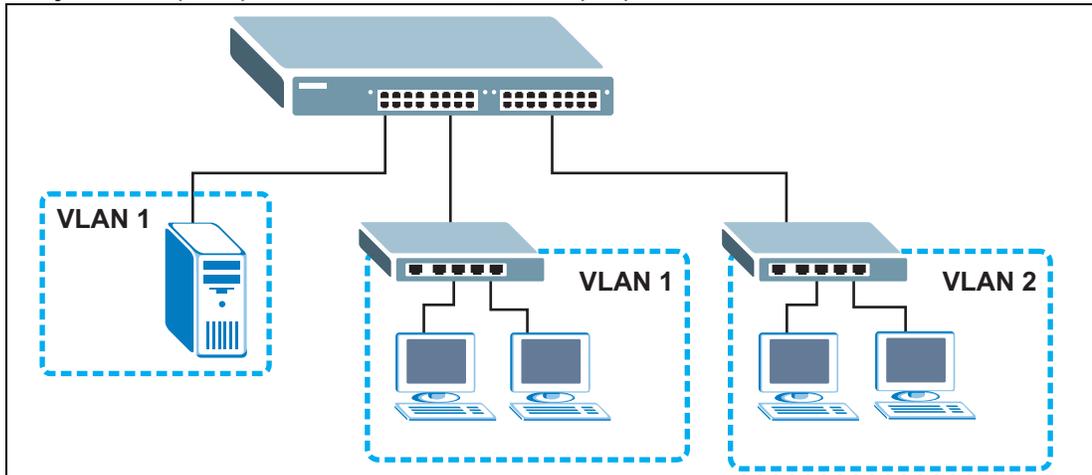
Рисунок 4 Применение виртуальной локальной сети на базе тегов



1.1.4.2 Пример виртуальных локальных сетей с общим сервером

Общие ресурсы, например, сервер, могут использоваться всеми портами в той же сети VLAN, что и сервер, как показано в данном примере. В этом примере в сеть VLAN 1 необходимо включить только те порты, которым требуется доступ к серверу. Порты также могут принадлежать к другим группам VLAN.

Рисунок 5 Пример использования общего сервера в VLAN



1.2 Способы управления коммутатором

Для управления коммутатором доступны следующие способы.

- Web-конфигуратор. Именно этот способ рекомендуется применять для повседневного управления коммутатором при помощи (поддерживаемого) браузера. См. [гл. 4 на стр. 55](#).

- Интерфейс командной строки. Интерфейс командной строки является альтернативой Web-конфигуратору и может потребоваться для настройки расширенных функций. См. Справочное руководство по интерфейсу командной строки.
- FTP. Протокол передачи файлов File Transfer Protocol можно использовать для обновления встроенного программного обеспечения и резервного копирования/восстановления конфигурации. См. [разд. 29.8 на стр. 265](#).
- SNMP. Мониторинг и/или управление устройством возможно с использованием менеджера SNMP. См. [разд. 30.3 на стр. 270](#).

1.3 Полезные советы по управлению коммутатором

Чтобы сделать коммутатор более защищенным, а управление коммутатором – более эффективным, необходимо регулярно выполнять следующие действия.

- Меняйте пароль. Используйте пароль, который трудно угадать, и который включает в себя различные виды символов, включая буквы и цифры.
- Запишите пароль и сохраните его в надежном месте.
- Осуществляйте резервное копирование конфигурации (и ознакомьтесь с порядком ее восстановления). Восстановление более ранней версии конфигурации может оказаться полезным в случае нестабильной работы или отказа устройства. Если вы забыли свой пароль, можно восстановить на коммутаторе заводские настройки по умолчанию. При наличии резервной копии более ранней версии файла конфигурации вам не придется повторно настраивать коммутатор от начала и до конца. Вы сможете просто восстановить последнюю конфигурацию.

ЧАСТЬ II

Аппаратное обеспечение

Установка и подключение аппаратного обеспечения (41)

Обзор аппаратного обеспечения (45)

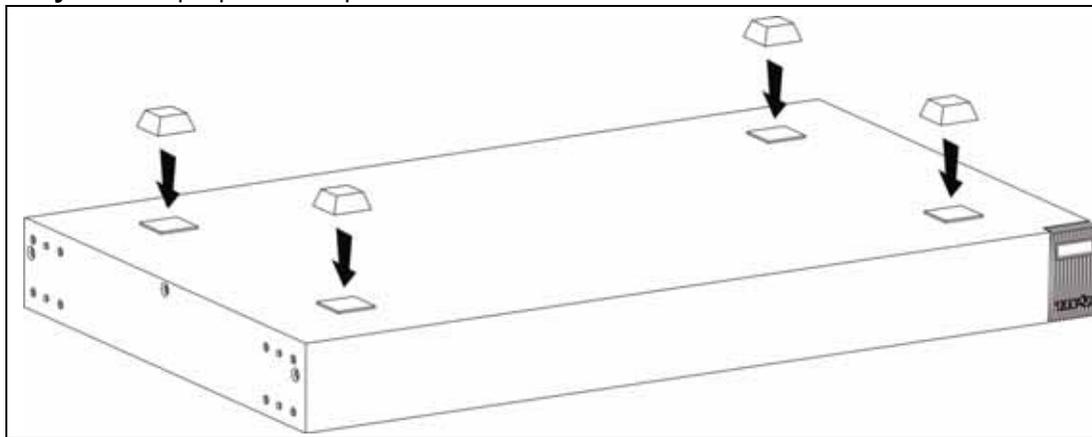
Установка и подключение аппаратного обеспечения

В данной главе описаны процедуры установки и подключения коммутатора.

2.1 Установка на столе

- 1 Убедитесь, что коммутатор сухой и чистый.
- 2 Установите коммутатор на ровной горизонтальной поверхности, достаточно устойчивой, чтобы выдержать вес коммутатора и подключенных к нему кабелей. Убедитесь, что рядом есть розетка.
- 3 Убедитесь, что вокруг коммутатора имеется достаточно свободного пространства для циркуляции воздуха и подключения кабелей и шнура питания.
- 4 Удалите наклейки с резиновых ножек.
- 5 Прикрепите резиновые ножки к каждому углу днища коммутатора. Эти ножки защищают коммутатор от вибрации и обеспечивают наличие свободного места между устройствами, установленными друг на друга.

Рисунок 6 Прикрепление резиновых ножек





НЕ закрывайте вентиляционные отверстия. При установке устройств друг на друга убедитесь, что между ними есть свободное пространство. Чтобы обеспечить нормальную вентиляцию, оставьте зазор как минимум в 4 дюйма (10 см) спереди и 3,4 дюйма (8 см) сзади коммутатора. Это особенно важно при установке в закрытой стойке.

2.2 Установка коммутатора в стойку

В данном разделе перечислены требования и меры предосторожности при установке устройства в аппаратную стойку, а также описана собственно процедура установки.

2.2.1 Требования к установке коммутатора в аппаратную стойку

- Два кронштейна.
- Восемь винтов М3 с плоской головкой и крестовая отвертка #2.
- Четыре винта М5 с плоской головкой и крестовая отвертка #2.



Использование винтов неправильного типа может повредить устройство.

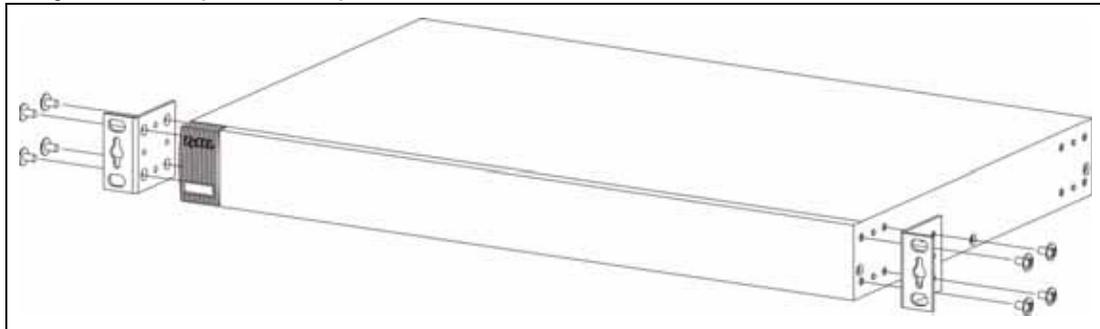
2.2.1.1 Меры предосторожности

- Убедитесь, что стойка может выдержать общий вес всего оборудования, которое в нее установлено.
- Убедитесь, что положение коммутатора не нарушает устойчивость стойки и не смещает центр тяжести к ее верхней части. Перед установкой примите все необходимые меры предосторожности для надежного закрепления стойки.

2.2.2 Крепление кронштейнов к коммутатору

- 1 Приложите кронштейн к одной из боковых панелей коммутатора, совместив четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели коммутатора.

Рисунок 7 Закрепление кронштейнов

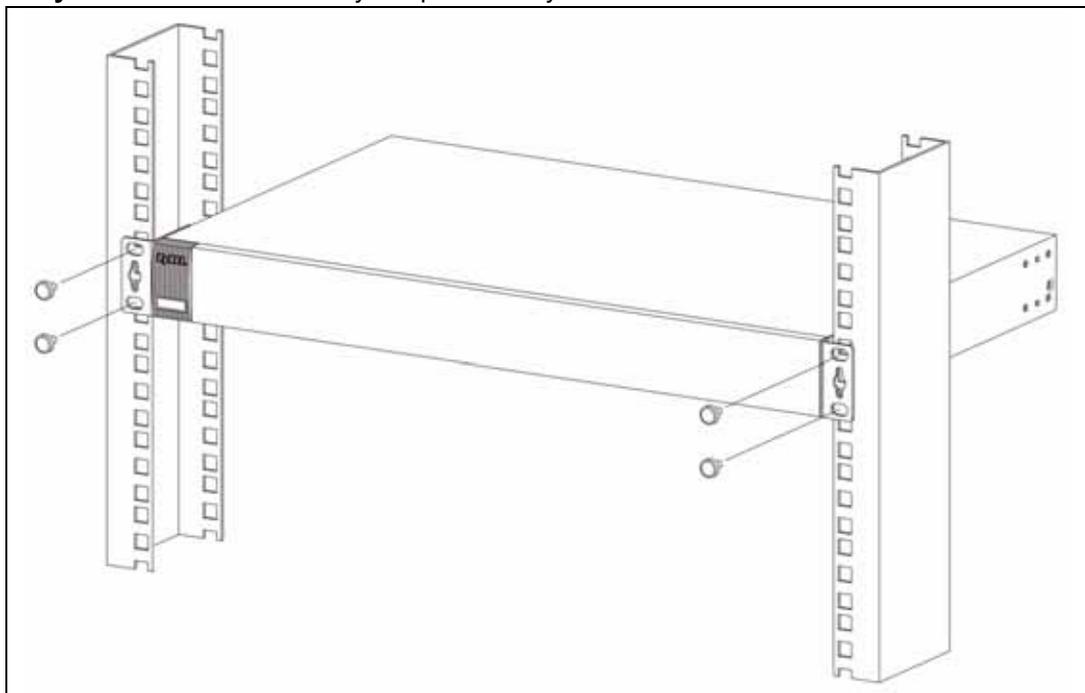


- 2 С помощью крестовой отвертки #2 прикрепите кронштейн к коммутатору винтами М3 с плоской головкой.
- 3 Повторите шаги 1 и 2, чтобы закрепить кронштейн на другой стороне коммутатора.
- 4 Теперь коммутатор можно устанавливать в стойку. Переходите к следующему разделу.

2.2.3 Установка коммутатора в стойку

- 1 Приложите кронштейн (уже прикрепленный винтами к боковой панели коммутатора) к одной стороне стойки и совместите два отверстия для винтов на кронштейне с такими же двумя отверстиями в стойке.

Рисунок 8 Установка коммутатора в стойку



- 2 С помощью крестовой отвертки #2 прикрепите кронштейн к стойке винтами М5 с плоской головкой.
- 3 Повторите шаги 1 и 2, чтобы закрепить кронштейн на другой стороне стойки.

Обзор аппаратного обеспечения

В данной главе описаны передняя и задняя панель коммутатора, а также показаны аппаратные подключения.

3.1 Подключения на передней панели

Передняя панель коммутатора показана на рисунке ниже.

Рисунок 9 Передняя панель: ES-3124

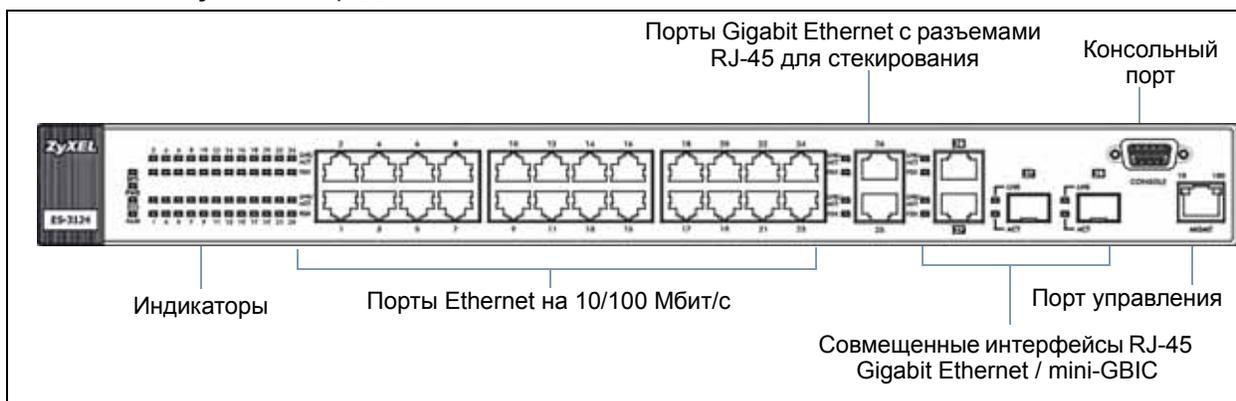


Рисунок 10 Передняя панель: ES-3124-4F

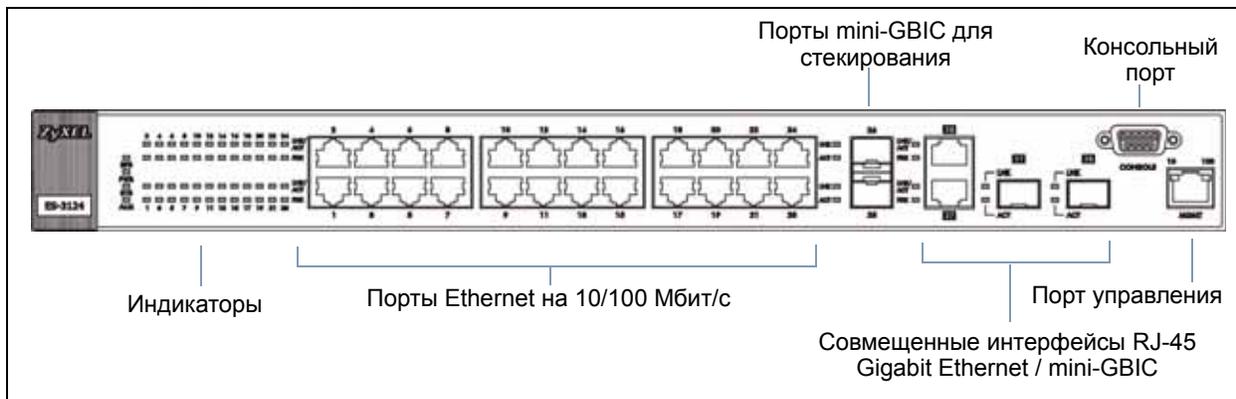


Рисунок 11 Передняя панель: ES-3124PWR

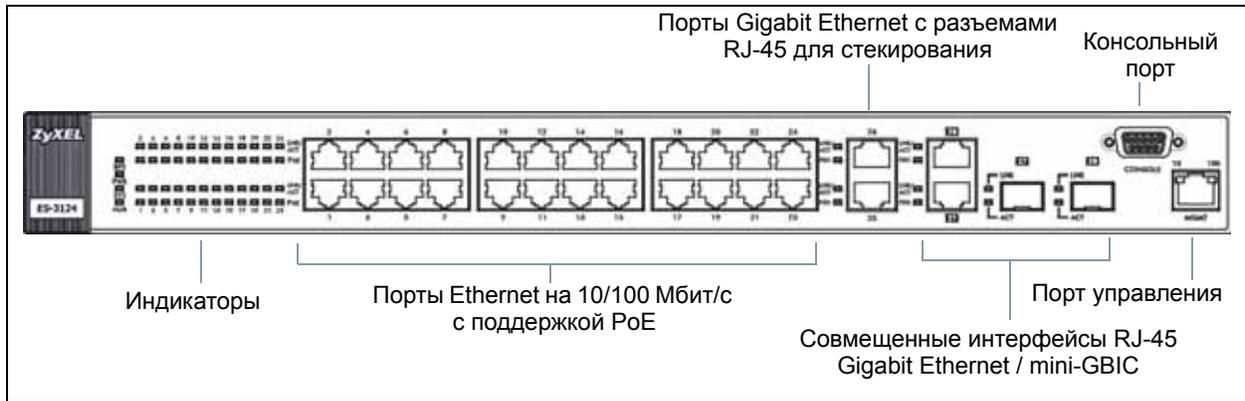
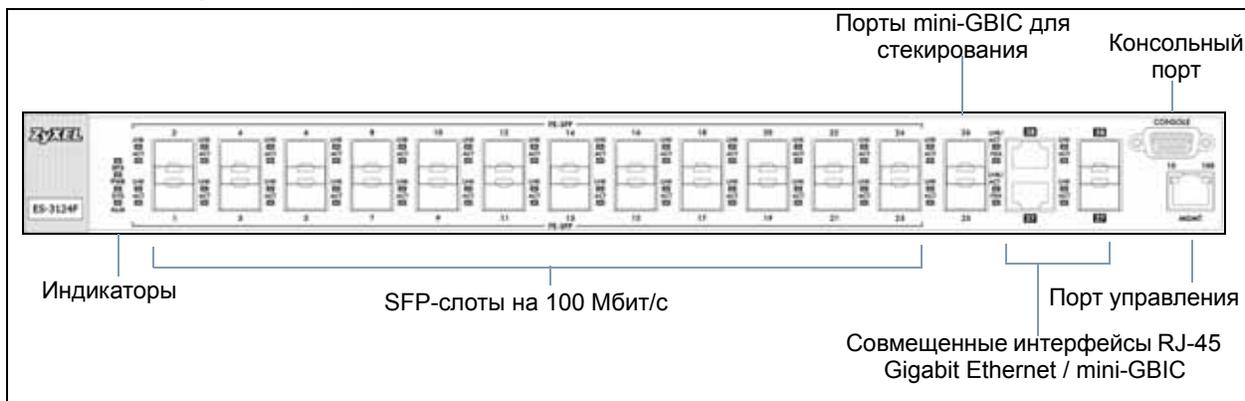


Рисунок 12 Передняя панель: ES-3124F



Расположенные на передней панели порты описаны в следующей таблице.

Таблица 2 Подключения на передней панели

РАЗЪЕМ	ОПИСАНИЕ
Все модели	
Консольный порт	К этому порту следует подключаться только тогда, когда требуется настроить коммутатор с помощью интерфейса командной строки через консольный порт.
Порт управления	Подключается к компьютеру с использованием Ethernet-кабеля с разъемом RJ-45 для локальной настройки коммутатора.
Совмещенные интерфейсы	Каждый из интерфейсов включает в себя порт для витой пары 1000 Base-T с разъемом RJ-45 и слот SFP (также называемый слотом mini-GBIC), причем в каждый момент времени может быть активен только один порт или трансивер.
2 порта на 100/1000 Мбит/с с разъемами RJ-45	Эти порты подключаются к высокоскоростным магистральным Ethernet-коммутаторам с использованием кабелей витой пары категории 5/5e/6 для соединений 1000Base-T.
2 слота mini-GBIC	В эти слоты можно вставить трансиверы mini-GBIC для подключения к магистральным Ethernet-коммутаторам посредством оптоволокна.
ES-3124, ES-3124-4F и ES-3124PWR	
24 порта Ethernet на 10/100 Мбит/с с разъемами RJ-45	К этим портам можно подключать компьютеры, концентраторы, Ethernet-коммутаторы или маршрутизаторы.

Таблица 2 Подключения на передней панели (продолжение)

РАЗЪЕМ	ОПИСАНИЕ
ES-3124F	
24 слота для модулей SFP Fast Ethernet на 100 Мбит/с	К этим портам подключаются компьютеры или коммутаторы.
ES-3124 и ES-3124PWR	
2 порта на 100/1000 Мбит/с с разъемами RJ-45	Эти порты подключаются к высокоскоростным магистральным Ethernet-коммутаторам или используются для последовательного соединения нескольких коммутаторов. Для соединений 1000Base-T используются кабели витой пары категории 5/5e/6.
ES-3124-4F и ES-3124F	
2 слота mini-GBIC	В эти слоты можно вставить трансиверы mini-GBIC для подключения к магистральным Ethernet-коммутаторам или последовательного соединения нескольких коммутаторов.
ES-3124PWR	
Питание устройств по витой паре (PoE)	24 порта Ethernet на 10/100 Мбит/с с разъемами RJ-45 обеспечивают питание устройств по витой паре согласно IEEE 802.3af.

3.1.1 Консольный порт

Для локального управления можно использовать компьютер с установленной на нем программой-эмулятором терминала, настроенной со следующими параметрами:

- Эмуляция терминала VT100
- Скорость 9600 бод
- Четность – нет, 8 бит данных, 1 стоп-бит
- Управление потоком – нет

Подключите 9-пиновый разъем типа «папа» консольного кабеля к консольному порту коммутатора. Подключите другой конец кабеля с разъемом типа «мама» к последовательному порту (COM1, COM2 или другому COM-порту) компьютера.

3.1.2 Порты Ethernet

Данный коммутатор оснащен 24 портами Ethernet на 10/100 Мбит/с с функциями автосогласования и автоматического определения типа кабеля. Порты Fast Ethernet на 10/100 Мбит/с могут работать на скорости 10 Мбит/с или 100 Мбит/с в полудуплексном или дуплексном режиме.

В данном коммутаторе также имеется две пары совмещенных портов Gigabit Ethernet/mini-GBIC. Порты mini-GBIC имеют приоритет перед портами Gigabit Ethernet. Это означает, что если порт mini-GBIC и соответствующий ему порт Gigabit Ethernet подключены одновременно, то порт Gigabit Ethernet работать не будет. Скорость на портах Gigabit Ethernet может быть либо 100 Мбит/с, либо 1000 Мбит/с, а режим – либо полудуплексным (на скорости 100 Мбит/с), либо дуплексным.

Порт с функцией автосогласования может определять и настраивать оптимальную скорость и режим дуплекса (полудуплекс или дуплекс) канала Ethernet для подключенного устройства.

Порт с функцией автоматического определения типа кабеля (автоматического выбора режима MDI/MDI-X) позволяет использовать для подключения как стандартный (прямой), так и кроссоверный (перекрещенный) кабели Ethernet.

3.1.2.1 Настройки Ethernet по умолчанию

По умолчанию для портов Ethernet коммутатора установлены следующие заводские настройки:

- Скорость: Автосогласование
- Режим дуплекса: Автосогласование
- Управление потоком: Нет

3.1.3 Слоты для трансиверов

Данные слоты предназначены для установки трансиверов mini-GBIC (конвертеров гигабитного интерфейса) или трансиверов SFP (Small Form-Factor Pluggable) на 100 Мбит/с. Трансивер – это устройство, совмещающее в себе функции передатчика и приемника. Трансиверы не входят в комплект поставки коммутатора. Разрешается использовать только трансиверы, отвечающие требованиям SFP Transceiver MultiSource Agreement (MSA). Более подробную информацию можно найти в спецификации INF-8074i Rev 1.0 комитета SFF.

Коммутатор оснащен двумя парами портов Gigabit Ethernet/mini-GBIC. Порты mini-GBIC имеют приоритет перед портами Gigabit Ethernet. Это означает, что если порт mini-GBIC и соответствующий ему порт Gigabit Ethernet подключены одновременно, то порт Gigabit Ethernet работать не будет.

В моделях ES-3124-4F и ES-3124F также предусмотрено два порта mini-GBIC для подключения к другим коммутаторам.

В модели ES-3124F имеется 24 порта SFP на 100 Мбит/с для подключения компьютеров или коммутаторов.

Трансиверы можно менять во время работы коммутатора. Для подключения к Ethernet-коммутаторам с различными типами оптоволоконных разъемов можно пользоваться различными типами трансиверов.

- Тип: Интерфейс подключения SFP
- Скорость подключения: 1 гигабит в секунду (1 Гбит/с)



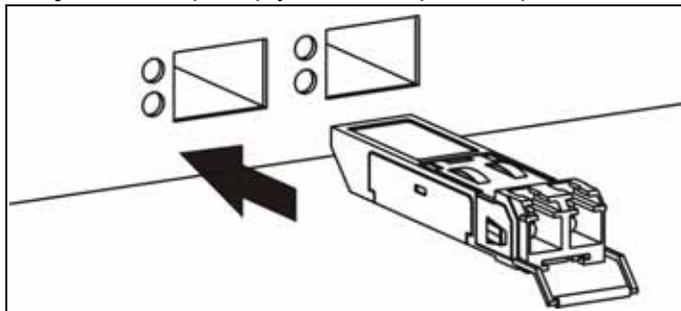
Во избежание возможной травмы глаз НЕ смотрите в разъемы работающего оптоволоконного модуля.

3.1.3.1 Установка трансивера

Для установки трансивера mini-GBIC или SFP на 100 Мбит/с выполните следующие действия.

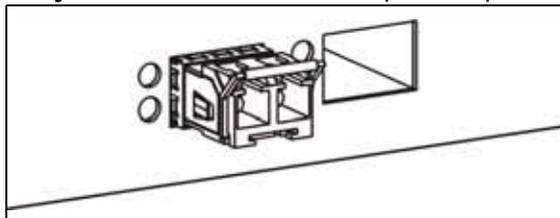
- 1 Вставьте трансивер в слот открытой секцией печатной платы вниз.

Рисунок 13 Пример установки трансивера



- 2 Надавите на трансивер, пока он не защелкнется на месте.
- 3 Данный коммутатор автоматически обнаружит установленный трансивер. Проверьте состояние светодиодных индикаторов, чтобы убедиться, что он работает.

Рисунок 14 Установленный трансивер

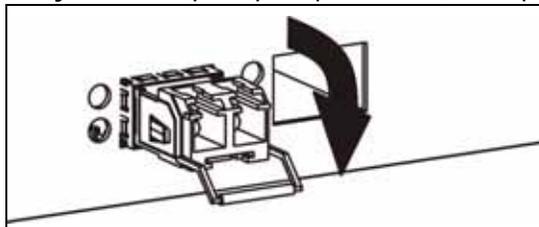


3.1.3.2 Удаление трансивера

Для удаления трансивера mini-GBIC (SFP-модуля) выполните следующие действия.

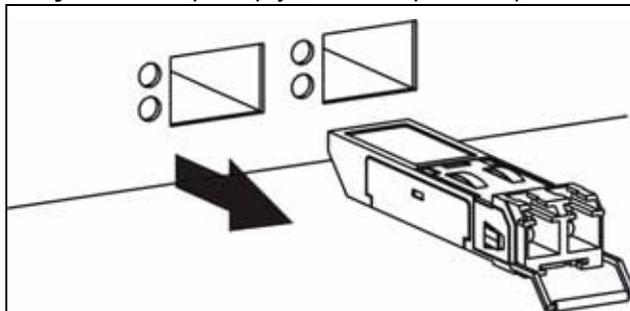
- 1 Откройте защелку трансивера (их вид может различаться).

Рисунок 15 Пример открытия защелки трансивера



- 2 Выньте трансивер из слота.

Рисунок 16 Пример удаления трансивера



3.2 Задняя панель

Задняя панель коммутатора показана на рисунке ниже. На задней панели находится разъем для подключения внешнего резервного источника питания (BPS), розетка питания и выключатель питания (только в моделях с питанием от постоянного тока).

Рисунок 17 Задняя панель (модели с питанием от переменного тока)

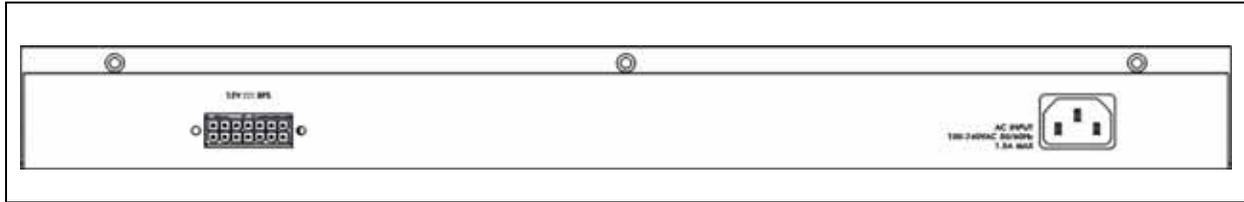
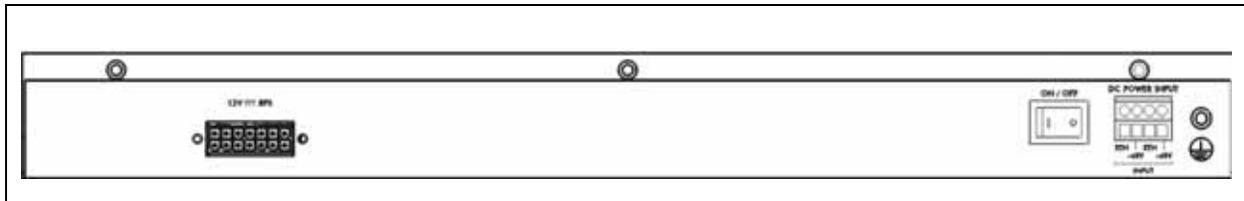


Рисунок 18 Задняя панель (модели с питанием от постоянного тока)



3.2.1 Разъем питания

Убедитесь, что параметры питающей сети соответствуют указанным на панели.

Для подключения питания к коммутатору вставьте разъем типа «мама» шнура питания в розетку на задней панели. Подключите другой конец шнура питания к источнику питания. Убедитесь, что притоку воздуха ничто не мешает.

3.2.2 Разъем для внешнего резервного источника питания

Данный коммутатор поддерживает внешний резервный источник питания (BPS).

Резервный источник питания непрерывно отслеживает состояние встроенного источника питания. В случае пропадания питания коммутатор автоматически переключается на питание от резервного источника. После переключения коммутатора на питание от резервного источника, даже в случае возобновления подачи питания, обратно на питание от встроенного источника питания он автоматически не переключается.

3.3 Индикаторы

Описание индикаторов приводится в следующей таблице.

Таблица 3 Индикаторы

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
BPS	Зеленый	Мигает	Данный коммутатор получает питание от резервного источника питания.
		Горит	Резервный источник питания подключен и активен.
		Не горит	Резервный источник питания не подключен или не активен.
PWR	Зеленый	Горит	Данный коммутатор включен.
		Не горит	Данный коммутатор выключен.
SYS	Зеленый	Мигает	Данный коммутатор перезагружается и выполняет самодиагностику.
		Горит	Данный коммутатор включен и функционирует нормально.
		Не горит	Питание выключено или коммутатор не готов / работает с ошибками.
ALM	Красный	Горит	Обнаружен сбой оборудования.
		Не горит	Данный коммутатор функционирует нормально.
Порты Ethernet (только на ES-3124 и ES-3124-4F)			
LNK/ACT	Зеленый	Мигает	Данный коммутатор осуществляет передачу/прием данных на скорости 10 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 10 Мбит/с.
	Желтый	Мигает	Данный коммутатор осуществляет передачу/прием данных на скорости 100 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 100 Мбит/с.
		Не горит	Соединение с сетью Ethernet не установлено.
FDX	Желтый	Горит	Порт работает в дуплексном режиме.
		Не горит	Порт работает в полудуплексном режиме, коллизии отсутствуют.
Порты Ethernet (только на ES-3124PWR)			
LNK/ACT	Зеленый	Мигает	Данный коммутатор осуществляет передачу/прием данных на скорости 10 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 10 Мбит/с.
	Желтый	Мигает	Данный коммутатор осуществляет передачу/прием данных на скорости 100 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 100 Мбит/с.
		Не горит	Соединение с сетью Ethernet не установлено.

Таблица 3 Индикаторы (продолжение)

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
PoE	Желтый	Горит	Данный коммутатор обеспечивает питанием подключенное устройство, которое поддерживает стандарт PoE.
		Не горит	Устройство к данному порту не подключено или коммутатор не обеспечивает питание устройства по витой паре.
Порты SFP на 100 Мбит/с (только на ES-3124F)			
LNK	Желтый	Горит	Соединение установлено успешно.
		Не горит	Ethernet-устройство к порту не подключено.
ACT	Желтый	Мигает	Осуществляется прием или передача данных через порт.
Порты Gigabit Ethernet			
LNK/ACT	Зеленый	Мигает	Данный коммутатор осуществляет передачу/прием данных на скорости 1000 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 1000 Мбит/с.
	Желтый	Мигает	Данный коммутатор осуществляет передачу/прием данных на скорости 100 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 100 Мбит/с.
	Не горит	Соединение с сетью Ethernet не установлено.	
FDX	Желтый	Горит	Порт Gigabit Ethernet работает в дуплексном режиме.
		Не горит	Порт Gigabit Ethernet работает в полудуплексном режиме, коллизии отсутствуют.
Порты mini-GBIC			
LNK	Зеленый	Горит	Соединение установлено успешно.
		Не горит	Ethernet-устройство к порту не подключено.
ACT	Зеленый	Мигает	Осуществляется прием или передача данных через порт.
Порт MGMT			
10	Зеленый	Мигает	Данный коммутатор осуществляет обмен данными (прием/передачу) с устройством Ethernet.
		Горит	Установлено соединение на скорости 10 Мбит/с.
	Не горит	Нет соединения на скорости 10 Мбит/с или соединения с устройством Ethernet.	
100	Желтый	Мигает	Данный коммутатор осуществляет обмен данными (прием/передачу) с устройством Ethernet.
		Горит	Установлено соединение на скорости 100 Мбит/с.
	Не горит	Нет соединения на скорости 100 Мбит/с или соединения с устройством Ethernet.	

ЧАСТЬ III

Web-конфигуратор

- Web-конфигуратор (55)
- Пример первичной настройки (67)
- Состояние системы и статистика портов (71)
- Основные настройки (77)
- Виртуальные локальные сети (VLAN) (91)
- Настройка пересылки на основе статических MAC-адресов (109)
- Фильтрация (111)
- Протокол покрывающего дерева (113)
- Управление пропускной способностью (135)
- Контроль широковещательных штормов (139)
- Зеркальное копирование (141)
- Агрегация каналов (143)
- Аутентификация портов (151)
- Средства безопасности портов (157)
- Классификация (161)
- Правила политики (167)
- Метод организации очередей (175)
- Стекирование VLAN (179)
- Мультивещание (185)
- Аутентификация и учет (201)
- Защита от подмены IP-адресов (215)
- Защита от образования петель (241)
- Статические маршруты (245)

Дифференцированное обслуживание (247)
DHCP (255)
Обслуживание (261)
Контроль доступа (269)
Диагностика (291)
Системный журнал Syslog (293)
Управление кластерами (297)
Таблица MAC-адресов (303)
Таблица ARP (305)
Настройка клонирования (307)

Web-конфигуратор

В данном разделе описаны настройки и функции Web-конфигуратора.

4.1 Введение

Web-конфигуратор – это интерфейс управления на основе HTML, который позволяет легко настраивать и управлять коммутатором через Интернет-браузер. Следует использовать программы Internet Explorer 6.0 и более поздних версий, или Netscape Navigator 7.0 и более поздних версий. Рекомендованное разрешение экрана – 1024 на 768 пикселей.

Для использования Web-конфигуратора нужно разрешить:

- Всплывающие окна браузера на устройстве. Блокировка всплывающих окон браузера по умолчанию включена в операционной системе Windows XP SP (Service Pack) 2.
- JavaScript (по умолчанию включен).
- Разрешения Java (по умолчанию включены).

4.2 Вход в систему

- 1 Запустите Web-браузер.
- 2 Введите «http://» и IP-адрес коммутатора (например, адрес по умолчанию – 192.168.1.1) в поле адреса. Нажмите [ENTER].
- 3 Появится экран ввода имени и пароля. Имя пользователя по умолчанию – **admin**, а соответствующий ему пароль по умолчанию – **1234**. Дата и время будут показаны так, как на рисунке, если вы не настроили сервер времени и не ввели дату и время в меню **General Setup**.

Рисунок 19 Web-конфигуратор: вход в систему



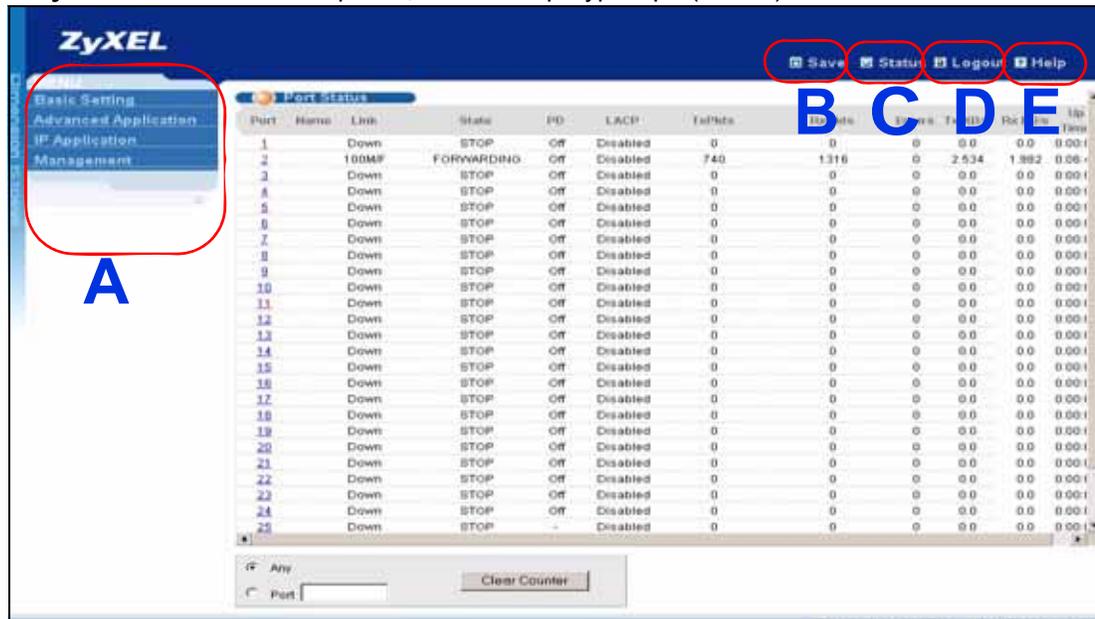
4 Нажмите **OK**, чтобы попасть на начальный экран Web-конфигуратора.

4.3 Окно состояния (Status)

После получения доступа к Web-конфигуратору первым отображается экран **Status**.

На приведенном ниже рисунке показаны элементы навигации по экрану Web-конфигуратора.

Рисунок 20 Начальная страница Web-конфигуратора (Status)



A – Нажатие на пункты меню раскрывает ссылки на пункты подменю; выбор одного из пунктов подменю открывает соответствующий экран в основном окне.

B, C, D, E – С помощью этих быстрых ссылок можно выполнять определенные действия независимо от текущего экрана.

В – Нажатие на данную ссылку вызывает сохранение конфигурации в энергонезависимой памяти коммутатора. Содержимое энергонезависимой памяти записывается в файл конфигурации, который используется коммутатором для загрузки, и не изменяется даже при отключении питания коммутатора. Более подробную информацию о сохранении настроек в определенный файл конфигурации можно найти в [разд. 29.3 на стр. 262](#).

С – Нажатие на данную ссылку вызывает переход на страницу состояния коммутатора.

D – Нажатие на данную ссылку вызывает выход из Web-конфигуратора.

E – Нажатие на данную ссылку открывает страницы справки. На страницах справки приводятся описания всех экранов настройки.

Чтобы открыть список ссылок в подменю, нажмите на основную ссылку в панели навигации.

Таблица 4 Обзор подменю панели навигации

BASIC SETTING (ОСНОВНЫЕ НАСТРОЙКИ)	ADVANCED APPLICATION (РАСШИРЕННЫЕ ПРИЛОЖЕНИЯ)	IP APPLICATION (IP-ПРИЛОЖЕНИЯ)	MANAGEMENT (УПРАВЛЕНИЕ)
			

Экраны различных подменю Web-конфигуратора перечислены в следующей таблице.

Таблица 5 Содержание экранов подменю Web-конфигуратора

BASIC SETTING (ОСНОВНЫЕ НАСТРОЙКИ)	ADVANCED APPLICATION (РАСШИРЕННЫЕ ПРИЛОЖЕНИЯ)	IP APPLICATION (IP-ПРИЛОЖЕНИЯ)	MANAGEMENT (УПРАВЛЕНИЕ)
System Info (Информация о системе) General Setup (Общие настройки) Switch Setup (Настройка коммутатора) IP Setup (Настройка протокола IP) Port Setup (Настройки портов)	VLAN Status (Состояние VLAN) VLAN Detail (Детали VLAN) VLAN Port Setting (Настройки портов VLAN) Subnet Based VLAN (VLAN на основе подсетей) Protocol Based VLAN (VLAN на основе протоколов) Static VLAN (Статические VLAN) Static MAC Forwarding (Пересылка на основе статических MAC-адресов) Filtering (Фильтрация) Spanning Tree Protocol Status (Состояние протокола покрывающего дерева) Spanning Tree Configuration (Настройка протокола покрывающего дерева) Rapid Spanning Tree Protocol (Быстрый протокол покрывающего дерева) Multiple Rapid Spanning Tree Protocol (Быстрый протокол нескольких экземпляров покрывающего дерева) Multiple Spanning Tree Protocol (Протокол нескольких экземпляров покрывающего дерева) Bandwidth Control (Управление пропускной способностью) Broadcast Storm Control (Контроль широковещательных штормов) Mirroring (Зеркальное копирование)	Static Routing (Статические маршруты) DiffServ (Дифференцированное обслуживание) 2-Rate 3 Color Marker (Маркировка TRTCM) DSCP Setting (Настройки DSCP) DHCP Status (Состояние DHCP) DHCP Relay (Ретрансляция DHCP) VLAN Setting (Настройки VLAN)	Maintenance (Обслуживание) Firmware Upgrade (Обновление встроенного программного обеспечения) Restore Configuration (Восстановление конфигурации) Backup Configuration (Резервное копирование конфигурации) Access Control (Контроль доступа) SNMP (Протокол SNMP) Trap Group (Группы «ловушек») Logins (Пользователи и пароли) Service Access Control (Контроль доступа к службам) Remote Management (Удаленное управление) Diagnostic (Диагностика) Syslog Setup (Настройки системного журнала) Syslog Server Setup (Настройка сервера syslog) Cluster Management Status (Состояние управления кластером) Clustering Management Configuration (Настройка управления кластерами)

Таблица 5 Содержание экранов подменю Web-конфигуратора (продолжение)

BASIC SETTING (ОСНОВНЫЕ НАСТРОЙКИ)	ADVANCED APPLICATION (РАСШИРЕННЫЕ ПРИЛОЖЕНИЯ)	IP APPLICATION (IP-ПРИЛОЖЕНИЯ)	MANAGEMENT (УПРАВЛЕНИЕ)
	<p>Link Aggregation Status (Состояние агрегации каналов)</p> <p>Link Aggregation Setting (Настройка агрегации каналов)</p> <p>Link Aggregation Control Protocol (Протокол управления агрегацией каналов LACP)</p> <p>Port Authentication (Аутентификация портов)</p> <p>802.1x</p> <p>MAC Authentication (Аутентификация по MAC-адресам)</p> <p>Port Security (Средства безопасности портов)</p> <p>Classifier (Классификация)</p> <p>Policy Rule (Правила политики)</p> <p>Queuing Method (Метод организации очередей)</p> <p>VLAN Stacking (Стекирование VLAN)</p> <p>Multicast Status (Состояние мультивещания)</p> <p>Multicast Setting (Настройка мультивещания)</p> <p>IGMP Snooping VLAN (VLAN отслеживания многоадресного трафика IGMP)</p> <p>IGMP Filtering Profile (Профиль фильтрации IGMP)</p> <p>MVR (Регистрация VLAN-сети мультивещания)</p> <p>Group Configuration (Настройка групп)</p> <p>Authentication and Accounting (Аутентификация и учет)</p> <p>RADIUS Server Setup (Настройка сервера RADIUS)</p> <p>TACACS+ Server Setup (Настройка сервера TACACS+)</p> <p>Auth and Acct Setup (Настройка аутентификации и учета)</p>		<p>MAC Table (Таблица MAC-адресов)</p> <p>ARP Table (Таблица ARP)</p> <p>Configure Clone (Настройка клонирования)</p>

Таблица 5 Содержание экранов подменю Web-конфигуратора (продолжение)

BASIC SETTING (ОСНОВНЫЕ НАСТРОЙКИ)	ADVANCED APPLICATION (РАСШИРЕННЫЕ ПРИЛОЖЕНИЯ)	IP APPLICATION (IP-ПРИЛОЖЕНИЯ)	MANAGEMENT (УПРАВЛЕНИЕ)
	IP Source Guard (Защита от подмены IP-адресов) IP Source Guard Static Binding (Статическая привязка для защиты от подмены IP-адресов) DHCP Snooping (Отслеживание DHCP) DHCP Snooping Configure (Настройка отслеживания DHCP) DHCP Snooping Port Configure (Настройка портов отслеживания DHCP) DHCP Snooping VLAN Configure (Настройка VLAN отслеживания DHCP) ARP Inspection Status (Состояние инспекции ARP-пакетов) ARP Inspection Log Status (Состояние журнала инспекции ARP-пакетов) ARP Inspection Configure (Настройка инспекции ARP-пакетов) ARP Inspection Port Configure (Настройка портов для инспекции ARP-пакетов) ARP Inspection VLAN Configure (Настройка сети VLAN для инспекции ARP-пакетов) Loopguard (Защита от образования петель)		

Пункты меню навигационной панели описаны в следующей таблице.

Таблица 6 Пункты меню навигационной панели

ПУНКТ	ОПИСАНИЕ
Basic Setting (Основные настройки)	
System Info (Информация о системе)	Этот пункт открывает экран общей информации о системе и мониторинга аппаратного обеспечения.
General Setup (Общие настройки)	Этот пункт открывает экран, позволяющий настроить общую идентификационную информацию о коммутаторе.
Switch Setup (Настройка коммутатора)	Этот пункт открывает экран, позволяющий настроить глобальные параметры коммутатора, такие как тип VLAN, получение таблицы MAC-адресов, протокол GARP и приоритеты очереди.

Таблица 6 Пункты меню навигационной панели (продолжение)

ПУНКТ	ОПИСАНИЕ
IP Setup (Настройка протокола IP)	Этот пункт открывает экран, позволяющий настроить IP-адрес и маску подсети управления (необходимые для управления коммутатором), а также сервер DNS (сервер доменных имен).
Port Setup (Настройки портов)	Этот пункт открывает экраны, позволяющие настроить отдельные порты коммутатора.
Advanced Application (Расширенные приложения)	
VLAN (Виртуальные локальные сети)	Этот пункт открывает экраны, позволяющие настроить виртуальные локальные сети на основе портов или стандарта 802.1Q (в зависимости от того, что было выбрано в меню Switch Setup). На этих экранах имеется также возможность настроить VLAN на основе протоколов и VLAN на основе подсетей.
Static MAC Forwarding (Пересылка на основе статических MAC-адресов)	Этот пункт открывает экраны, позволяющие настроить статические MAC-адреса для каждого из портов. Такие статические MAC-адреса не имеют срока действия.
Filtering (Фильтрация)	Этот пункт открывает экран, позволяющий настроить правила фильтрации.
Spanning Tree Protocol (Протокол покрывающего дерева)	Этот пункт открывает экраны, позволяющие настроить протоколы RSTP/MRSTP/MSTP для предотвращения петель в сети.
Bandwidth Control (Управление пропускной способностью)	Этот пункт открывает экраны, позволяющие настроить пределы пропускной способности от одного или нескольких начальных пунктов к одному или нескольким указанным пунктам назначения.
Broadcast Storm Control (Контроль широковещательных штормов)	Этот пункт открывает экран, позволяющий настроить фильтры широковещательной передачи.
Mirroring (Зеркальное копирование)	Этот пункт открывает экраны, позволяющие настроить копирование трафика от одного или нескольких портов на другой порт, чтобы можно было проверить трафик на первом порту, не вмешиваясь в его поток.
Link Aggregation (Агрегация каналов)	Этот пункт открывает экран, позволяющий логически объединить несколько физических каналов в один логический канал большей пропускной способности.
Port Authentication (Аутентификация портов)	Этот пункт открывает экран, позволяющий настроить аутентификацию портов на основе IEEE 802.1x, а также аутентификацию по MAC-адресам для клиентов, подключающихся к коммутатору.
Port Security (Средства безопасности портов)	Этот пункт открывает экран, позволяющий включить получение таблицы MAC-адресов и установить максимальное количество MAC-адресов, которые может запомнить порт.
Classifier (Классификация)	Этот пункт открывает экран, позволяющий настроить на коммутаторе группировку пакетов по определенным критериям.
Policy Rule (Правила политики)	Этот пункт открывает экран, позволяющий настроить на коммутаторе особую обработку сгруппированных пакетов.
Queuing Method (Метод организации очередей)	Этот пункт открывает экран, позволяющий настроить методы постановки в очередь, а также установить значения весов для каждого из портов.
VLAN Stacking (Стекирование VLAN)	Этот пункт открывает экран, позволяющий настроить стекирование сетей VLAN.
Multicast (Мультивещание)	Этот пункт открывает экран, позволяющий настроить различные функции мультивещания и создать VLAN-сети мультивещания.

Таблица 6 Пункты меню навигационной панели (продолжение)

ПУНКТ	ОПИСАНИЕ
Auth and Acct (Аутентификация и учет)	Этот пункт открывает экран, позволяющий настроить различные функции аутентификации и учета с использованием внешних серверов. В качестве таких внешних серверов могут выступать серверы RADIUS (Remote Authentication Dial-In User Service) или TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard (Защита от подмены IP-адресов)	Этот пункт открывает экран, позволяющий настроить фильтрацию несанкционированных DHCP и ARP-пакетов в вашей сети.
Loop Guard (Защита от образования петель)	Этот пункт открывает экран, позволяющий настроить защиту от образования сетевых петель на границе сети.
IP Application (IP-приложения)	
Static Route (Статические маршруты)	Этот пункт открывает экраны, позволяющие настроить статические маршруты. Статический маршрут указывает коммутатору, куда следует направлять IP-трафик, посредством ручной настройки параметров протокола TCP/IP.
DiffServ (Дифференцированное обслуживание)	Этот пункт открывает экраны, позволяющие включить DiffServ, настроить правила маркировки и определить отображения между битами DSCP и IEEE802.1p.
DHCP (Протокол DHCP)	Этот пункт открывает экран, позволяющий настроить протокол DHCP.
Management (Управление)	
Maintenance (Обслуживание)	Этот пункт открывает экраны, позволяющие работать с файлами конфигурации и встроенного программного обеспечения, а также осуществлять перезагрузку системы.
Access Control (Контроль доступа)	Этот пункт открывает экраны, позволяющие изменить имя входа и пароль доступа к системе, а также настроить протокол SNMP и удаленное управление.
Diagnostic (Диагностика)	Этот пункт открывает экраны, позволяющие просматривать системные журналы и тестировать порты.
Syslog (Системный журнал)	Этот пункт открывает экраны, позволяющие настраивать системные журналы и сервер системного журнала.
Cluster Management (Управление кластерами)	Этот пункт открывает экран, позволяющий настроить управление кластерами и просмотреть его состояние.
MAC Table (Таблица MAC-адресов)	Этот пункт открывает экран, позволяющий просматривать MAC-адреса (и типы) устройств, подключенных к каким-либо портам, а также идентификаторы виртуальных локальных сетей VLAN ID.
ARP Table (Таблица ARP)	Этот пункт открывает экран, позволяющий просмотреть таблицу соответствия MAC-адресов и IP-адресов.
Configure Clone (Настройка клонирования)	Данный пункт открывает экран, позволяющий скопировать настройки одного из портов на другие порты.

4.3.1 Изменение пароля

После первого входа в систему рекомендуется изменить пароль администратора по умолчанию. Нажмите **Management > Access Control > Logins**, чтобы отобразить следующий экран.

Рисунок 21 Изменение пароля администратора

Logins Access Control

Administrator

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Edit Logins

Login	User Name	Password	Retype to confirm
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

4.4 Сохранение конфигурации

Закончив изменение настроек на экране, нажмите **Apply** для сохранения изменений в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

Чтобы сохранить конфигурацию в энергонезависимой памяти, нажмите на ссылку **Save** в правом верхнем углу Web-конфигуратора. Под энергонезависимой памятью коммутатора понимается память, содержимое которой сохраняется даже при отключении питания коммутатора.



После завершения сеанса настройки обязательно воспользуйтесь ссылкой **Save**.

4.5 Блокировка коммутатора

Выполнение любого из следующих действий приводит к блокированию возможности внутрисетового управления коммутатором (управления через порты передачи данных) для всех пользователей:

- 1 Удаление виртуальной локальной сети управления (по умолчанию – VLAN 1).
- 2 Удаление всех виртуальных локальных сетей на основе портов, членом которых является порт CPU. «Порт CPU» – это управляющий порт коммутатора.
- 3 Установка фильтрации всего трафика для порта CPU.
- 4 Отключение всех портов.
- 5 Ошибка в текстовом конфигурационном файле.
- 6 Утрата пароля и/или IP-адреса.

- 7 Запрет доступа к коммутатору для всех служб.
- 8 Изменение номера порта службы и его утрата.



Соблюдайте осторожность, чтобы не заблокировать доступ к коммутатору для себя и всех остальных пользователей. В случае блокирования доступа попробуйте воспользоваться для настройки коммутатора внеполосным каналом управления (через порт управления).

4.6 Сброс коммутатора

Если коммутатор оказался заблокирован для вас (и остальных пользователей), или вы забыли пароль администратора, потребуется загрузить файл конфигурации по умолчанию.

4.6.1 Загрузка файла конфигурации

При загрузке файла конфигурации с заводскими настройками имеющийся файл конфигурации заменяется файлом с заводскими настройками. При этом все предыдущие настройки будут сброшены, а скорость консольного порта вернется к стандартным параметрам (9600 бод, 8 бит данных, четности нет, 1 стоп-бит, управление потоком отключено). Кроме того, будет установлен пароль «1234» и IP-адрес 192.168.1.1.

Для загрузки файла конфигурации сделайте следующее:

- 1 Подключитесь к консольному порту с помощью программы-эмулятора терминала, установленной на компьютере. Более подробную информацию можно найти в [разд. 3.1.1 на стр. 47](#).
- 2 Отключите и включите снова питание коммутатора, чтобы начать сессию. При повторном включении питания коммутатора вы увидите начальный экран.
- 3 Получив сообщение «Press any key to enter Debug Mode within 3 seconds...», нажмите любую клавишу для входа в режим отладки.
- 4 Наберите команду `atlc` после сообщения «Enter Debug Mode».
- 5 Дождитесь сообщения «Starting XMODEM upload», после чего активируйте режим загрузки XMODEM на своем терминале.
- 6 После загрузки файла конфигурации наберите команду `atgo` для перезагрузки коммутатора.

Рисунок 22 Сброс коммутатора: через консольный порт

```

Bootbase Version: V0.7 | 02/17/2006 11:56:33
RAM:Size = 64 Mbytes
DRAM POST: Testing: 65536K   OK
DRAM Test SUCCESS !
FLASH: Intel 32M

ZyNOS Version: V3.80(AIC.0)b0 | 01/19/2007 19:06:37

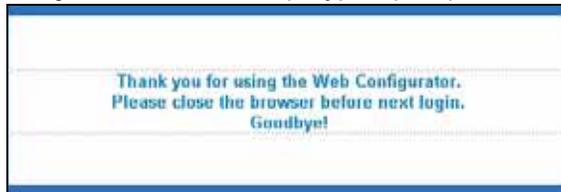
Press any key to enter debug mode within 3 seconds.....
Enter Debug Mode
ES-3124> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total 393216 bytes received.
Erasing..
.....
OK
ES-3124> atgo

```

Теперь коммутатор перезагружен с файлом настроек по умолчанию, включая пароль «1234».

4.7 Выход из Web-конфигуратора

Чтобы выйти из Web-конфигуратора, нажмите **Logout** на экране. Для повторного входа после выхода необходимо будет заново ввести пароль. Данное действие рекомендуется выполнить после окончания сеанса управления по соображениям безопасности.

Рисунок 23 Web-конфигуратор: экран выхода

4.8 Помощь

Страница онлайн-справки по Web-конфигуратору содержит описания отдельных экранов, а также дополнительную информацию.

Чтобы получить в режиме онлайн описание конкретного экрана, выберите пункт **Help** на соответствующем экране Web-конфигуратора.

Пример первичной настройки

В данной главе описаны настройки коммутатора на примере конкретной сети.

5.1 Обзор

Первичная настройка включает в себя следующие шаги:

- Создание виртуальной локальной сети VLAN
- Определение идентификаторов VLAN для портов
- Настройка IP-адреса управления коммутатором

5.1.1 Создание виртуальной локальной сети VLAN

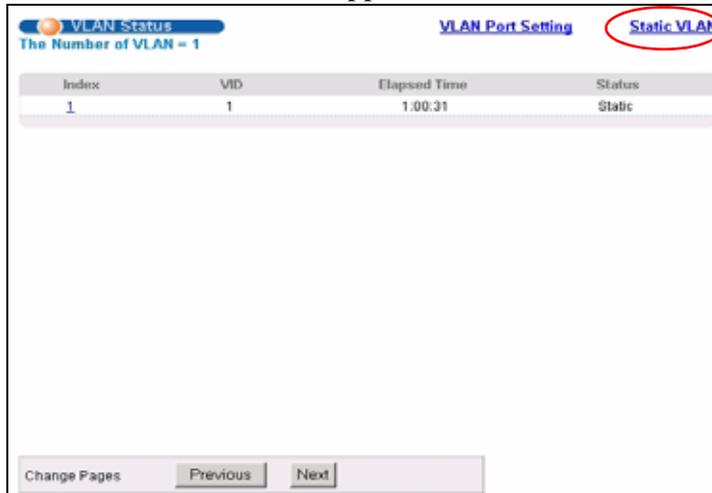
Виртуальные локальные сети ограничивают широковещательные кадры той группой VLAN, к которой принадлежит порт (порты). Для этого можно использовать виртуальные локальные сети на основе портов или статические виртуальные локальные сети на основе тегов с фиксированными портами-членами. В данном примере порт 1 конфигурируется в качестве члена виртуальной локальной сети VLAN 2.

Рисунок 24 Пример первичной настройки сети: виртуальная локальная сеть

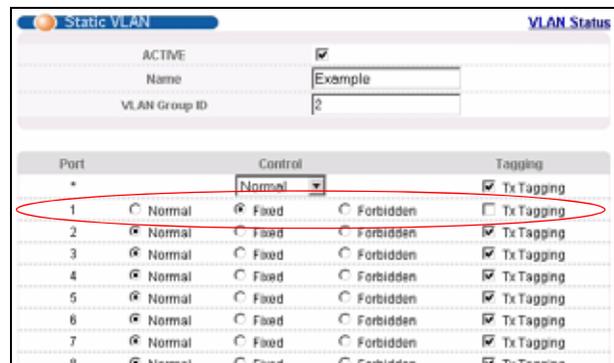


Index	VID	Elapsed Time	Status
1	1	1:00:31	Static

1 Нажмите **Advanced Application > VLAN > Static VLAN**.



- 2 На экране **Static VLAN** выберите **ACTIVE**, введите имя-описание в поле **Name** и введите 2 в поле **VLAN Group ID** для сети **VLAN2**.



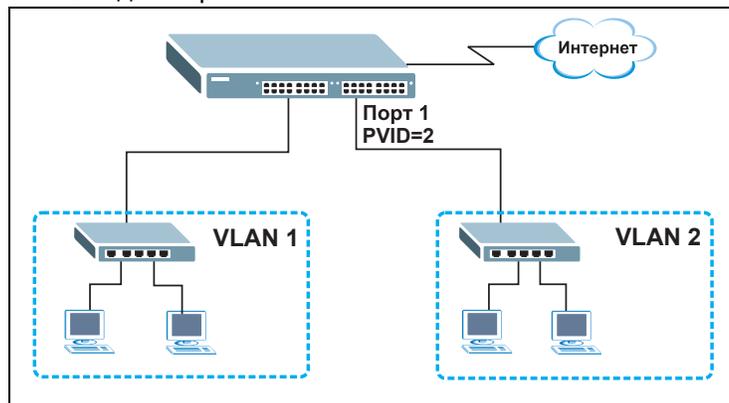
Поле **VLAN Group ID** на этом экране и поле **VID** на экране меню **IP Setup** относятся к одному и тому же идентификатору виртуальной локальной сети VLAN ID.

- 3 Поскольку сеть **VLAN2** подключена к порту 1 коммутатора, выберите пункт **Fixed**, чтобы назначить порт 1 постоянным членом только этой VLAN.
- 4 Чтобы не поддерживающие идентификаторы VLAN устройства (например, компьютеры и концентраторы) правильно принимали кадры, снимите выделение с переключателя **TX Tagging** – тогда коммутатор будет удалять теги VLAN перед отправкой.
- 5 Нажмите **Add**, чтобы сохранить настройки в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

5.1.2 Назначение идентификатора виртуальной локальной сети VID для порта

Идентификатор виртуальной локальной сети для порта (PVID) используется для добавления тегов к кадрам без тегов, поступающим на этот порт, чтобы такие кадры направлялись в ту группу VLAN, которую определяет тег. В данном примере необходимо установить 2 в качестве идентификатора VID для порта 1, чтобы все немеченные тегами кадры, принятые через этот порт, отправлялись в виртуальную локальную сеть VLAN 2.

Рисунок 25 Пример первичной настройки сети: идентификатор виртуальной локальной сети для порта



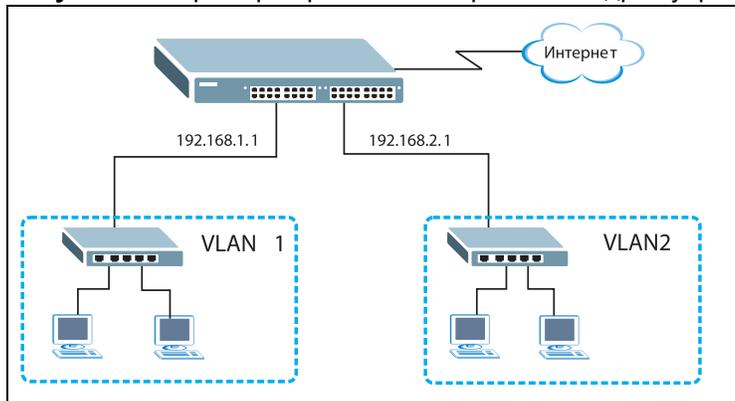
- 1 Нажмите **Advanced Application > VLAN > VLAN Port Setting**.
- 2 Введите 2 в поле **PVID** для порта 1 и нажмите **Apply**, чтобы сохранить изменения в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

Port	Ingress Check	PVID	GVIP	Acceptable Frame Type	VLAN Trunking
1	<input type="checkbox"/>	2	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

5.2 Настройка IP-адреса управления коммутатором

По умолчанию в качестве IP-адреса управления на коммутаторе используется адрес 192.168.1.1. Для управления устройством можно настроить другой IP-адрес из отличной подсети. Пример показан на следующем рисунке.

Рисунок 26 Пример первичной настройки: IP-адрес управления



- 1 Подключите компьютер к любому из портов Ethernet на коммутаторе. Убедитесь, что компьютер находится в той же подсети, что и коммутатор.
- 2 Откройте Web-браузер и введите в строке адреса 192.168.1.1 (IP-адрес по умолчанию), чтобы получить доступ к Web-конфигуратору. Дополнительную информацию можно найти в [разд. 4.2 на стр. 55](#).
- 3 Нажмите **Basic Setting > IP Setup**.
- 4 Введите нужную информацию на экране **IP Setup**.
Для сети **VLAN2** введите в качестве IP-адреса 192.168.2.1 и маску подсети 255.255.255.0.
- 5 В поле **VID** введите идентификатор группы VLAN, к которой должен принадлежать этот IP-адрес управления. Это должно быть то же значение, которое было введено в поле **VLAN ID** на экране меню **Static VLAN**.
- 6 Установите переключатель **Manageable**, чтобы разрешить управление коммутатором через порты, принадлежащие сети **VLAN2**, с использованием указанного IP-адреса.
- 7 При необходимости повторите данную процедуру для сети **VLAN1**.

Index	IP Address	IP Subnet Mask	VID	Default Gateway	Manageable	Delete
	192.168.2.1	255.255.255.0	2	192.168.2.254	<input checked="" type="checkbox"/>	

Нажмите **Add**, чтобы сохранить изменения в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

Состояние системы и статистика портов

В данной главе описаны экраны состояния системы (начальная страница Web-конфигуратора) и детальной информации по портам.

6.1 Обзор

Начальная страница Web-конфигуратора содержит сводную статистику по портам со ссылками на каждый порт, позволяющими отобразить детальную статистику каждого порта.

6.2 Сводная информация о состоянии портов

Для просмотра статистики по портам нажмите **Status** на любом из экранов конфигуратора, чтобы отобразить окно **Status**, как показано на иллюстрации.

Рисунок 27 Экран Status

Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
2		100MF	FORWARDING	Off	Disabled	1844956	2307414	0	8.324	1.600	81:00:32
3		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
4		100MF	FORWARDING	Off	Disabled	2305107	1039712	1	0.0	0.0	29:57:40
5		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Off	Disabled	4737	249	0	0.0	0.0	0:00:00
7		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00

Поля экрана описаны в следующей таблице.

Таблица 7 Экран Status

ПОЛЕ	ОПИСАНИЕ
Port	Номер Ethernet-порта. Нажмите на номер порта, чтобы отобразить экран подробной статистики порта Port Details (см. рис. 28 на стр. 73).
Name	Имя, назначенное данному порту на экране Basic Setting > Port Setup .

Таблица 7 Экран Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
Link	В этом поле отображается скорость (10M для 10 Мбит/с, 100M для 100 Мбит/с или 1000M для 1000 Мбит/с) и режим дуплекса (F для дуплекса или H для полудуплекса). Кроме того, в поле отображается тип кабеля (Copper для витой пары или Fiber для оптоволокну) для комбинированных портов.
State	Если активирован протокол покрывающего дерева STP, в этом поле отображается состояние порта по протоколу STP (дополнительную информацию можно найти в разд. 11.1.3 на стр. 115). Если протокол STP отключен, в этом поле отображается FORWARDING в случае установленного соединения и STOP в противном случае.
PD (только на моделях PWR)	В этом поле отображается On , если на данном порту включено питание устройств по витой паре (PoE) и к нему подключено питаемое устройство. Если питаемое устройство отсоединено или питание устройств по витой паре на данном порту отключено, в этом поле отображается Off .
LACP	В этом поле отображается состояние протокола LACP (протокол управления агрегацией каналов) – включен он или нет на данном порту.
TxPkts	В этом поле отображается количество переданных этим портом кадров.
RxPkts	В этом поле отображается количество принятых этим портом кадров.
Errors	В этом поле отображается количество принятых этим портом кадров с ошибками.
Tx KB/s	В этом поле отображается количество переданных этим портом килобайт в секунду.
Rx KB/s	В этом поле отображается количество принятых этим портом килобайт в секунду.
Up Time	В этом поле отображается полное количество часов, минут и секунд, в течение которых порт работал.
Clear Counter	Чтобы сбросить статистику для отдельного порта, введите номер соответствующего порта и нажмите кнопку Clear Counter ; чтобы сбросить статистику для всех портов – выберите Any и также нажмите кнопку Clear Counter .

6.2.1 Экран Status: Port Details

Чтобы отобразить статистику по отдельному порту, выберите номер в столбце **Port** на экране **Status**. Этот экран используется для отображения состояния и подробных данных о работе отдельного порта коммутатора.

Рисунок 28 Экран Status: Port Details

Port Info		Port NO.	1
Name			
Link		Down	
Status		STOP	
PD PowerConsumption (mW)		0	
PD MaxCurrent (mA)		0.0	
PD MaxPower (mW)		0	
LACP		Disabled	
TxPkts		0	
RxPkts		0	
Errors		0	
Tx Kbps/s		0.0	
Rx Kbps/s		0.0	
Up Time		0:00:00	
TX Packet			
Tx Packets		0	
Multicast		0	
Broadcast		0	
Pause		0	
Tagged		0	
RX Packet			
Rx Packets		0	
Multicast		0	
Broadcast		0	
Pause		0	
Control		0	
TX Collision			
Single		0	
Multiple		0	
Excessive		0	
Late		0	
Error Packet			
Rx CRC		0	
Length		0	
Runt		0	
Distribution			
64		0	
65 to 127		0	
128 to 255		0	
256 to 511		0	
512 to 1023		0	
1024 to 1510		0	
Giant		0	

Поля экрана описаны в следующей таблице.

Таблица 8 Экран Status > Port Details

ПОЛЕ	ОПИСАНИЕ
Port Info	
Port NO.	В этом поле отображается номер порта.
Name	В этом поле отображается имя порта.
Link	В этом поле отображается скорость (10M для 10 Мбит/с, 100M для 100 Мбит/с или 1000M для 1000 Мбит/с) и режим дуплекса (F для дуплекса или H для полудуплекса). Кроме того, в поле отображается тип кабеля (Copper для витой пары или Fiber для оптоволокну).
Status	Если активирован протокол покрывающего дерева STP, в этом поле отображается состояние порта по протоколу STP (дополнительную информацию можно найти в разд. 11.1.3 на стр. 115). Если протокол STP отключен, в этом поле отображается FORWARDING в случае установленного соединения и STOP в противном случае.
PD PowerConsumption (mW)	Данное поле предусмотрено только в моделях PWR, причем для портов Gigabit Ethernet и портов mini-GBIC оно недоступно. В этом поле отображается мощность, потребляемая питаемым устройством на соответствующем порту.

Таблица 8 Экран Status > Port Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
PD MaxCurrent (mA)	Данное поле предусмотрено только в моделях PWR, причем для портов Gigabit Ethernet и портов mini-GBIC оно недоступно. В этом поле отображается максимальное значение тока, которое коммутатор может подать на питаемое устройство. Если питаемое устройство потребляет мощность свыше максимального значения, обеспечиваемого коммутатором, подача питания со стороны коммутатора прекращается. Через каждый из портов Ethernet на 10/100 Мбит/с коммутатор может подавать на питаемое устройство ток до 351,36 мА, а совокупная мощность всех питаемых устройств, подключенных к коммутатору, не может превышать 123,2 Вт.
PD MaxPower (mW)	Данное поле предусмотрено только в моделях PWR, причем для портов Gigabit Ethernet и портов mini-GBIC оно недоступно. В этом поле отображается максимальная мощность, которую коммутатор может подать через порт.
LACP	В этом поле указано, включен ли для данного порта протокол LACP.
TxPkts	В этом поле отображается количество переданных этим портом кадров.
RxPkts	В этом поле отображается количество принятых этим портом кадров.
Errors	В этом поле отображается количество принятых этим портом кадров с ошибками.
Tx KB/s	В этом поле отображается количество переданных этим портом килобайт в секунду.
Rx KB/s	В этом поле отображается количество принятых этим портом килобайт в секунду.
Up Time	В этом поле отображается полное время, в течение которого поддерживалось соединение.
Tx Packet	В следующих полях отображается подробная информация о переданных пакетах.
TX Packets	В этом поле отображается количество переданных цельных пакетов (одноадресных, мультивещательных, широковещательных).
Multicast	В этом поле отображается количество переданных цельных мультивещательных пакетов.
Broadcast	В этом поле отображается количество переданных цельных широковещательных пакетов.
Pause	В этом поле отображается количество переданных пакетов 802.3x типа Pause.
Tagged	В этом поле отображается количество переданных пакетов с тегами VLAN.
Rx Packet	В следующих полях отображается подробная информация о принятых пакетах.
RX Packets	В этом поле отображается количество принятых цельных пакетов (одноадресных, мультивещательных, широковещательных).
Multicast	В этом поле отображается количество принятых цельных мультивещательных пакетов.
Broadcast	В этом поле отображается количество принятых цельных широковещательных пакетов.
Pause	В этом поле отображается количество принятых пакетов 802.3x типа Pause.
Control	В этом поле отображается количество принятых управляющих пакетов (в том числе с ошибками CRC), однако без учета пакетов Pause стандарта 802.3x.
TX Collision	В следующих полях отображается информация о коллизиях в процессе передачи.
Single	Количество успешно переданных пакетов, передача которых была запрещена в точности одиночной коллизией.

Таблица 8 Экран Status > Port Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
Multiple	Количество успешно переданных пакетов, передача которых была запрещена несколькими коллизиями.
Excessive	Количество пакетов, передача которых оказалась невозможна из-за избыточного количества коллизий. Под избыточным количеством коллизий понимается максимальное количество коллизий, после которого сбрасывается счетчик попыток повторной передачи.
Late	Количество зафиксированных с опозданием коллизий, то есть коллизий, обнаруженных после передачи как минимум 512 бит пакета.
Error Packet	В следующих полях отображается подробная информация о принятых пакетах с ошибками.
RX CRC	В этом поле отображается количество пакетов, принятых с ошибкой (ошибками) циклического избыточного кода CRC.
Length	В этом поле отображается количество принятых пакетов, длина которых выходит за пределы диапазона.
Runt	В этом поле отображается количество принятых пакетов, оказавшихся слишком короткими (менее 64 октетов), включая пакеты с ошибками CRC.
Distribution	
64	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет 64 октета.
От 65 до 127	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 65 до 127 октетов.
От 128 до 255	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 128 до 255 октетов.
От 256 до 511	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 256 до 511 октетов.
От 512 до 1023	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 512 до 1023 октетов.
От 1024 до 1518	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 1024 до 1518 октетов.
Giant	В этом поле отображается количество пакетов, отброшенных из-за превышения максимального размера кадра.

Основные настройки

В данной главе описаны настройки экранов **System Info (Информация о системе)**, **General Setup (Общие настройки)**, **Switch Setup (Настройка коммутатора)**, **IP Setup (Настройка протокола IP)** и **Port Setup (Настройки портов)**.

7.1 Обзор

На экране **System Info** отображается общая информация о коммутаторе (например, номер версии встроенного программного обеспечения), а также получаемые путем опроса параметры аппаратного обеспечения (например, скорость вращения вентиляторов). На экране **General Setup** можно настроить общую идентификационную информацию о коммутаторе. Кроме того, на экране **General Setup** можно вручную установить время или выбрать режим получения даты и времени с внешнего сервера при включении коммутатора. Тогда в системных журналах коммутатора будет отображаться реальное время. На экране **Switch Setup** можно установить и настроить глобальные функции коммутатора. На экране **IP Setup** можно настроить IP-адрес коммутатора, маску (маски) подсети и адрес сервера DNS для управления коммутатором.

7.2 Информация о системе

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Basic Setting > System Info**. Здесь можно узнать версию встроенного программного обеспечения, а также отслеживать температуру, скорость вращения вентиляторов и напряжение коммутатора.

Рисунок 29 Экран Basic Setting > System Info

System Name		ES-3124PWR			
ZyNOS F/W Version		V3.70(TY.0)80 7/10/2006			
Ethernet Address		00 13 49 00 00 02			

PoE Status					
Total Power (W)		375.0			
Consuming Power (W)		0.0			
Remaining Power (W)		375.0			

Hardware Monitor					
Temperature Unit <input type="button" value="C"/>					
Temperature (C)	Current	MAX	MIN	Threshold	Status
CPU	33.0	33.0	25.5	85.0	Normal
MAC	35.5	35.5	26.0	85.0	Normal
PHY1	29.0	29.0	25.0	85.0	Normal
PHY2	30.5	30.5	26.0	85.0	Normal
PHY3	30.0	30.5	26.0	85.0	Normal
ENV	34.0	34.0	25.0	65.0	Normal
FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	6194	6277	6009	2750	Normal
FAN2	6114	6222	6061	2750	Normal
FAN3	5950	6035	5803	2750	Normal
FAN4	6334	6450	6087	3250	Normal
FAN5	6277	6392	6061	3250	Normal
FAN6	6696	6696	6334	3250	Normal
FAN7	6222	6392	5984	3250	Normal
Voltage (V)	Current	MAX	MIN	Threshold	Status
VCCOREA	2.560	2.560	2.560	+/-10%	Normal
VINRO	1.264	1.264	1.248	+/-10%	Normal
3.3VIN	3.360	3.360	3.360	+/-8%	Normal
1.2VIN	11.916	11.916	11.916	+/-11%	Normal
1.3VIN	1.328	1.328	1.328	+/-10%	Normal
1.25VIN	1.264	1.264	1.248	+/-8%	Normal
1.0VIN	1.040	1.040	1.040	+/-10%	Normal
BPS_12VIN	--	--	--	--	Absent

Поля экрана описаны в следующей таблице.

Таблица 9 Экран Basic Setting > System Info

ПОЛЕ	ОПИСАНИЕ
System Name	В этом поле отображается имя-описание коммутатора, с помощью которого его можно идентифицировать.
ZyNOS F/W Version	В этом поле отображается номер версии текущего встроенного программного обеспечения коммутатора, в том числе дата его создания.
Ethernet Address	В этом поле отображается MAC-адрес коммутатора для сети Ethernet.
PoE Status	Данный раздел имеется только на моделях PWR.
Total Power (W)	Совокупная мощность в ваттах, которую коммутатор может обеспечить для питания устройств через Ethernet.
Consuming Power (W)	Мощность, потребляемая подключенными к коммутатору устройствами с поддержкой PoE.
Remaining Power (W)	Остающийся запас мощности в ваттах, которую коммутатор может обеспечить для питания устройств через Ethernet.

Таблица 9 Экран Basic Setting > System Info (продолжение)

ПОЛЕ	ОПИСАНИЕ
Hardware Monitor	
Temperature Unit	Предусмотренные в коммутаторе датчики температуры позволяют обнаруживать и сообщать о повышении температуры выше установленного порогового значения. В этом поле можно выбрать единицы измерения температуры (градусы по Цельсию – Centigrade, или градусы по Фаренгейту – Fahrenheit).
Temperature	MAC, CPU и PHY указывают расположение датчиков температуры на печатной плате коммутатора. ENV относится к температуре окружающей среды (воздуха) для коммутатора (только на моделях PWR).
Current	В этом поле отображается текущая температура, измеренная данным датчиком.
MAX	В этом поле отображается максимальная температура, измеренная данным датчиком.
MIN	В этом поле отображается минимальная температура, измеренная данным датчиком.
Threshold	В этом поле отображается верхний лимит температуры для данного датчика.
Status	Если температура не превышает порогового значения, в этом поле указывается Normal , в противном случае – Error .
FAN Speed (RPM)	Для соблюдения надлежащего теплового режима устройства огромное значение имеет правильная работа вентиляторов (наряду с хорошо вентилируемым, охлаждаемым помещением). В каждом из вентиляторов имеется датчик, который обнаруживает и сообщает о понижении скорости работы вентилятора ниже указанного порогового значения.
Current	В этом поле отображается текущая скорость вентилятора в оборотах в минуту (RPM).
MAX	В этом поле отображается максимальная измеренная скорость вентилятора в оборотах в минуту (RPM).
MIN	В этом поле отображается минимальная измеренная скорость вентилятора в оборотах в минуту (RPM). Если скорость слишком низкая и не поддается измерению (меньше 2000 об/мин), в этом поле указывается «<41».
Threshold	В этом поле отображается минимальная допустимая скорость работы вентилятора.
Status	Если скорость вентилятора выше установленного минимального значения, в этом поле указывается Normal . Если скорость вентилятора ниже установленного минимума, в этом поле указывается Error .
Voltage (V)	Для каждого значения напряжения в блоке питания имеется датчик, который способен обнаруживать и сообщать о выходе напряжения из допустимого диапазона.
Current	Текущее значение напряжения.
MAX	В этом поле отображается максимальное напряжение, измеренное в данной точке.
MIN	В этом поле отображается минимальное напряжение, измеренное в данной точке.
Threshold	В этом поле отображается допустимый процент отклонения напряжения от номинала, при котором коммутатор будет по-прежнему работать.
Status	Если напряжение в данной точке находится в допустимом диапазоне, в этом поле отображается Normal ; в противном случае отображается Error .

7.3 Общие настройки

На этом экране можно сконфигурировать общие параметры, такие как имя системы и время. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Basic Setting** и **General Setup**.

Рисунок 30 Экран Basic Setting > General Setup

Поля экрана описаны в следующей таблице.

Таблица 10 Экран Basic Setting > General Setup

ПОЛЕ	ОПИСАНИЕ
System Name	Выберите имя-описание, с помощью которого можно будет идентифицировать коммутатор. Максимальная длина имени – 64 печатных символа; пробелы допускаются.
Location	Введите адрес географического местоположения коммутатора. В поле можно ввести до 32 печатных символов ASCII; пробелы допускаются.
Contact Person's Name	Введите имя ответственного лица для данного коммутатора. В поле можно ввести до 32 печатных символов ASCII; пробелы допускаются.
Use Time Server when Bootup	<p>Укажите протокол службы времени, используемый вашим сервером времени. Не все серверы времени поддерживают все протоколы, поэтому нужный протокол, возможно, придется подбирать методом проб и ошибок. Основные различия между ними заключаются в формате времени.</p> <p>При выборе формата Daytime (RFC 867) коммутатор отображает день, месяц, год и время без учета поправки для часового пояса. При использовании этого формата рекомендуется использовать сервер времени, находящийся в вашем географическом часовом поясе.</p> <p>Формат Time (RFC-868) представляет собой 4-байтное целое, соответствующее общему количеству секунд с 0:0:0 1970/1/1.</p> <p>Формат NTP (RFC-1305) аналогичен формату Time (RFC-868).</p> <p>По умолчанию установлено значение None. Время вводится вручную. Каждый раз при включении коммутатора время и дата сбрасываются на 0:0 1970-1-1.</p>

Таблица 10 Экран Basic Setting > General Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Time Server IP Address	Введите IP-адрес сервера времени. Данный коммутатор будет искать сервер времени не более 60 секунд. При выборе недоступного сервера времени этот экран будет заблокирован на 60 секунд. Подождите.
Current Time	В этом поле отображается время, соответствующее моменту открытия этого меню (или его обновления).
New Time (hh:min:ss)	Введите новое время в формате «часы, минуты, секунды». После нажатия на Apply в поле Current Time появится новое время.
Current Date	В этом поле отображается дата, соответствующая моменту открытия этого меню.
New Date (yyyy-mm-dd)	Введите новую дату в формате «год, месяц, день». После нажатия на Apply в поле Current Date появится новая дата.
Time Zone	Выберите в ниспадающем списке разницу во времени между поясом UTC (всеобщее скоординированное время, ранее известное как GMT или время по Гринвичу) и вашим часовым поясом.
Daylight Saving Time	Период летнего времени – период с поздней весны до начала осени, когда во многих странах принято переводить часы на один час вперед в целях более рационального использования светлого времени суток по вечерам. При использовании летнего времени необходимо установить данный переключатель.
Start Date	Укажите день и час, когда начинается действие летнего времени (в случае выбора переключателя Daylight Saving Time). Время отображается в 24-часовом формате. Ниже приводится несколько примеров: Действие летнего времени в большинстве Соединенных Штатов начинается со второго воскресенья марта. В каждом из часовых поясов Соединенных Штатов летнее время вступает в силу в 2:00 по местному времени. Таким образом, для Соединенных Штатов необходимо выбрать Second (второе), Sunday (воскресенье), March (марта) и 2:00 . В странах Европейского Союза действие летнего времени начинается в последнее воскресенье марта. Во всех часовых поясах Европейского Союза летнее время вводится одномоментно (в 01:00 по Гринвичу или всеобщему скоординированному времени). Таким образом, для Европейского Союза необходимо выбрать Last (последнее), Sunday (воскресенье), March (март), а содержимое последнего поля зависит от конкретного часового пояса. Например, для Германии необходимо выбрать 2:00 , так как часовой пояс Германии соответствует +1 часу относительно Гринвича (GMT+1).
End Date	Укажите день и час, когда прекращается действие летнего времени (в случае выбора переключателя Daylight Saving Time). Время отображается в 24-часовом формате. Ниже приводится несколько примеров: Действие летнего времени в большинстве Соединенных Штатов прекращается с первого воскресенья ноября. В каждом из часовых поясов Соединенных Штатов летнее время отменяется в 2:00 по местному времени. Таким образом, для Соединенных Штатов необходимо выбрать First (первое), Sunday (воскресенье), November (ноября) и 2:00 . В странах Европейского Союза действие летнего времени прекращается в последнее воскресенье октября. Во всех часовых поясах Европейского Союза летнее время отменяется одномоментно (в 01:00 по Гринвичу или всеобщему скоординированному времени). Таким образом, для Европейского Союза необходимо выбрать Last (последнее), Sunday (воскресенье), October (октября), а содержимое последнего поля зависит от конкретного часового пояса. Например, для Германии необходимо выбрать 2:00 , так как часовой пояс Германии соответствует +1 часу относительно Гринвича (GMT+1).

Таблица 10 Экран Basic Setting > General Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

7.4 Введение в виртуальные локальные сети (VLAN)

Виртуальные локальные сети (VLAN, Virtual Local Area Network) позволяют разделить одну физическую сеть на несколько логических. Устройства в логической сети принадлежат к одной группе. Устройство может принадлежать к нескольким группам. При использовании сетей VLAN устройство не может отправлять или принимать данные от устройств, не принадлежащих к той же группе (группам); такой трафик должен проходить через маршрутизатор.

При использовании в бизнес-центрах с несколькими арендаторами виртуальные локальные сети VLAN – важнейший компонент обеспечения изоляции и безопасности абонентов сети. При условии надлежащей настройки виртуальные локальные сети не позволяют какому-либо пользователю получить доступ к ресурсам, принадлежащим другому пользователю в той же локальной сети, то есть пользователь не увидит принтеры и жесткие диски другого пользователя в том же здании.

Кроме того, виртуальные локальные сети повышают производительность сети за счет ограничения широковещательной рассылки сравнительно небольшими и легко управляемыми логическими широковещательными доменами. В традиционных коммутируемых средах все широковещательные пакеты направляются на все без исключения порты. При использовании виртуальных локальных сетей широковещательные пакеты рассылаются лишь в конкретном широковещательном домене.



Механизм поддержки виртуальных локальных сетей VLAN работает только в одном направлении; им контролируется только исходящий трафик.

Информацию о виртуальных локальных сетях на основе портов и на основе тегов 802.1Q можно найти в [гл. 8 на стр. 91](#).

7.5 Экран Switch Setup

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Basic Setting** и **Switch Setup**. Экраны настройки виртуальных локальных сетей VLAN изменяются в зависимости от того, какой пункт выбран в поле **VLAN Type**: **802.1Q** или **Port Based**. Информацию по виртуальным локальным сетям можно найти в соответствующей главе.

Рисунок 31 Экран Basic Setting > Switch Setup

Field	Value	Unit
VLAN Type	802.1Q	
Bridge Control Protocol Transparency	Active	
MAC Address Learning	Active	
Aging Time	300	seconds
Join Timer	200	milliseconds
Leave Timer	600	milliseconds
Leave All Timer	10000	milliseconds
Priority Queue Assignment	level7: 7, level6: 6, level5: 5, level4: 4, level3: 3, level2: 1, level1: 0, level0: 2	

Поля экрана описаны в следующей таблице.

Таблица 11 Экран Basic Setting > Switch Setup

ПОЛЕ	ОПИСАНИЕ
VLAN Type	Выберите 802.1Q или Port Based . Экран VLAN Setup изменится в зависимости от того, какой тип виртуальных локальных сетей VLAN выбран на этом экране: 802.1Q или Port Based . Дополнительную информацию можно найти в гл. 8 на стр. 91 .
Bridge Control Protocol Transparency	Выберите Active , чтобы разрешить на коммутаторе обработку протоколов управления мостами (например, STP). Кроме того, необходимо будет определить порядок обработки блоков данных мостового протокола BPDU на экране Port Setup .
MAC Address Learning	Функция получения (запоминания) MAC-адресов снижает объем исходящего широковещательного трафика. Получение MAC-адресов работает только на активных портах.
Aging Time	Введите время от 10 до 3000 секунд. Это период, в течение которого все динамически полученные MAC-адреса хранятся в таблице MAC-адресов. По его истечении они устаревают и должны быть получены заново.
GARP Timer: Коммутаторы присоединяются к виртуальным локальным сетям VLAN путем передачи декларации. Декларация представляет собой передачу сообщения Join с использованием протокола GARP. Декларации отменяются путем передачи сообщения Leave . Сообщение Leave All отменяет все декларации. Таймеры GARP определяют значения тайм-аута для декларации. Более подробную информацию можно найти в главе о VLAN.	

Таблица 11 Экран Basic Setting > Switch Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Join Timer	Параметр Join Timer определяет длительность таймера Join Period для протокола регистрации VLAN по GARP (GVRP) в миллисекундах. У каждого порта имеется таймер Join Period . Допустимый диапазон значений параметра Join Time – от 100 до 65 535 миллисекунд; по умолчанию это значение равно 200 миллисекундам. Более подробную информацию можно найти в главе о VLAN.
Leave Timer	Параметр Leave Time определяет длительность таймера Leave Period для протокола GVRP в миллисекундах. У каждого порта имеется отдельный таймер Leave Period . Значение параметра Leave Time должно быть в два раза больше параметра Join Timer ; по умолчанию оно равно 600 миллисекундам.
Leave All Timer	Параметр Leave All Timer определяет длительность таймера Leave All Period для протокола GVRP в миллисекундах. У каждого порта имеется отдельный таймер Leave All Period. Значение параметра Leave All Timer должно больше параметра Leave Timer.
<p>Priority Queue Assignment</p> <p>Стандарт IEEE 802.1p различает до 8 отдельных типов трафика путем добавления в кадр MAC-уровня тега, содержащего биты определения класса обслуживания. Кадры без явного тега приоритета получают на входящем порту приоритет по умолчанию. Следующие два поля используются для определения соответствия между уровнями приоритетов и физическими очередями.</p> <p>У коммутатора имеется восемь физических очередей, которые можно поставить в соответствие 8 уровням приоритета. Трафик, попадающий в очередь с большим номером, проходит через коммутатор быстрее, тогда как трафик в очередях с меньшим номером может быть отброшен при перегрузке в сети.</p>	
<p>Уровень приоритета (следующие описания относятся к типам трафика, описанным в стандарте IEEE 802.1d (в него входит стандарт 802.1p)).</p>	
Level 7	Обычно используется для трафика сетевого управления, например, сообщений настройки маршрутизаторов.
Level 6	Обычно используется для голосового трафика, который особенно чувствителен к джиттеру (джиттер – колебания времени задержки).
Level 5	Обычно используется для видеотрафика, которому требуется высокая пропускная способность и который также чувствителен к джиттеру.
Level 4	Обычно используется для трафика с контролируемой нагрузкой и высокой чувствительностью к задержкам, например, транзакций SNA.
Level 3	Обычно используется для трафика, доставляемого по принципу «максимума усилий», то есть более высокого класса, чем доставляемого по принципу «наибольших усилий». Сюда может входить важный бизнес-трафик, для которого допустимы небольшие задержки.
Level 2	Для трафика, доставляемого при наличии «лишней пропускной способности».
Level 1	Обычно используется для некритического, «фонового» трафика, например, для передачи больших объемов данных, которые разрешены, но не должны мешать другим приложениям и пользователям.
Level 0	Обычно используется для трафика, доставляемого по принципу «наибольших усилий».
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

7.6 Настройки протокола IP

Экран **IP Setup** используется для настройки шлюза по умолчанию, сервера DNS по умолчанию и добавления IP-доменов.

7.6.1 IP-интерфейсы

Для управления через сеть коммутатору должен быть назначен IP-адрес. По умолчанию используется IP-адрес 192.168.1.1. Маска подсети определяет, какую часть в IP-адресе занимает номер сети. По умолчанию используется маска 255.255.255.0.

Имеется возможность настроить IP-адреса для получения доступа и управления коммутатором с портов, принадлежащих определенным сетям VLAN.



Предварительно необходимо настроить сеть VLAN.

Рисунок 32 Экран Basic Setting > IP Setup

The screenshot shows the 'IP Setup' configuration interface. It includes the following elements:

- Domain Name Server:** 0.0.0.0
- Default Management:** In-band, Out-of-band
- In-band Management IP Address:**
 - DHCP Client
 - Static IP Address
 - IP Address: 192.168.1.1
 - IP Subnet Mask: 255.255.255.0
 - Default Gateway: 0.0.0.0
 - VID: 1
- Out-of-band Management IP Address:**
 - DHCP Client
 - Static IP Address
 - IP Address: 192.168.0.1
 - IP Subnet Mask: 255.255.255.0
 - Default Gateway: 0.0.0.0
- Buttons:** Apply, Cancel
- In band IP Addresses Table:**

Index	IP Address	IP Subnet Mask	VID	Default Gateway	Manageable	Delete
	0.0.0.0	0.0.0.0		0.0.0.0	<input type="checkbox"/>	
- Buttons:** Add, Cancel, Delete, Cancel

Поля экрана описаны в следующей таблице.

Таблица 12 Экран Basic Setting > IP Setup

ПОЛЕ	ОПИСАНИЕ
Domain Name Server	Сервер DNS (системы доменных имен) определяет соответствие между доменным именем и IP-адресом, и наоборот. Введите IP-адрес сервера DNS, чтобы вместо IP-адресов можно было использовать доменные имена.
Default Management	Укажите, по какому из путей (внутриполосному In-Band или внеполосному Out-of-band) данный коммутатор должен отправлять собственные пакеты (такие как «ловушки» SNMP), а также пакеты от неизвестных источников. В случае выбора Out-of-band данный коммутатор будет отправлять пакеты на внеполосный порт управления. При этом устройства, подключенные к другим портам, данных пакетов не получат. В случае выбора In-Band данный коммутатор будет отправлять пакеты на все порты, за исключением внеполосного порта управления; подключенные к последнему устройства данных пакетов не получат.
In-band Management IP Address	
DHCP Client	Выберите данную опцию, если коммутатор должен автоматически получать IP-адрес, маску подсети, IP-адрес шлюза по умолчанию и IP-адрес сервера DNS через сервер DHCP.
Static IP Address	Выберите данную опцию, если сервер DHCP не используется или коммутатору необходимо присвоить статический IP-адрес. В этом случае потребуется заполнить следующие поля.
IP Address	Введите IP-адрес коммутатора в виде десятичных чисел, разделенных точками, например 192.168.1.1.
IP Subnet Mask	Введите IP-маску подсети коммутатора в виде десятичных чисел, разделенных точками, например 255.255.255.0.
Default Gateway	Введите IP-адрес исходящего шлюза по умолчанию в виде десятичных чисел, разделенных точками, например 192.168.1.254.
VID	Введите идентификационный номер сети VLAN, связанной с IP-адресом коммутатора. Этот идентификатор VLAN ID соответствует CPU и используется только для управления. По умолчанию используется значение «1». По умолчанию все порты являются членами данной «VLAN управления», благодаря чему устройством можно управлять через любой порт. Если порт не входит в состав данной VLAN, то пользователи на этом порту не смогут получить доступа к устройству. Чтобы получить доступ к коммутатору, к нему необходимо подключиться через порт, являющийся членом VLAN управления.
Out-of-band Management IP Address	
IP Address	Введите IP-адрес коммутатора в виде десятичных чисел, разделенных точками, например 192.168.0.1. В случае изменения данного IP-адреса перед попыткой доступа к коммутатору убедитесь, что подключенный к данному порту управления компьютер находится в той же подсети.
IP Subnet Mask	Введите IP-маску подсети коммутатора в виде десятичных чисел, разделенных точками, например 255.255.255.0.
Default Gateway	Введите IP-адрес исходящего шлюза по умолчанию в виде десятичных чисел, разделенных точками, например 192.168.0.254.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоа в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы сбросить все поля.

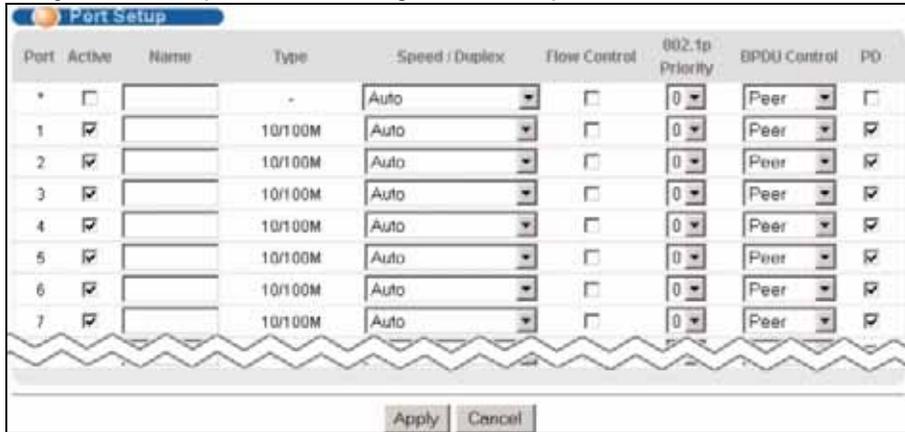
Таблица 12 Экран Basic Setting > IP Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
In-band IP Addresses	Имеется возможность создать IP-адреса для получения доступа и управления коммутатором с портов, принадлежащих определенным сетям VLAN. Предварительно необходимо настроить сети VLAN.
IP Address	Введите IP-адрес для управления коммутатором членами VLAN, указанной в поле VID ниже.
IP Subnet Mask	Введите маску подсети в виде десятичных чисел, разделенных точками.
VID	Введите идентификационный номер группы VLAN.
Default Gateway	Введите IP-адрес шлюза по умолчанию в виде десятичных чисел, разделенных точками.
Manageable	Установите этот переключатель, чтобы разрешить управление коммутатором с использованием указанного IP-адреса.
Add	Нажмите Add , чтобы сохранить новую запись в оперативной памяти коммутатора. После этого она появится в итоговой таблице внизу экрана.
Cancel	Нажмите Cancel , чтобы сбросить все поля.
Index	В этом поле отображается порядковый номер записи. Нажмите на этот номер, чтобы отредактировать правило.
IP Address	В этом поле отображается IP-адрес.
IP Subnet Mask	В этом поле отображается маска подсети.
VID	В этом поле отображается идентификационный номер VLAN.
Default Gateway	В этом поле отображается IP-адрес исходящего шлюза по умолчанию.
Manageable	В этом поле отображается, возможно ли управление коммутатором с использованием указанного IP-адреса.
Delete	Нажмите Delete , чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

7.7 Настройки портов

Настройки портов коммутатора осуществляются на этом экране. Чтобы открыть экран настроек, выберите в навигационной панели **Basic Setting > Port Setup**.

Рисунок 33 Экран Basic Setting > Port Setup



Поля экрана описаны в следующей таблице.

Таблица 13 Экран Basic Setting > Port Setup

ПОЛЕ	ОПИСАНИЕ
Port	Порядковый номер порта.
*	<p>Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Active	Установите этот переключатель, чтобы включить порт. По умолчанию все порты включены. Передача данных происходит только через включенные порты.
Name	<p>Введите имя-описание для идентификации порта. В поле можно ввести до 64 алфавитно-цифровых символов.</p> <p>Примечание: Из-за ограниченного места на некоторых экранах Web-конфигуратора имя порта может отображаться не полностью.</p>
Type	В этом поле используется обозначение 10/100M для подключений Ethernet/Fast Ethernet и 10/100/1000M – для подключений Gigabit Ethernet.

Таблица 13 Экран Basic Setting > Port Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Speed/Duplex	<p>Выберите скорость и режим дуплекса для Ethernet-соединения на этом порту. Возможны значения Auto (автосогласование), 10M/Half Duplex (10 Мбит/с, полудуплекс), 10M/Full Duplex (10 Мбит/с, дуплекс), 100M/Half Duplex (100 Мбит/с, полудуплекс), 100M/Full Duplex (100 Мбит/с, дуплекс) и 1000M/Full Duplex (1000 Мбит/с, дуплекс) (только для портов Gigabit Ethernet).</p> <p>Примечание: Для портов Fast Ethernet на модуле SFP тип соединения имеет фиксированное значение 100M/Full Duplex (100 Мбит/с, дуплекс).</p> <p>Значение Auto (автосогласование) позволяет порту автоматически согласовать с подключенным портом и выбрать скорость соединения и режим дуплекса, которые поддерживают оба порта. Когда автосогласование включено, порт коммутатора автоматически обменивается данными с портом на другой стороне и сам выбирает скорость соединения и режим дуплекса. Если порт на другой стороне не поддерживает автосогласование, или на нем эта функция отключена, коммутатор определяет скорость по сигналу в кабеле и выставляет полудуплексный режим. Когда функция автосогласования отключена, при подключении порт использует заранее определенную скорость и режим дуплекса. Таким образом, чтобы соединение произошло, у порта на другой стороне должны быть точно такие же параметры, что и у порта коммутатора.</p>
Flow Control	<p>Концентрация трафика на порту вызывает падение пропускной способности и перегружает буферную память, из-за чего происходит отбрасывание пакетов и потеря кадров. Функция управления потоком (Flow Control) используется для регулирования передачи сигналов в зависимости от пропускной способности принимающего порта.</p> <p>Данный коммутатор использует управление потоком по стандарту IEEE 802.3x в дуплексном режиме и управление потоком методом обратного давления (противодавления) в полудуплексном режиме.</p> <p>Управление потоком по стандарту IEEE 802.3x в дуплексном режиме подразумевает отправку сигнала паузы на передающий порт, что позволяет приостановить передачу при переполнении буфера принимающего порта.</p> <p>Управление потоком методом обратного давления обычно применяется в полудуплексном режиме и предполагает отправку на передающий порт сигнала коллизии (имитацию состояния коллизии), из-за чего передающий порт на некоторое время приостанавливает передачу. Чтобы включить эту функцию, установите переключатель Flow Control.</p>
802.1p Priority	<p>Это значение приоритета добавляется к входящим кадрам, не имеющим тега приоритета очередности (802.1p). Дополнительную информацию можно найти в описании поля Priority Queue Assignment в табл. 11 на стр. 83.</p>
BPDU Control	<p>Выберите способ обработки блоков данных мостового протокола BPDU, получаемых через данный порт. Предварительно необходимо включить режим прозрачности мостовых протоколов (Bridging Control Protocol Transparency) на экране Switch Setup.</p> <p>В случае выбора Peer все принимаемые через данный порт блоки данных мостового протокола BPDU будут обрабатываться.</p> <p>В случае выбора Tunnel все принимаемые через данный порт блоки BPDU будут ретранслироваться.</p> <p>В случае выбора Discard все принимаемые через данный порт блоки BPDU будут отбрасываться.</p> <p>В случае выбора Network блоки BPDU, не имеющие тега VLAN, будут обрабатываться, а блоки BPDU с тегами – ретранслироваться.</p>

Таблица 13 Экран Basic Setting > Port Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
PD	<p>Данное поле предусмотрено только в моделях PWR, причем для гигабитных портов и портов mini-GBIC оно недоступно.</p> <p>Питаемым устройством (powered device, PD) называется устройство (например, точка доступа или коммутатор), поддерживающее стандарт питания по витой паре PoE, благодаря чему оно может получать питание от другого устройства через порт Ethernet на 10/100 Мбит/с.</p> <p>Установите переключатель для тех портов, через которые необходимо разрешить питание коммутатором подключенных устройств.</p>
Apply	<p>Нажмите Apply, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.</p>
Cancel	<p>Нажмите Cancel, чтобы начать настройку на этом экране заново.</p>

Виртуальные локальные сети (VLAN)

Тип отображаемого экрана зависит от того, какой тип VLAN (параметр **VLAN Type**) был выбран на экране настроек коммутатора (**Switch Setup**). В данной главе рассматривается конфигурирование виртуальных локальных сетей на основе тегов (стандарт 802.1Q) и виртуальных локальных сетей на основе портов.

8.1 Введение в виртуальные локальные сети на основе тегов (согласно IEEE 802.1Q)

В виртуальных локальных сетях на основе тегов для определения принадлежности кадра к определенной VLAN на мостах используется явный тег (идентификатор VLAN) в MAC-заголовке – такие теги не привязаны к коммутатору, на котором были созданы. Виртуальные локальные сети могут создаваться статически (вручную) или динамически с помощью протокола динамической регистрации VLAN по GARP (GVRP). Идентификатор VLAN ассоциирует кадр с конкретной сетью VLAN и предоставляет информацию, которая необходима коммутаторам для обработки кадра при его прохождении по сети. Кадр с тегом на четыре байта больше кадра без тега и включает в себя два байта TPID (идентификатор протокола тега, он находится в поле типа/длины Ethernet-кадра) и два байта TCI (контрольная информация тега, начинается после поля адреса источника в Ethernet-кадре).

Однобитный флаг CFI (индикатор канонического формата) для Ethernet-коммутаторов всегда устанавливается равным нулю. Если у кадра, полученного через Ethernet-порт, флаг CFI равен 1, то этот кадр нельзя передать «как есть» на порт без тега. Оставшиеся 12 бит определяют идентификатор VLAN, поэтому максимально возможное количество сетей VLAN составляет 4 096. Следует иметь в виду, что уровень приоритета пользователя и идентификатор VLAN не зависят друг от друга. Кадр с идентификатором VLAN (VID), равным нулю (0), называется кадром приоритета. В таком кадре значение имеет только уровень приоритета, а в качестве идентификатора VID кадру назначается идентификатор VID по умолчанию входящего порта. Из 4096 возможных идентификаторов VLAN значение VID, равное нулю, используется для идентификации кадров приоритета, а значение 4095 (FFF) зарезервировано, поэтому максимальное количество конфигураций VLAN составляет 4094.

TPID 2 байта	Приоритет пользователя 3 бита	CFI 1 бит	VLAN ID 12 бит
-----------------	----------------------------------	--------------	-------------------

8.1.1 Пересылка кадров с тегами и без тегов

Через каждый порт коммутатора могут проходить как кадры с тегами, так и кадры без тегов. Чтобы переслать кадр с коммутатора с поддержкой VLAN на основе 802.1Q на коммутатор без поддержки таких VLAN, коммутатор сначала определяет, куда требуется переслать этот кадр, а потом удаляет тег VLAN. Чтобы переслать кадр с коммутатора без поддержки VLAN на основе 802.1Q на коммутатор, поддерживающий такие VLAN, коммутатор сначала определяет, куда требуется переслать этот кадр, а потом вставляет тег VLAN, содержащий идентификатор VLAN по умолчанию входящего порта. В качестве PVID по умолчанию используется VLAN 1 для всех портов, но эту установку можно изменить.

Широковещательные кадры (а также кадры мультивещания для известной системе группы мультивещания) дублируются только на те порты, которые входят в группу VID (за исключением самого входящего порта), ограничивая таким образом широковещание конкретным доменом.

8.2 Автоматическая регистрация VLAN

Для автоматической регистрации членов VLAN коммутаторами используются протоколы GARP и GVRP.

8.2.1 Протокол GARP

Протокол GARP (протокол регистрации по общим атрибутам) позволяет коммутаторам в сети регистрировать и снимать регистрацию значений атрибутов на других устройствах с поддержкой GARP внутри локальных сетей на основе мостов. GARP – это протокол, предоставляющий общий механизм работы для протоколов, которые имеют более конкретное применение, таких как протокол GVRP.

8.2.1.1 Таймеры GARP

Коммутаторы присоединяются к виртуальным локальным сетям VLAN путем передачи декларации. Декларация представляет собой передачу сообщения Join с использованием протокола GARP. Декларации отменяются путем передачи сообщения Leave. Сообщение Leave All отменяет все декларации. Таймеры GARP определяют значения тайм-аута для декларации.

8.2.2 Протокол GVRP

GVRP (GARP VLAN Registration Protocol, протокол регистрации VLAN по GARP) является протоколом регистрации, который определяет способ регистрации коммутаторами необходимых членов VLAN на портах в сети. Включение этой функции разрешает создание групп VLAN за пределами локального коммутатора.

Общая терминология сетей VLAN на основе IEEE 802.1Q описана в следующей таблице.

Таблица 14 Терминология сетей VLAN на основе IEEE 802.1Q

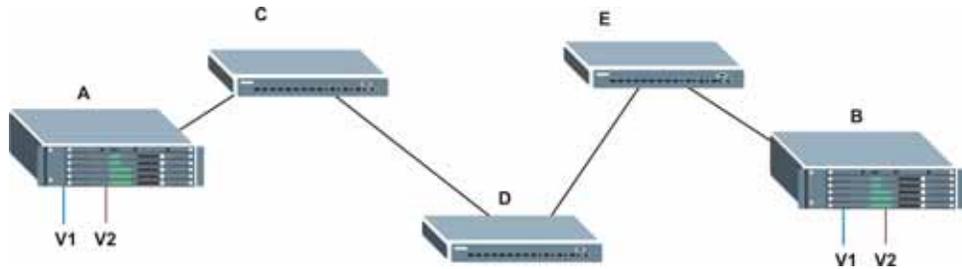
ПАРАМЕТРЫ VLAN	ТЕРМИН	ОПИСАНИЕ
Тип VLAN	Постоянная VLAN	Статическая виртуальная локальная сеть VLAN, созданная вручную.
	Динамическая VLAN	Сеть VLAN, настроенная в процессе регистрации/дерегистрации протоколом GVRP.
Административный контроль над VLAN	Фиксированная регистрация	Порты с фиксированной регистрацией являются постоянными членами VLAN.
	Регистрация запрещена	Портам с запрещенной регистрацией запрещено присоединяться к указанной VLAN.
	Нормальная регистрация	Порты динамически присоединяются к VLAN с использованием протокола GVRP.
Управление тегами VLAN	С тегами	Порты, принадлежащие к данной VLAN, добавляют теги ко всем передаваемым исходящим кадрам.
	Без тегов	Порты, принадлежащие к данной VLAN, не добавляют теги ко всем передаваемым исходящим кадрам.
Порт VLAN	Идентификатор VLAN порта	Идентификатор VLAN, назначаемый получаемым через этот порт кадрам без тегов.
	Допустимый тип кадра	Можно выбрать один из режимов – принимать ли на порт входящие кадры как с тегами, так и без тегов, принимать только кадры с тегами или только кадры без тегов.
	Фильтрация входящих кадров	Если этот параметр включен, коммутатор отбрасывает входящие кадры для VLAN, членом которых не является данный порт.

8.3 Магистральные порты VLAN

Включение параметра **VLAN Trunking** для порта позволяет разрешить прохождение через этот порт кадров, принадлежащих неизвестным группам VLAN. Это полезно, если требуется настроить группы VLAN на конечных устройствах без необходимости настраивать те же группы на промежуточных устройствах.

См. следующий рисунок. Предположим, что требуется создать группы VLAN 1 и 2 (V1 и V2) на устройствах А и В. Без функции магистральных соединений VLAN (**VLAN Trunking**) необходимо будет настроить группы VLAN 1 и 2 на всех промежуточных коммутаторах С, D и E; в противном случае они будут отбрасывать кадры с тегами неизвестных групп VLAN. Однако, если на порту(портах) каждого промежуточного коммутатора будет включен параметр **VLAN Trunking**, то группы VLAN нужно будет создать только на конечных устройствах (А и В). Устройства С, D и E автоматически позволят кадрам с тегами групп VLAN 1 и 2 (то есть групп VLAN, о которых этим устройствам не известно) проходить через свои магистральные порты VLAN.

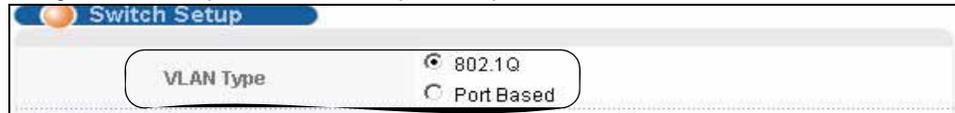
Рисунок 34 Магистральные порты VLAN



8.4 Выбор типа VLAN

Тип VLAN выбирается на экране **Basic Setting > Switch Setup**.

Рисунок 35 Экран Switch Setup: выбор типа VLAN



8.5 Статические VLAN

Статические виртуальные локальные сети используются, если входящий через порт кадр должен быть

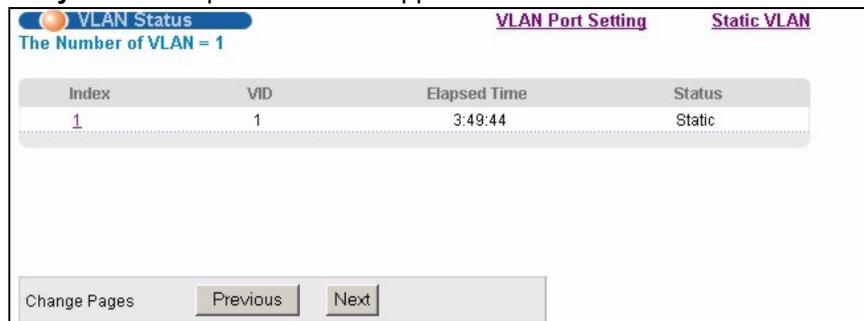
- отправлен в группу VLAN обычным образом, в зависимости от его тега VLAN.
- отправлен в группу независимо от того, имеется у него тег VLAN или нет.
- заблокирован от направления в группу VLAN независимо от его тега VLAN.

Кроме того, имеется возможность добавлять ко всем исходящим кадрам (ранее не имевшим тегов), отправляемым через порт, указанный идентификатор VLAN.

8.5.1 Состояние статической VLAN

Дополнительную информацию о статических VLAN можно найти в [разд. 8.1 на стр. 91](#). Чтобы отобразить показанный ниже экран **VLAN Status**, выберите в навигационной панели **Advanced Application > VLAN**.

Рисунок 36 Экран Advanced Application > VLAN: VLAN Status



Поля экрана описаны в следующей таблице.

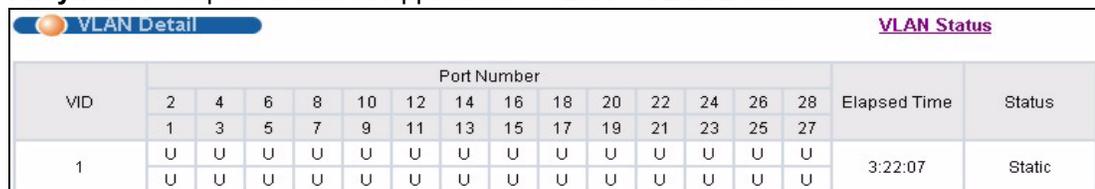
Таблица 15 Экран Advanced Application > VLAN: VLAN Status

ПОЛЕ	ОПИСАНИЕ
The Number of VLAN	Количество виртуальных локальных сетей (VLAN), настроенных на коммутаторе.
Index	Порядковый номер VLAN. Нажатие на порядковом номере позволяет отобразить более подробную информацию о сети VLAN.
VID	Идентификационный номер VLAN, определенный ранее на экране Static VLAN .
Elapsed Time	В этом поле отображается время, в течение которого была зарегистрирована обычная VLAN или настроена статическая VLAN.
Status	В этом поле указано, каким образом VLAN была настроена на коммутаторе; Dynamic – с использованием протокола GVRP, Static – добавлена в качестве постоянной записи или Other – добавлена другим способом, например, с использованием механизма регистрации VLAN-сети мультивещания (MVR).
Change Pages	Нажмите Previous или Next , чтобы отобразить предыдущий/следующий экран, если информация о состоянии не помещается на одном экране.

8.5.2 Подробная информация о статической VLAN

На этом экране отображаются подробные настройки портов и информация о состоянии группы VLAN. Дополнительную информацию о статических VLAN можно найти в [разд. 8.1 на стр. 91](#). Чтобы отобразить экран подробной информации о сети VLAN, нажмите на порядковом номере сети на экране **VLAN Status**.

Рисунок 37 Экран Advanced Application > VLAN > VLAN Detail



VLAN Detail		Port Number														Elapsed Time		Status
VID		2	4	6	8	10	12	14	16	18	20	22	24	26	28			
1		U	U	U	U	U	U	U	U	U	U	U	U	U	U	3:22:07	Static	

Поля экрана описаны в следующей таблице.

Таблица 16 Экран Advanced Application > VLAN > VLAN Detail

ПОЛЕ	ОПИСАНИЕ
VLAN Status	Нажатие на этой ссылке позволяет перейти к экрану VLAN Status .
VID	Идентификационный номер VLAN, определенный ранее на экране Static VLAN .
Port Number	В этом столбце отображаются порты, участвующие в VLAN. Порт с тегом обозначается буквой T , порт без тега – буквой U , а порты, не являющиеся членами VLAN – знаком «–».
Elapsed Time	В этом поле отображается время, в течение которого была зарегистрирована обычная VLAN или настроена статическая VLAN.
Status	В этом поле указано, каким образом VLAN была настроена на коммутаторе; Dynamic – с использованием протокола GVRP, Static – добавлена в качестве постоянной записи или Other – добавлена другим способом, например, с использованием механизма регистрации VLAN-сети мультивещания (MVR).

8.5.3 Настройка статической VLAN

На этом экране можно настроить и просмотреть параметры сети VLAN на основе 802.1Q коммутатора. Дополнительную информацию о статических VLAN можно найти в [разд. 8.1 на стр. 91](#). Для настройки статической VLAN нажмите **Static VLAN** на экране **VLAN Status**. Откроется экран меню, показанный ниже.

Рисунок 38 Экран Advanced Application > VLAN > Static VLAN

The screenshot shows the 'Static VLAN' configuration interface. At the top, there is a title bar with 'Static VLAN' and a 'VLAN Status' link. Below the title bar, there is an 'ACTIVE' checkbox. Underneath, there are input fields for 'Name' and 'VLAN Group ID'. The main part of the screen is a table with three columns: 'Port', 'Control', and 'Tagging'. The 'Port' column has a '*' row and rows for ports 1 through 8. The 'Control' column has a dropdown menu set to 'Normal' and radio buttons for 'Normal', 'Fixed', and 'Forbidden'. The 'Tagging' column has a checked 'Tx Tagging' checkbox. Below the table, there are 'Add', 'Cancel', and 'Clear' buttons. At the bottom, there is a summary table with columns 'VID', 'Active', 'Name', and 'Delete', and 'Delete' and 'Cancel' buttons.

Поля экрана описаны в следующей таблице.

Таблица 17 Экран Advanced Application > VLAN > Static VLAN

ПОЛЕ	ОПИСАНИЕ
ACTIVE	Установите этот переключатель, чтобы включить настройки VLAN.
Name	Введите имя-описание VLAN, с помощью которого ее можно идентифицировать. Максимальная длина имени – 64 печатных символа; пробелы допускаются.
VLAN Group ID	Введите идентификатор VLAN для данной статической записи; допустимое значение находится в диапазоне от 1 до 4094.
Port	Номер порта – определяет настраиваемый порт.
*	<p>Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>

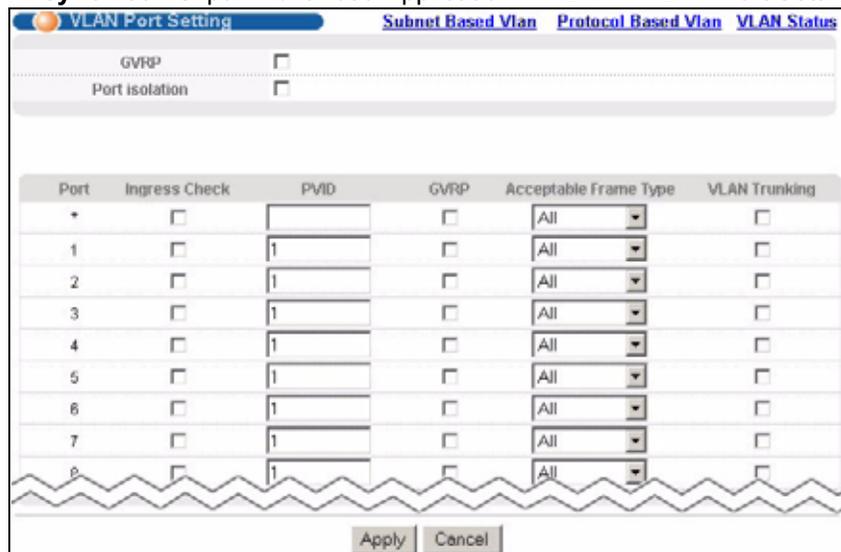
Таблица 17 Экран Advanced Application > VLAN > Static VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Control	Выберите Normal , если порт должен присоединяться к данной группе VLAN динамически с использованием протокола GVRP. Данный параметр выбран по умолчанию. Выберите Fixed , если порт должен стать постоянным членом данной группы VLAN. Выберите Forbidden , чтобы запретить порту присоединяться к группе VLAN.
Tagging	Установите переключатель TX Tagging , чтобы порт добавлял теги ко всем исходящим кадрам, отправляемым с идентификатором этой группы VLAN.
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clear	Нажмите Clear , чтобы начать настройку на этом экране заново.
VID	В этом поле отображается идентификационный номер группы VLAN. Нажмите на этот номер, чтобы редактировать настройки VLAN.
Active	В этом поле отображается текущее состояние настроек VLAN – включены (Yes) или отключены (No).
Name	В этом поле отображается имя-описание группы VLAN.
Delete	Нажмите Delete , чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

8.5.4 Настройка порта VLAN

Для настройки параметров статической VLAN (на основе IEEE 802.1Q) для порта используется экран VLAN Port Setting. Дополнительную информацию о статических VLAN можно найти в [разд. 8.1 на стр. 91](#). Нажмите на ссылке **VLAN Port Setting** на экране **VLAN Status**.

Рисунок 39 Экран Advanced Application > VLAN > VLAN Port Setting



Поля экрана описаны в следующей таблице.

Таблица 18 Экран Advanced Application > VLAN > VLAN Port Setting

ПОЛЕ	ОПИСАНИЕ
GVRP	GVRP (GARP VLAN Registration Protocol, протокол регистрации VLAN по GARP) является протоколом регистрации, который определяет способ регистрации коммутаторами необходимых членов VLAN на портах в сети. Включение этой функции разрешает создание групп VLAN за пределами локального коммутатора.
Port Isolation	С помощью параметра изоляции портов Port Isolation можно запретить каждому из портов обмениваться данными друг с другом – обмен будет разрешен только с портом управления CPU и гигабитными портами каскадирования. Этот вариант является самым ограничивающим, но в то же время и самым безопасным.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Ingress Check	Если данный переключатель для порта установлен, коммутатор отбрасывает входящие кадры для VLAN, членом которых не является данный порт. Снимите выделение с переключателя, если требуется отключить фильтрацию входящих кадров.
PVID	Введите номер от 1 до 4094 в качестве идентификатора VLAN для порта.
GVRP	Установите этот переключатель, чтобы включить на этом порту протокол GVRP.
Acceptable Frame Type	Укажите тип кадров, разрешенных для данного порта. Можно выбрать значения All , Tag Only и Untag Only . Выбор All в ниспадающем списке разрешает прием через этот порт как кадров с тегами, так и кадров без тегов. Это значение выбрано по умолчанию. Выбор Tag Only разрешает прием через этот порт только кадров с тегами. Все кадры без тегов будут отброшены. Выбор Untag Only разрешает прием через этот порт только кадров без тегов. Все кадры с тегами будут отброшены.
VLAN Trunking	Установите переключатель VLAN Trunking для портов, подключенных к другим коммутаторам или маршрутизаторам (но не для портов, напрямую подключенных к конечным пользователям), чтобы разрешить прохождение через коммутатор кадров, принадлежащих к неизвестным группам VLAN.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

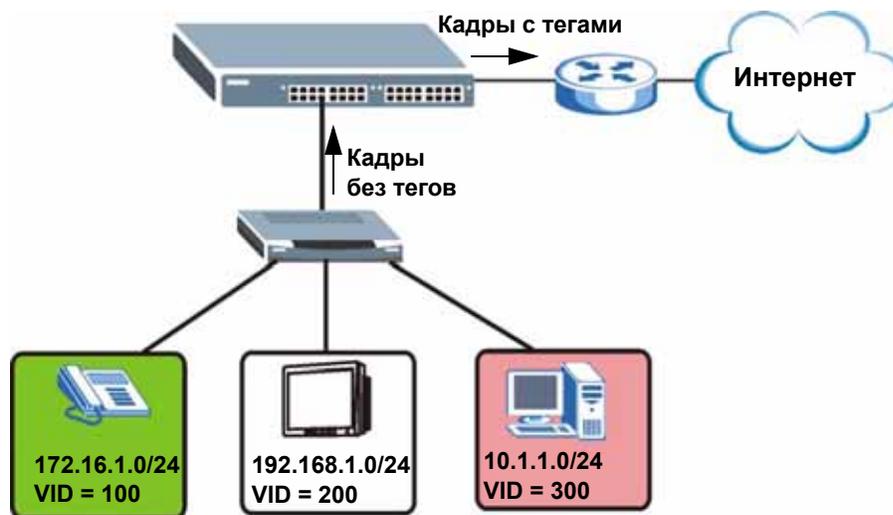
8.6 VLAN на основе подсетей

VLAN на основе подсетей позволяют сгруппировать трафик по логическим сетям VLAN на основе указанных IP-подсетей источников пакетов. При поступлении кадра через порт коммутатор проверяет, не был ли добавлен к нему тег и из какой IP-подсети он поступил. Пакеты без тегов от одной и той же IP-подсети помещаются в одну VLAN на основе подсетей. Одно из преимуществ VLAN на основе подсетей заключается в возможности назначения приоритетов для трафика из конкретных IP-подсетей.

Например, провайдер услуг Интернета (ISP) может распределить различные типы предоставляемых клиентам услуг по различным IP-подсетям. Трафик услуг голосовой связи будет назначен IP-подсети 172.16.1.0/24, видео – подсети 192.168.1.0/24, а передачи данных – подсети 10.1.1.0/24. После этого на коммутаторе можно настроить группировку входящего трафика в зависимости от IP-подсети, из которой поступают входящие кадры.

Например, для трафика из IP-подсети 172.16.1.0/24 (услуги голосовой связи) может быть настроена VLAN на основе подсетей с приоритетом 6 и идентификатором VID, равным 100. Для трафика из IP-подсети 192.168.1.0/24 (услуги передачи видео) может быть настроена VLAN на основе подсетей с приоритетом 5 и идентификатором VID, равным 200. Наконец, для трафика из IP-подсети 10.1.1.0/24 (услуги передачи данных) может быть настроена VLAN на основе подсетей с приоритетом 3 и идентификатором VID, равным 300. Все не имеющие тегов входящие кадры будут классифицироваться на основе IP-подсети источника, с назначением соответствующего приоритета. Таким образом, трафик видео получит наивысший приоритет, а трафик передачи данных – самый низкий.

Рисунок 40 Пример использования VLAN на основе подсетей



8.7 Настройка VLAN на основе подсетей

Чтобы отобразить показанный ниже экран настроек, выберите **Subnet Based VLAN** на экране **VLAN Port Setting**.



VLAN на основе подсетей применяются только к не имеющим тегов пакетам и работают лишь при использовании VLAN на основе тегов IEEE 802.1Q.

Рисунок 41 Экран Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN

Поля экрана описаны в следующей таблице.

Таблица 19 Экран Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на коммутаторе VLAN на основе подсетей.
DHCP-Vlan Override	При включении функции отслеживания DHCP клиенты DHCP могут обновлять свои IP-адреса через DHCP VLAN или через другой сервер DHCP во VLAN на основе подсетей. Установите данный переключатель, чтобы клиенты DHCP в данной IP-подсети принудительно получали IP-адреса через DHCP VLAN.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.

Таблица 19 Экран Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Active	Установите данный переключатель, чтобы включить создаваемую или изменяемую VLAN на основе подсети.
Name	Введите до 32 алфавитно-цифровых символов для обозначения данной VLAN на основе подсети.
IP	Введите IP-адрес подсети, для которой необходимо настроить VLAN.
Mask-Bits	Введите количество битов в маске подсети. Чтобы определить количество битов, переведите маску подсети в двоичную форму и подсчитайте число единичных битов. Возьмем, к примеру, маску «255.255.255.0». 255 в двоичной форме – это восемь единиц. Всего в маске 3 байта со значением «255», поэтому количество единичных битов будет три на восемь (24).
Source Port	Введите порт, к которому привязана данная VLAN на основе подсети.
VID	Введите идентификатор сети VLAN, к которой привязываются при помощи тегов все не имеющие тегов кадры из IP-подсети для данной VLAN на основе подсети. Данная VLAN должна быть предварительно определена на экранах Advanced Applications, VLAN .
Priority	Выберите уровень приоритета, назначаемый коммутатором кадрам из данной VLAN.
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Index	Порядковый номер данной VLAN на основе подсети. Нажатие на любом из этих номеров позволяет отредактировать параметры существующей VLAN на основе подсети.
Active	В данном поле указано, является ли данная VLAN на основе подсети активной.
Name	В этом поле отображается имя VLAN на основе подсети.
IP	В этом поле отображается IP-адрес подсети для данной VLAN на основе подсети.
Mask-Bits	В этом поле отображается маска подсети в виде количества единичных битов для данной VLAN на основе подсети.
Source Port	В этом поле указано, к какому порту привязана данная VLAN на основе подсети.
VID	В данном поле отображается идентификатор VLAN ID для кадров, принадлежащих к данной VLAN на основе подсети.
Priority	В данном поле отображается приоритет, назначаемый кадрам из данной VLAN на основе подсети.
Delete	Нажмите на данную кнопку, чтобы удалить выделенные для удаления VLAN на основе подсетей.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

8.8 VLAN на основе протоколов

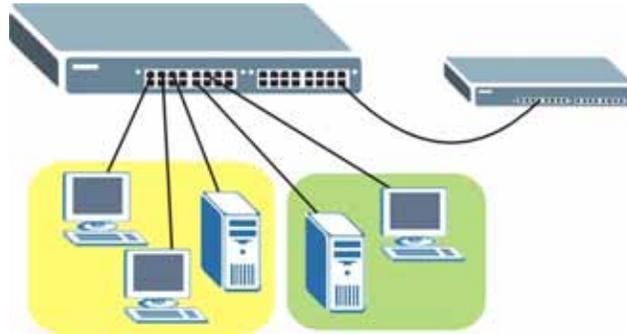
VLAN на основе протоколов позволяют сгруппировать трафик по логическим сетям VLAN на основе указанных протоколов. При поступлении от устройства более низкого уровня кадра через порт (для которого настроена VLAN на основе протокола) коммутатор проверяет, не был ли добавлен к нему тег, а также используемый кадром протокол. Пакеты без тегов с одним и тем же протоколом помещаются в одну VLAN на основе протокола. Одно из преимуществ VLAN на основе протоколов заключается в возможности назначения приоритетов для трафика с конкретным протоколом.



VLAN на основе протоколов применяются только к не имеющим тегов пакетам и работают лишь при использовании VLAN на основе тегов IEEE 802.1Q.

Например, пусть порты 1, 2, 3 и 4 принадлежат статической VLAN 100, а порты 4, 5, 6, 7 – статической VLAN 120. Пользователь настраивает VLAN на основе протоколов А с приоритетом 3 для трафика ARP, принимаемого через порты 1, 2 и 3. Также настраивается VLAN на основе протоколов В с приоритетом 2 для трафика Apple Talk, принимаемого через порты 6 и 7. В этом случае весь трафик ARP от устройств более низкого уровня, принимаемый через порты 1, 2 и 3, будет помещаться в одну группу, а весь трафик Apple Talk, поступающий через порты 6 и 7 – в другую, причем этот трафик будет иметь более высокий приоритет по сравнению с трафиком ARP при отправке на магистральный коммутатор С.

Рисунок 42 Пример использования VLAN на основе протоколов



8.9 Настройка VLAN на основе протоколов

Чтобы отобразить показанный ниже экран настроек, выберите **Protocol Based VLAN** на экране **VLAN Port Setting**.



VLAN на основе протоколов применяются только к не имеющим тегов пакетам и работают лишь при использовании VLAN на основе тегов IEEE 802.1Q.

Рисунок 43 Экран Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN

Поля экрана описаны в следующей таблице.

Таблица 20 Экран Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить данную VLAN на основе протокола.
Port	Введите порт, который должен быть включен в данную VLAN на основе протокола. Данный порт должен принадлежать статической VLAN – только в этом случае он может использоваться во VLAN на основе протокола. Дополнительную информацию о настройке VLAN можно найти в гл. 8 на стр. 91 .
Name	Введите до 32 алфавитно-цифровых символов для обозначения данной VLAN на основе протокола.
Ethernet-type	Выберите один из предустановленных протоколов из ниспадающего списка или выберите значение Others и введите номер протокола в шестнадцатеричном виде. Например, протокол IP имеет в шестнадцатеричном виде номер 0800, а протокол Novell IPX – номер 8137. Примечание: Протоколы с номерами в диапазоне от 0x0000 до 0x05ff (в шестнадцатеричном виде) использовать во VLAN на основе протоколов не допускается.

Таблица 20 Экран Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
VID	Введите идентификатор VLAN, к которой принадлежит порт. Данная VLAN должна быть предварительно определена на экранах Advanced Applications, VLAN .
Priority	Выберите уровень приоритета, назначаемый коммутатором кадрам из данной VLAN.
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Index	Порядковый номер данной VLAN на основе протокола. Нажатие на любом из этих номеров позволяет отредактировать параметры существующей VLAN на основе протокола.
Active	В данном поле указано, является ли данная VLAN на основе протокола активной.
Port	В этом поле указано, какой порт принадлежит к данной VLAN на основе протокола.
Name	В этом поле отображается имя VLAN на основе протокола.
Ethernet Type	В этом поле указано, какой из протоколов Ethernet принадлежит к данной VLAN на основе протокола.
VID	В этом поле отображается идентификатор VLAN порта.
Priority	В данном поле отображается приоритет, назначаемый кадрам из данной VLAN на основе протокола.
Delete	Нажмите на данную кнопку, чтобы удалить выделенные для удаления VLAN на основе протоколов.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

8.10 Пример создания VLAN на основе протокола IP

В данном примере показано создание VLAN на основе протокола IP, в которую включаются порты 1, 4 и 8. Для этого необходимо выполнить следующие действия:

- 1 Активировать данную VLAN на основе протокола.
- 2 Ввести номер порта, который должен быть включен в данную VLAN на основе протокола. Введите **1**.
- 3 Указать имя-описание данной VLAN на основе протокола. Введите **IP-VLAN**.
- 4 Выбрать протокол. Оставьте выбранное по умолчанию значение **IP**.
- 5 Ввести идентификатор существующей VLAN. В нашем примере используется уже созданная статическая VLAN с идентификатором 5. Введите **5**.
- 6 Оставить приоритет равным значению по умолчанию **0** и нажать **Add**.

Рисунок 44 Пример настройки VLAN на основе протокола

The screenshot shows a web-based configuration interface for 'Protocol Based VLAN'. The title bar includes 'Protocol Based VLAN' and 'Vlan Port Setting'. The configuration form has the following fields:

- Active:** A checked checkbox.
- Port:** A text input field containing the number '1'.
- Name:** A text input field containing 'IP-VLAN'.
- Ethernet-type:** A dropdown menu with 'IP' selected. Below it is an unchecked radio button labeled 'Others' followed by a text input field and '(Hex)'.
- VID:** A text input field containing '5'.
- Priority:** A dropdown menu with '0' selected.

Below the form are two buttons: 'Add' and 'Cancel'. At the bottom of the interface is a table with the following columns: Index, Active, Port, Name, Ethernet-type, VID, Priority, Delete. Below the table are two buttons: 'Delete' and 'Cancel'.

Чтобы добавить дополнительные порты в данную VLAN на основе протокола:

- 1 Нажмите на порядковый номер записи в таблице VLAN на основе протоколов. Нажмите на **1**
- 2 Измените значение в поле **Port** на номер следующего порта, который требуется добавить.
- 3 Нажмите **Add**.

8.11 Настройка VLAN на основе портов

Виртуальные локальные сети на основе портов – это такие VLAN, в которых решение о пересылке пакета принимается на основе MAC-адреса назначения и связанного с ним порта.

Для VLAN на основе портов требуется разрешение исходящей передачи для всех портов. Таким образом, чтобы позволить двум пользователям общаться друг с другом, например, между конференц-залами в отеле, необходимо разрешить исходящую передачу данных для обоих портов.

VLAN на основе портов действуют только на том коммутаторе, на котором они были созданы.



При активировании VLAN на основе портов коммутатор по умолчанию назначает ей идентификатор 1. Изменить его нельзя.



На тех экранах (например, **IP Setup** и **Filtering**), где требуется ввести идентификатор VLAN, в качестве такого идентификатора следует вводить 1.

Экран настройки VLAN на основе портов показан на следующем рисунке. В состав VLAN входит управляющий порт CPU и все Ethernet-порты.

8.11.1 Настройка VLAN на основе портов

Выберите **Port Based** в качестве типа VLAN (**VLAN Type**) на экране **Switch Setup**, затем нажмите **VLAN** в навигационной панели. Появится следующий экран.

Рисунок 45 Экран Advanced Application > VLAN: Port Based VLAN Setup (All Connected)

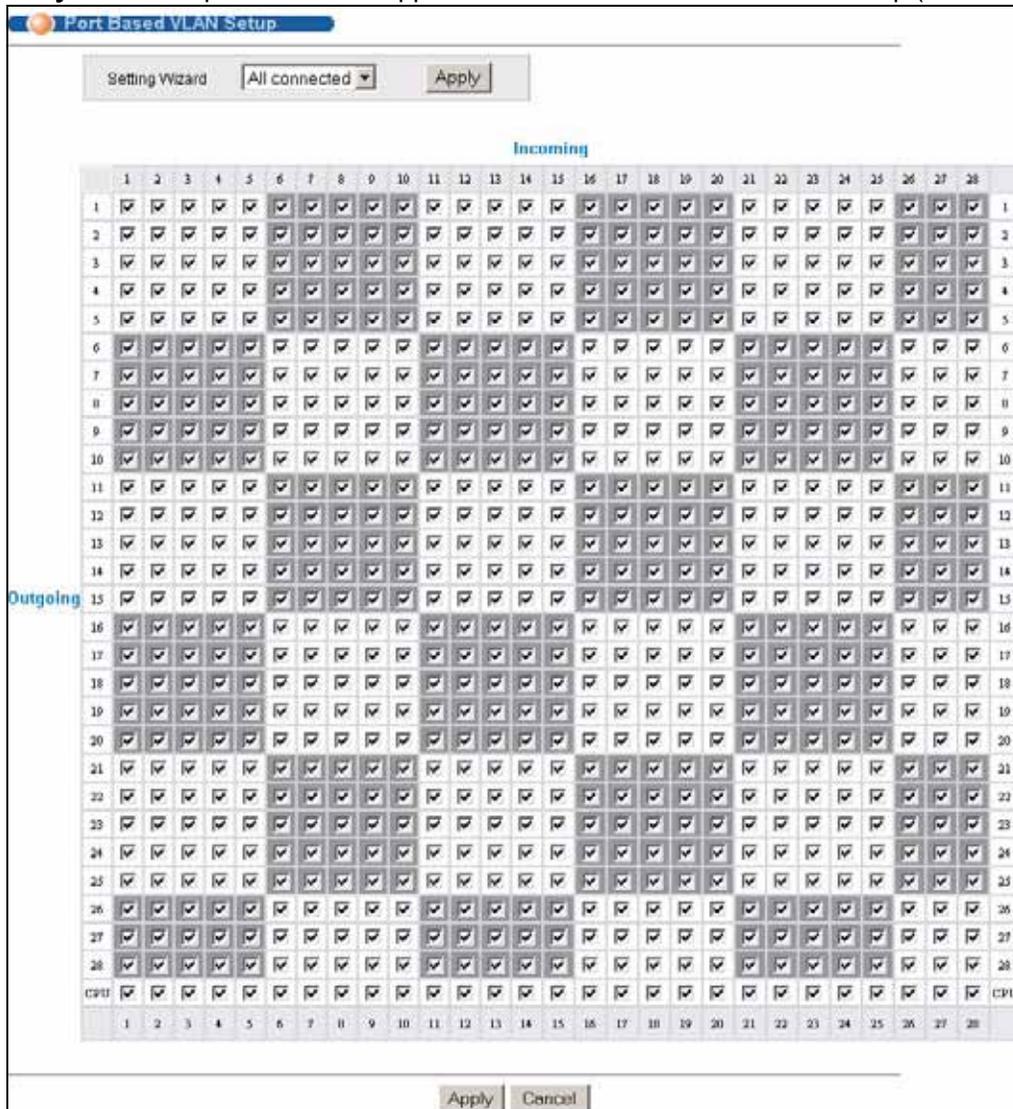
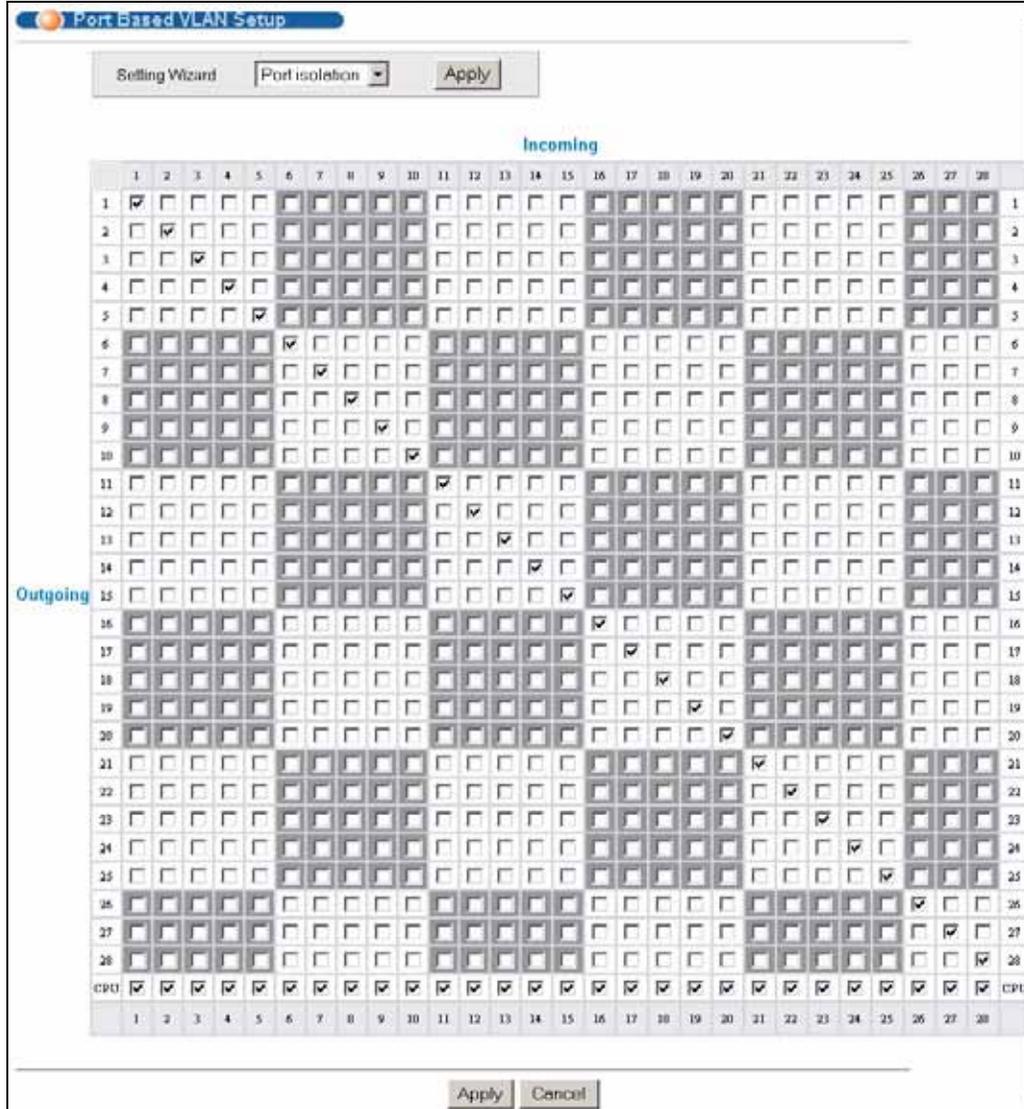


Рисунок 46 Экран Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



Поля экрана описаны в следующей таблице.

Таблица 21 Экран Advanced Application > VLAN: Port Based VLAN Setup

ПОЛЕ	ОПИСАНИЕ
Setting Wizard	<p>Выберите значение All connected или Port isolation.</p> <p>Значение All connected означает, что все порты могут обмениваться данным друг с другом, то есть виртуальных локальных сетей нет. Выбраны все входящие и исходящие порты. Этот вариант наиболее гибок, но в то же время наименее безопасен.</p> <p>Значение Port isolation означает, что каждый порт может обмениваться данными только с управляющим портом CPU, и не может с остальными портами. При этом будут выбраны все входящие порты, а из исходящих – только порт CPU. Этот вариант является самым ограничивающим, но в то же время и самым безопасным.</p> <p>Сделав выбор, нажмите кнопку Apply (она находится в правой верхней части экрана), чтобы отобразить экраны в том виде, как указано выше. Вы можете вносить изменения в эти настройки, добавляя или удаляя входящие или исходящие порты, но тогда необходимо нажимать кнопку Apply в нижней части экрана.</p>
Incoming	<p>Входящие порты; входящий порт – это тот порт, через который пакет данных попадает в коммутатор. Чтобы позволить двум абонентским портам общаться друг с другом, оба порта необходимо определить как входящие. Числа в верхнем ряду относятся к входящим портам, а соответствующие им исходящие порты перечислены слева. Порт CPU – это управляющий порт коммутатора. По умолчанию он входит в виртуальную локальную сеть со всеми Ethernet-портами. Если в состав этой VLAN не входит какой-либо из портов, то управлять коммутатором через этот порт нельзя.</p>
Outgoing	<p>Исходящие порты; исходящий порт – это тот порт, через который пакет данных покидает коммутатор. Чтобы позволить двум абонентским портам общаться друг с другом, оба порта необходимо определить как исходящие. Порт CPU – это управляющий порт коммутатора. По умолчанию он входит в виртуальную локальную сеть со всеми Ethernet-портами. Если в состав этой VLAN не входит какой-либо из портов, то управлять коммутатором через этот порт нельзя.</p>
Apply	<p>Нажмите Apply, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.</p>
Cancel	<p>Нажмите Cancel, чтобы начать настройку на этом экране заново.</p>

Настройка пересылки на основе статических MAC-адресов

Описанные ниже экраны используются для настройки пересылки на основе статических MAC-адресов.

9.1 Обзор

В данной главе рассказывается о настройке правил пересылки на основе MAC-адресов устройств в вашей сети.

9.2 Настройка пересылки на основе статических MAC-адресов

Статический MAC-адрес – это адрес, вручную внесенный в таблицу MAC-адресов. Статические MAC-адреса не имеют срока действия. При настройке правил для статических MAC-адресов для порта определяются статические MAC-адреса. Это позволяет снизить объемы широковещательного трафика.

Пересылка на основе статических MAC-адресов вместе со средствами безопасности портов позволяют разрешить доступ к коммутатору только тем компьютерам, MAC-адреса которых указаны в таблице MAC-адресов для порта. Более подробную информацию о средствах безопасности портов можно найти в [гл. 17 на стр. 157](#).

Чтобы отобразить показанный ниже экран настройки, выберите в навигационной панели **Advanced Applications > Static MAC Forwarding**.

Рисунок 47 Экран Advanced Application > Static MAC Forwarding

Поля экрана описаны в следующей таблице.

Таблица 22 Экран Advanced Application > Static MAC Forwarding

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить правило. Правило можно временно отключить, не удаляя его – снять выделение с этого переключателя.
Name	Введите имя-описание, по которому можно будет идентифицировать это правило пересылки на основе статических MAC-адресов.
MAC Address	Введите MAC-адрес в соответствующем формате, то есть шесть пар шестнадцатеричных чисел. Примечание: Статические MAC-адреса не имеют срока действия.
VID	Введите идентификационный номер VLAN.
Port	Введите номер порта, на который будет направляться трафик для MAC-адреса, введенного в предыдущем поле.
Add	Нажмите Add , чтобы сохранить правило в оперативной памяти коммутатора. Это правило будет утеряно в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clear	Нажмите Clear , чтобы начать настройку на этом экране заново.
Index	Нажмите на порядковый номер, чтобы изменить правило пересылки на основе статических MAC-адресов для данного порта.
Active	В этом поле указано, активно данное правило пересылки на основе статических MAC-адресов (Yes) или нет (No). Правило можно временно отключить, не удаляя его.
Name	Введите имя-описание, по которому можно будет идентифицировать это правило пересылки на основе статических MAC-адресов.
MAC Address	В этом поле отображается MAC-адрес, а также идентификационный номер VLAN, к которой принадлежит MAC-адрес.
VID	В этом поле отображается идентификационный номер группы VLAN.
Port	В этом поле отображается порт, на который будет направляться трафик для MAC-адреса, указанного в соседнем поле.
Delete	Нажмите Delete , чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

Фильтрация

В этой главе описана фильтрация MAC-адресов на портах.

10.1 Настройка правила фильтрации

Фильтрация позволяет отсеивать трафик, проходящий через коммутатор, на основе MAC-адреса источника и/или пункта назначения и идентификатора группы VLAN.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application > Filtering**.

Рисунок 48 Экран Advanced Application > Filtering

Поля экрана описаны в следующей таблице.

Таблица 23 Экран Advanced Application > Filtering

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить правило. Правило можно временно отключить, не удаляя его, если снять выделение с этого переключателя.
Name	Введите имя-описание (до 32 отображаемых ASCII-символов) для этого правила. Оно будет использоваться только для идентификации.

Таблица 23 Экран Advanced Application > Filtering (продолжение)

ПОЛЕ	ОПИСАНИЕ
Action	<p>Выберите Discard source, чтобы отбрасывать кадры от указанного MAC-адреса источника (указанного в поле MAC). При этом коммутатор будет по-прежнему отправлять кадры на указанный MAC-адрес.</p> <p>Выберите Discard destination, чтобы отбрасывать кадры на указанный MAC-адрес назначения (указанный в поле MAC). При этом коммутатор будет по-прежнему получать кадры от указанного MAC-адреса.</p> <p>Выберите Discard source и Discard destination, чтобы заблокировать трафик от указанного в поле MAC адреса и на этот адрес.</p>
MAC	Введите MAC-адрес в соответствующем формате, то есть шесть пар шестнадцатеричных чисел.
VID	Введите идентификационный номер группы VLAN.
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clear	Нажмите Clear , чтобы вернуться к заводским настройкам.
Index	В этом поле отображается порядковый номер правила. Нажмите на этот номер, чтобы изменить настройки.
Active	В этом поле отображается Yes , если правило активно, и No , если правило отключено.
Name	В этом поле отображается имя-описание для данного правила. Оно будет использоваться только для идентификации.
MAC Address	В этом поле отображается MAC-адрес источника/пункта назначения, а также идентификационный номер VLAN, к которой принадлежит MAC-адрес.
VID	В этом поле отображается идентификационный номер группы VLAN.
Delete	В столбце Delete установите переключатели правил, которые нужно удалить, затем нажмите кнопку Delete .
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей в столбце Delete .

Протокол покрывающего дерева

Данный коммутатор поддерживает протокол покрывающего дерева (STP), быстрый протокол покрывающего дерева (RSTP) и протокол нескольких экземпляров покрывающего дерева (MSTP), как это определено в следующих стандартах.

- IEEE 802.1d – протокол покрывающего дерева
- IEEE 802.1w – быстрый протокол покрывающего дерева
- IEEE 802.1s – протокол нескольких экземпляров покрывающего дерева

Данный коммутатор также позволяет настроить несколько конфигураций STP (несколько деревьев). После этого порты могут быть отнесены к различным деревьям.

11.1 Обзор протоколов STP/RSTP

Протокол (R)STP обнаруживает и разрывает сетевые петли и обеспечивает наличие запасных каналов между коммутаторами, мостами или маршрутизаторами. Он позволяет коммутатору взаимодействовать с другими устройствами, поддерживающими протокол (R)STP, благодаря чему достигается наличие только одного пути между любыми двумя станциями в сети.

Данный коммутатор поддерживает быстрый протокол покрывающего дерева RSTP, определенный стандартом IEEE 802.1w. Он обеспечивает более быструю сходимость покрывающего дерева по сравнению с STP (и в то же время обратно совместим с мостами, поддерживающими только протокол STP). При использовании RSTP информация об изменении топологии непосредственно распространяется по всей сети от устройства, вызвавшего изменение топологии. При использовании STP для этого требуется большее время, так как устройство, вызвавшее изменение топологии, прежде всего уведомляет об этом корневой мост, который в свою очередь распространяет изменение по сети. Как в RSTP, так и в STP осуществляется удаление ненужных полученных адресов из базы данных фильтрации. При использовании RSTP порт может находиться в состояниях Discarding, Learning и Forwarding.



В данном руководстве пользователя упоминание «STP» относится как к протоколу STP, так и к протоколу RSTP.

11.1.1 Терминология STP

Корневой мост – это основание покрывающего дерева.

Стоимость пути – это стоимость передачи кадра в локальную сеть через этот порт. Стоимость рекомендуется назначать в зависимости от скорости канала, к которому подключен порт. Чем медленнее канал, тем выше стоимость.

Таблица 24 Стоимость путей протокола STP

	СКОРОСТЬ КАНАЛА	РЕКОМЕНДУЕМОЕ ЗНАЧЕНИЕ	РЕКОМЕНДУЕМЫЙ ДИАПАЗОН	ДОПУСТИМЫЙ ДИАПАЗОН
Стоимость пути	4 Мбит/с	250	От 100 до 1000	От 1 до 65 535
Стоимость пути	10 Мбит/с	100	От 50 до 600	От 1 до 65 535
Стоимость пути	16 Мбит/с	62	От 40 до 400	От 1 до 65 535
Стоимость пути	100 Мбит/с	19	От 10 до 60	От 1 до 65 535
Стоимость пути	1 Гбит/с	4	От 3 до 10	От 1 до 65 535
Стоимость пути	10 Гбит/с	2	От 1 до 5	От 1 до 65 535

На каждом мосту корневым портом является порт, через который данный мост осуществляет связь с корнем. Таким портом на данном коммутаторе является порт с наименьшей стоимостью пути к корню. Если корневого порта нет, то данный коммутатор считается корневым мостом сети покрывающего дерева.

Для каждого сегмента локальной сети выбирается назначенный мост. Среди всех мостов, подключенных к локальной сети, этот мост имеет наименьшую стоимость пути к корню.

11.1.2 Как работает протокол STP

После того, как мост с помощью протокола STP определяет покрывающее дерево с наименьшей стоимостью пути, он активирует корневой порт и порты, назначенные для подключенных локальных сетей, а также отключает все остальные порты, принимающие участие в покрывающем дереве. Сетевые пакеты, таким образом, направляются только через подключенные порты, что исключает возможность возникновения сетевых петель.

Коммутаторы, поддерживающие протокол STP, периодически обмениваются блоками данных мостового протокола (BPDU). При изменении топологии локальной сети, соединенной мостами, создается новое покрывающее дерево.

После создания стабильной сетевой топологии все мосты ожидают блоков BPDU типа Hello от корневого моста. Если мост не получает блока данных Hello по истечении заранее определенного интервала (Max Age), то он понимает это как отсутствие канала к корневому мосту. Тогда этот мост предпринимает попытки связаться с другими мостами, чтобы перенастроить сеть и создать новую действующую сетевую топологию.

11.1.3 Состояния портов по протоколу STP

В целях устранения зацикливания пакетов протокол STP назначает порту одно из пяти состояний. Для предотвращения появления кратковременных петель не разрешается переключение порта моста из состояния блокировки непосредственно в состояние пересылки.

Таблица 25 Состояния портов по протоколу STP

СОСТОЯНИЕ ПОРТА	ОПИСАНИЕ
Disabled	Протокол STP отключен (по умолчанию).
Blocking	Принимаются и обрабатываются только пакеты BPDU настройки и управления.
Listening	Принимаются и обрабатываются все пакеты BPDU. Примечание: Состояние «Listening» не используется в RSTP.
Learning	Принимаются и обрабатываются все пакеты BPDU. Кадры информации направляются процессу получения (запоминания), но не пересылаются.
Forwarding	Принимаются и обрабатываются все пакеты BPDU. Все кадры информации принимаются и пересылаются.

11.1.4 Быстрый протокол нескольких экземпляров покрывающего дерева

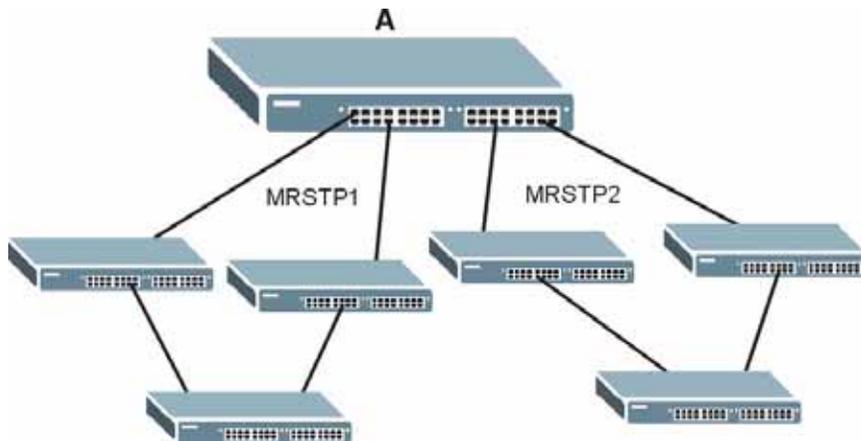
Протокол MRSTP (быстрый протокол нескольких экземпляров покрывающего дерева, Multiple RSTP) представляет собой фирменную функцию ZyXEL, совместимую с протоколами RSTP и STP. Поддержка MRSTP позволяет настроить на коммутаторе несколько экземпляров покрывающего дерева и назначать порты каждому дереву. Каждое из покрывающих деревьев работает независимо с использованием собственной информации о мостах.

В показанном ниже примере на коммутаторе А используются два экземпляра RSTP (**MRSTP 1** и **MRSTP2**).

Для настройки MRSTP необходимо включить MRSTP на коммутаторе и указать порты, принадлежащие к каждому из экземпляров покрывающего дерева.



Каждый порт может принадлежать только к одному дереву STP.

Рисунок 49 Пример сети с поддержкой MRSTP

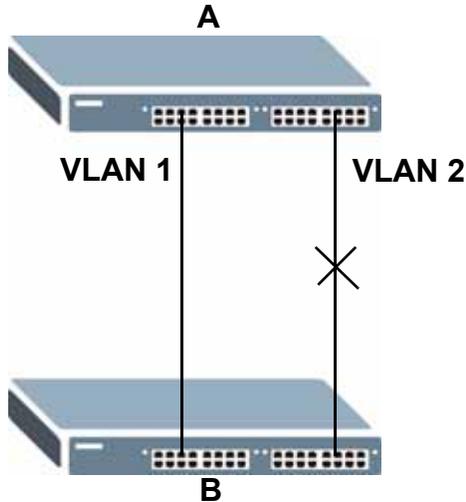
11.1.5 Протокол MSTP

Протокол нескольких экземпляров покрывающего дерева MSTP (IEEE 802.1s) обратно совместим с протоколами STP/RSTP и устраняет ограничения, характерные для существующих протоколов STP и RSTP за счет реализации следующих функций:

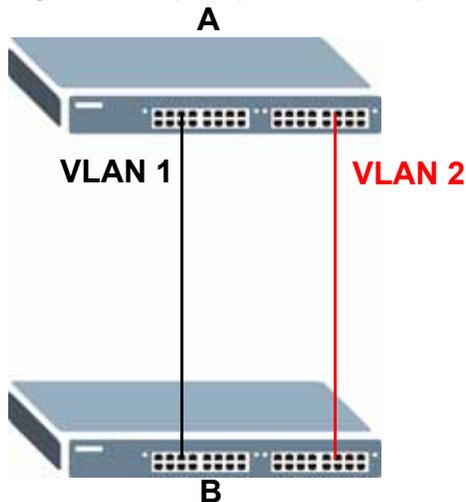
- Одно общее и внутреннее покрывающее дерево (Common and Internal Spanning Tree, CIST), представляющее структуру связности всей сети.
- Группировка нескольких мостов (или коммутирующих устройств) в регионы, которые рассматриваются сетью как один мост.
- Связывание VLAN с конкретным экземпляром покрывающего дерева (MSTI). Благодаря MSTI можно использовать одно и то же покрывающее дерево для нескольких сетей VLAN.
- Возможность балансировки нагрузки благодаря использованию для трафика различных VLAN конкретных путей в регионе.

11.1.5.1 Пример сети с поддержкой MSTP

На приведенном ниже рисунке показан пример сети, в которой на двух коммутаторах настроены две сети VLAN. В случае использования на коммутаторах протокола STP или RSTP канал для VLAN 2 будет заблокирован, так как протоколы STP и RSTP допускают наличие только одного канала и блокируют избыточные каналы.

Рисунок 50 Пример сети с поддержкой STP/RSTP

При использовании MSTP сети VLAN 1 и 2 можно связать с различными экземплярами покрывающего дерева в сети. Таким образом, трафик для двух сетей VLAN будет проходить по различным путям. Пример сети с использованием протокола MSTP показан на следующем рисунке.

Рисунок 51 Пример сети с поддержкой MSTP

11.1.5.2 Регион MST

Регионом MST называется логическая группа нескольких сетевых устройств, которая для остальной сети представляется в виде одного устройства. Каждое из устройств с поддержкой MSTP может принадлежать только одному региону MST. При поступлении блоков BPDU в регион MST стоимость внешнего пути (или путей, выходящих из данного региона) увеличивается на единицу. Стоимость внутреннего пути (или путей внутри данного региона) увеличивается на единицу при прохождении блока BPDU через регион.

На устройствах, принадлежащие одному региону MST, настраиваются одинаковые идентификационные параметры MSTP. Сюда входят следующие параметры:

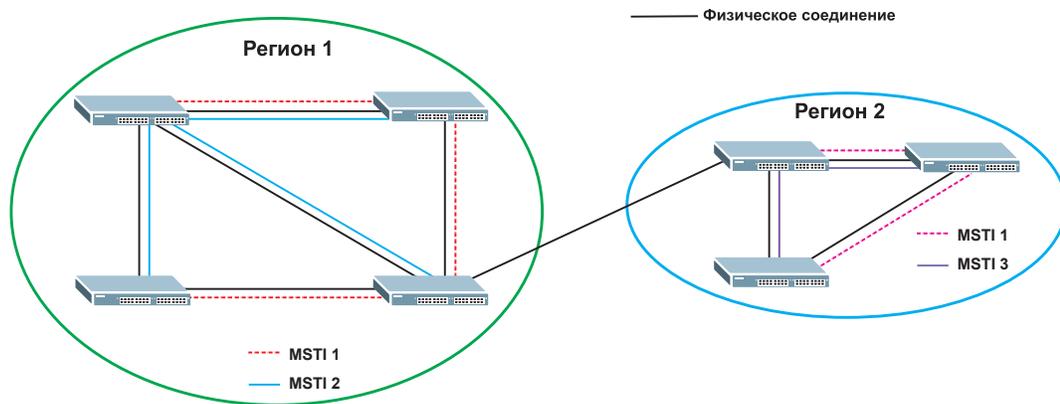
- Имя региона MST
- Номер версии в качестве уникального номера региона MST
- Связывание VLAN с конкретным экземпляром MST

11.1.5.3 Экземпляр MST

Экземпляр MST (MSTI) называется экземпляр покрывающего дерева. Для VLAN можно определить работу с использованием конкретного MSTI. Каждый созданный экземпляр MSTI идентифицируется по уникальному номеру (также называемому идентификатором MST ID), известному внутри региона. Таким образом, MSTI не охватывает несколько регионов MST.

Пример с двумя регионами MST показан на следующем рисунке. В регионах 1 и 2 имеется 2 экземпляра покрывающего дерева.

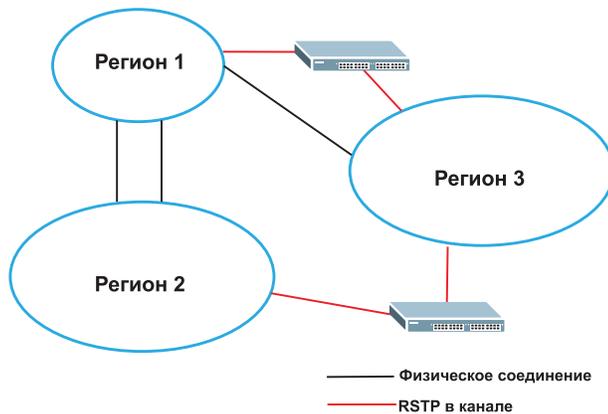
Рисунок 52 Экземпляры MSTI в различных регионах



11.1.5.4 Общее и внутреннее покрывающее дерево (CIST)

CIST представляет структуру связности всей сети в целом и является эквивалентом покрывающего дерева протоколов STP/RSTP. CIST представляет собой используемый по умолчанию экземпляр MST (MSTID 0). Все виртуальные локальные сети VLAN, которые не связаны с конкретным экземпляром MST, связаны с CIST. В сети с поддержкой MSTP имеется только одно дерево CIST, которое охватывает регионы MST и отдельные устройства с поддержкой протокола покрывающего дерева. Сеть может включать в себя несколько регионов MST и другие сегменты, в которых используется RSTP.

Рисунок 53 Пример сети с использованием MSTP и традиционного протокола RSTP



11.2 Экран состояния протокола STP

Вид экрана состояния протокола покрывающего дерева зависит от того, какой стандарт был выбран для сети. Чтобы открыть приведенный ниже экран, нажмите **Advanced Application > Spanning Tree Protocol**.

Рисунок 54 Экран Advanced Application > Spanning Tree Protocol

Spanning Tree Protocol Status		
	Configuration	RSTP
	MRSTP	MSTP
Spanning Tree Protocol: RSTP		
Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	0000-000000000000
Hello Time (second)	0	0
Max Age (second)	0	0
Forwarding Delay (second)	0	0
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times		0
Time Since Last Change		0:00:00

Вид данного экрана зависит от того, какой из режимов STP (RSTP, MRSTP или MSTP) был выбран на коммутаторе. Подробное описание данного экрана приводится в разделе, следующим за разделом с описанием настройки соответствующего режима STP. Чтобы выбрать один из режимов STP для коммутатора, нажмите на **Configuration**.

11.3 Настройка протокола покрывающего дерева

На экране **Spanning Tree Configuration** можно активировать на коммутаторе один из режимов STP. Нажмите на **Configuration** на экране **Advanced Application > Spanning Tree Protocol**.

Рисунок 55 Экран Advanced Application > Spanning Tree Protocol > Configuration

Поля экрана описаны в следующей таблице.

Таблица 26 Экран Advanced Application > Spanning Tree Protocol > Configuration

ПОЛЕ	ОПИСАНИЕ
Spanning Tree Mode	На коммутаторе можно активировать один из режимов STP: Выберите Rapid Spanning Tree , Multiple Rapid Spanning Tree или Multiple Spanning Tree . Общую информацию о STP можно найти в разд. 11.1 на стр. 113 .
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

11.4 Настройка быстрого протокола покрывающего дерева

Данный экран используется для настройки RSTP; более подробную информацию о RSTP можно найти в [разд. 11.1 на стр. 113](#). Нажмите на **RSTP** на экране **Advanced Application > Spanning Tree Protocol**.

Рисунок 56 Экран Advanced Application > Spanning Tree Protocol > RSTP

Port	Active	Priority	Path Cost
*	<input type="checkbox"/>		
1	<input checked="" type="checkbox"/>	128	15
2	<input checked="" type="checkbox"/>	128	14
3	<input checked="" type="checkbox"/>	128	13
4	<input checked="" type="checkbox"/>	128	12
5	<input type="checkbox"/>	128	19
6	<input type="checkbox"/>	128	19
7	<input type="checkbox"/>	128	19
8	<input type="checkbox"/>	128	19

Поля экрана описаны в следующей таблице.

Таблица 27 Экран Advanced Application > Spanning Tree Protocol > RSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите Status , чтобы отобразить экран состояния RSTP Status (см. рис. 57 на стр. 123).
Active	<p>Установите этот переключатель, чтобы включить протокол RSTP. Снимите выделение с переключателя, чтобы отключить RSTP.</p> <p>Примечание: Чтобы включить протокол RSTP на коммутаторе, необходимо также активировать режим Rapid Spanning Tree на экране Advanced Application > Spanning Tree Protocol > Configuration.</p>
Bridge Priority	<p>Приоритет моста используется для определения корневого коммутатора, корневого порта и назначенного порта. Коммутатор с наивысшим приоритетом (наименьшее числовое значение) становится корневым коммутатором протокола STP. Если у всех коммутаторов одинаковый приоритет, то корневым становится коммутатором с наименьшим MAC-адресом. Выберите значение в ниспадающем списке.</p> <p>Чем меньшее числовое значение будет выбрано, тем выше будет приоритет у этого моста.</p> <p>Параметр Bridge Priority определяет корневой мост, который, в свою очередь, определяет параметры Hello Time, Max Age и Forwarding Delay.</p>

Таблица 27 Экран Advanced Application > Spanning Tree Protocol > RSTP

ПОЛЕ	ОПИСАНИЕ
Hello Time	Временной интервал в секундах между конфигурационными сообщениями BPDU (блоки данных мостового протокола), генерируемыми корневым коммутатором. Диапазон допустимых значений – от 1 до 10 секунд.
Max Age	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая сообщений BPDU, прежде чем он предпримет попытку произвести настройку заново. Все порты коммутатора (за исключением назначенных портов) должны получать сообщения BPDU через регулярные промежутки времени. Любой порт с устаревшей информацией протокола STP (содержащейся в последнем сообщении BPDU) становится назначенным портом для подключенной локальной сети. Если это корневой порт, то новый корневой порт выбирается из портов коммутатора, подключенных к сети. Диапазон допустимых значений – от 6 до 40 секунд.
Forwarding Delay	Временной интервал (в секундах), в течение которого корневой ожидает, прежде чем сменить состояния. Эта задержка необходима для того, чтобы коммутатор успел получить информацию о топологии прежде, чем он начнет пересылать кадры. Кроме того, каждому порту требуется время для получения информации о конфликтах, которая может заставить его вернуться в состояние блокировки; в противном случае могут возникнуть временные петли данных. Диапазон допустимых значений – от 4 до 30 секунд. Как правило: Примечание: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить на этом порту протокол RSTP.
Priority	Здесь можно определить приоритет для каждого из портов. Уровень приоритета определяет, какой из портов нужно отключить, когда на нескольких портах коммутатора образуется петля. Порты с более высоким значением приоритета отключаются первыми. Допустимый диапазон значений – от 0 до 255, по умолчанию устанавливается уровень приоритета 128.
Path Cost	Стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Данное значение рекомендуется выбирать в зависимости от скорости моста. Чем ниже скорость, тем выше стоимость – дополнительную информацию можно найти в табл. 24 на стр. 114 .
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

11.5 Состояние быстрого протокола покрывающего дерева

Чтобы отобразить следующий экран состояния, нажмите в навигационной панели **Advanced Application > Spanning Tree Protocol**. Более подробную информацию о RSTP можно найти в [разд. 11.1 на стр. 113](#).



Данный экран доступен лишь в том случае, если на коммутаторе был включен протокол RSTP.

Рисунок 57 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP

Spanning Tree Protocol Status		
	Configuration	RSTP MRSTP MSTP
Spanning Tree Protocol: RSTP		
Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	0000-000000000000
Hello Time (second)	0	0
Max Age (second)	0	0
Forwarding Delay (second)	0	0
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times		0
Time Since Last Change		0:00:00

Поля экрана описаны в следующей таблице.

Таблица 28 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP

ПОЛЕ	ОПИСАНИЕ
Configuration	Нажмите Configuration , чтобы выбрать нужный режим STP. Чтобы изменить настройки RSTP коммутатора, нажмите RSTP .
Bridge	Root относится к основанию покрывающего дерева (корневой мост). Our Bridge – данный коммутатор. Данный коммутатор также может быть корневым мостом.
Bridge ID	Уникальный идентификатор данного моста, состоящий из уровня приоритета моста и MAC-адреса. Если коммутатор является корневым, то в полях Root и Our Bridge указывается один и тот же идентификатор.
Hello Time (second)	Временной интервал (в секундах), в течение которого корневой коммутатор передает конфигурационное сообщение. Значения параметров Hello Time, Max Age и Forwarding Delay определяет корневой мост.
Max Age (second)	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая конфигурационного сообщения, прежде чем он предпримет попытку произвести настройку заново.
Forwarding Delay (second)	Время (в секундах), в течение которого корневой коммутатор ожидает перед сменой состояний (то есть от Listening к Learning и затем к Forwarding).
	Примечание: Состояние «Listening» не используется в RSTP.

Таблица 28 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP

ПОЛЕ	ОПИСАНИЕ
Cost to Bridge	Стоимость пути от корневого порта на данном коммутаторе к корневому коммутатору.
Port ID	Уровень приоритета и номер порта на коммутаторе, через который этот коммутатор должен связываться с корнем покрывающего дерева.
Topology Changed Times	Количество смен конфигурации покрывающего дерева.
Time Since Last Change	Время, прошедшее с последней смены конфигурации покрывающего дерева.

11.6 Настройка протокола MRSTP

Чтобы настроить протокол MRSTP, нажмите на **MRSTP** на экране **Advanced Application > Spanning Tree Protocol**. Более подробную информацию о MRSTP можно найти в [разд. 11.1 на стр. 113](#).

Рисунок 58 Экран Advanced Application > Spanning Tree Protocol > MRSTP

Tree	Active	Bridge Priority	Hello Time	MAX Age	Forwarding Delay
1	<input type="checkbox"/>	32768	2 seconds	20 seconds	15
2	<input type="checkbox"/>	32768	2 seconds	20 seconds	15

Port	Active	Priority	Path Cost	Tree
*	<input type="checkbox"/>			1
1	<input type="checkbox"/>	128	19	1
2	<input type="checkbox"/>	128	19	1
3	<input type="checkbox"/>	128	19	1
4	<input type="checkbox"/>	128	19	1
5	<input type="checkbox"/>	128	19	1
6	<input type="checkbox"/>	128	19	1
7	<input type="checkbox"/>	128	19	1
8	<input type="checkbox"/>	128	19	1

Поля экрана описаны в следующей таблице.

Таблица 29 Экран Advanced Application > Spanning Tree Protocol > MRSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите Status , чтобы отобразить экран состояния MRSTP Status (см. рис. 57 на стр. 123).
Tree	Порядковый номер дерева STP (только для чтения).

Таблица 29 Экран Advanced Application > Spanning Tree Protocol > MRSTP

ПОЛЕ	ОПИСАНИЕ
Active	<p>Установите этот переключатель, чтобы включить дерево протокола STP. Снимите выделение с переключателя, чтобы отключить дерево протокола STP.</p> <p>Примечание: Чтобы включить протокол MRSTP на коммутаторе, необходимо также активировать режим Multiple Rapid Spanning Tree на экране Advanced Application > Spanning Tree Protocol > Configuration.</p>
Bridge Priority	<p>Приоритет моста используется для определения корневого коммутатора, корневого порта и назначенного порта. Коммутатор с наивысшим приоритетом (наименьшее числовое значение) становится корневым коммутатором протокола STP. Если у всех коммутаторов одинаковый приоритет, то корневым становится коммутатором с наименьшим MAC-адресом. Выберите значение в ниспадающем списке.</p> <p>Чем меньшее числовое значение будет выбрано, тем выше будет приоритет у этого моста.</p> <p>Параметр Bridge Priority определяет корневой мост, который, в свою очередь, определяет параметры Hello Time, Max Age и Forwarding Delay.</p>
Hello Time	<p>Временной интервал в секундах между конфигурационными сообщениями BPDU (блоки данных мостового протокола), генерируемыми корневым коммутатором. Диапазон допустимых значений – от 1 до 10 секунд.</p>
MAX Age	<p>Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая сообщений BPDU, прежде чем он предпримет попытку произвести настройку заново. Все порты коммутатора (за исключением назначенных портов) должны получать сообщения BPDU через регулярные промежутки времени. Любой порт с устаревшей информацией протокола STP (содержащейся в последнем сообщении BPDU) становится назначенным портом для подключенной локальной сети. Если это корневой порт, то новый корневой порт выбирается из портов коммутатора, подключенных к сети. Диапазон допустимых значений – от 6 до 40 секунд.</p>
Forwarding Delay	<p>Временной интервал (в секундах), в течение которого корневой ожидает, прежде чем сменить состояния. Эта задержка необходима для того, чтобы коммутатор успел получить информацию о топологии прежде, чем он начнет пересылать кадры. Кроме того, каждому порту требуется время для получения информации о конфликтах, которая может заставить его вернуться в состояние блокировки; в противном случае могут возникнуть временные петли данных. Диапазон допустимых значений – от 4 до 30 секунд.</p> <p>Как правило:</p> <p>Примечание: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$</p>
Port	<p>В этом поле отображается номер порта.</p>
*	<p>Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Active	<p>Установите этот переключатель, чтобы включить на этом порту протокол STP.</p>

Таблица 29 Экран Advanced Application > Spanning Tree Protocol > MRSTP

ПОЛЕ	ОПИСАНИЕ
Priority	Здесь можно определить приоритет для каждого из портов. Уровень приоритета определяет, какой из портов нужно отключить, когда на нескольких портах коммутатора образуется петля. Порты с более высоким значением приоритета отключаются первыми. Допустимый диапазон значений – от 0 до 255, по умолчанию устанавливается уровень приоритета 128.
Path Cost	Стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Данное значение рекомендуется выбирать в зависимости от скорости моста. Чем ниже скорость, тем выше стоимость – дополнительную информацию можно найти в табл. 24 на стр. 114 .
Tree	Укажите, к какому дереву STP должен принадлежать данный порт.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

11.7 Состояние протокола MRSTP

Чтобы отобразить следующий экран состояния, нажмите в навигационной панели **Advanced Application > Spanning Tree Protocol**. Более подробную информацию о MRSTP можно найти в [разд. 11.1 на стр. 113](#).



Данный экран доступен лишь в том случае, если на коммутаторе был включен протокол MRSTP.

Рисунок 59 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP

Spanning Tree Protocol Status		
Spanning Tree Protocol: MRSTP		
Tree <input type="text" value="1"/>		
Bridge	Root	Our Bridge
Bridge ID	8000-001349000002	8000-001349000002
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times	0	
Time Since Last Change	0:00:00	

Поля экрана описаны в следующей таблице.

Таблица 30 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP

ПОЛЕ	ОПИСАНИЕ
Configuration	Нажмите Configuration , чтобы выбрать нужный режим STP. Для изменения настроек MRSTP коммутатора нажмите на MRSTP .
Tree	Выберите дерево STP, настройки которого необходимо отобразить.
Bridge	Root относится к основанию покрывающего дерева (корневой мост). Our Bridge – данный коммутатор. Данный коммутатор также может быть корневым мостом.
Bridge ID	Уникальный идентификатор данного моста, состоящий из уровня приоритета моста и MAC-адреса. Если коммутатор является корневым, то в полях Root и Our Bridge указывается один и тот же идентификатор.
Hello Time (second)	Временной интервал (в секундах), в течение которого корневой коммутатор передает конфигурационное сообщение. Значения параметров Hello Time, Max Age и Forwarding Delay определяет корневой мост.
Max Age (second)	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая конфигурационного сообщения, прежде чем он предпримет попытку произвести настройку заново.
Forwarding Delay (second)	Время (в секундах), в течение которого корневой коммутатор ожидает перед сменой состояний (то есть от Listening к Learning и затем к Forwarding). Примечание: Состояние «Listening» не используется в RSTP.
Cost to Bridge	Стоимость пути от корневого порта на данном коммутаторе к корневому коммутатору.
Port ID	Уровень приоритета и номер порта на коммутаторе, через который этот коммутатор должен связываться с корнем покрывающего дерева.
Topology Changed Times	Количество смен конфигурации покрывающего дерева.
Time Since Last Change	Время, прошедшее с последней смены конфигурации покрывающего дерева.

11.8 Настройка протокола MSTP

Чтобы настроить протокол MSTP, нажмите на **MSTP** на экране **Advanced Application > Spanning Tree Protocol**. Более подробную информацию о MSTP можно найти в [разд. 11.1.5 на стр. 116](#).

Рисунок 60 Экран Advanced Application > Spanning Tree Protocol > MSTP

Multiple Spanning Tree Protocol
Status

Bridge:

Active	<input type="checkbox"/>
Hello Time	<input type="text" value="2"/> seconds
MAX Age	<input type="text" value="20"/> seconds
Forwarding Delay	<input type="text" value="15"/> seconds
Maximum hops	<input type="text" value="128"/>
Configuration Name	<input type="text" value="001349000002"/>
Revision Number	<input type="text" value="0"/>

Apply Cancel

Instance:

Instance	<input type="text"/>
Bridge Priority	<input type="text" value="0"/> ▼
VLAN Range	Start <input type="text"/> End <input type="text"/> Add Remove Clear
Enabled VLAN(s)	<div style="border: 1px solid gray; height: 50px; width: 100%;"></div>

Port	Active	Priority	Path Cost
*	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
1	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="19"/>
2	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="19"/>
3	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="19"/>
4	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="19"/>
5	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="19"/>
6	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="19"/>
7	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="19"/>
8	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="19"/>

Add Cancel

Instance	VLAN	Active Port	Delete
0	1-4093	-	

Delete Cancel

Поля экрана описаны в следующей таблице.

Таблица 31 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите Status , чтобы отобразить экран состояния MSTP Status (см. рис. 61 на стр. 132).
Active	Установите этот переключатель, если необходимо включить протокол MSTP на коммутаторе. Снимите выделение с переключателя, если требуется отключить протокол MSTP на коммутаторе. Примечание: Чтобы включить протокол MSTP на коммутаторе, необходимо также активировать режим Multiple Spanning Tree на экране Advanced Application > Spanning Tree Protocol > Configuration .
Hello Time	Временной интервал в секундах между конфигурационными сообщениями BPDU (блоки данных мостового протокола), генерируемыми корневым коммутатором. Диапазон допустимых значений – от 1 до 10 секунд.
MaxAge	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая сообщений BPDU, прежде чем он предпримет попытку произвести настройку заново. Все порты коммутатора (за исключением назначенных портов) должны получать сообщения BPDU через регулярные промежутки времени. Любой порт с устаревшей информацией протокола STP (содержащейся в последнем сообщении BPDU) становится назначенным портом для подключенной локальной сети. Если это корневой порт, то новый корневой порт выбирается из портов коммутатора, подключенных к сети. Диапазон допустимых значений – от 6 до 40 секунд.
Forwarding Delay	Временной интервал (в секундах), в течение которого корневой ожидает, прежде чем сменить состояния. Эта задержка необходима для того, чтобы коммутатор успел получить информацию о топологии прежде, чем он начнет пересылать кадры. Кроме того, каждому порту требуется время для получения информации о конфликтах, которая может заставить его вернуться в состояние блокировки; в противном случае могут возникнуть временные петли данных. Диапазон допустимых значений – от 4 до 30 секунд. Как правило: Примечание: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Maximum hops	Введите количество переходов (от 1 до 255) в регионе MSTP, после которого блок данных BPDU будет отбрасываться, и информация порта будет считаться устаревшей.
Configuration Name	Введите имя-описание (до 32 символов) для региона MST.
Revision Number	Введите идентификационный номер конфигурации региона. Этот номер должен быть одинаковым на всех устройствах, принадлежащих одному региону.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Instance	В этом разделе определяются параметры MSTI (экземпляра покрывающего дерева).

Таблица 31 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
Instance	Введите номер, используемый для идентификации данного экземпляра MST на коммутаторе. Данный коммутатор поддерживает номера экземпляров в диапазоне 0-16.
Bridge Priority	Укажите приоритет коммутатора для конкретного экземпляра покрывающего дерева. Чем меньше это значение, тем с большей вероятностью коммутатор будет выбран в качестве корневого моста в рамках данного экземпляра покрывающего дерева. В качестве приоритета допускается использовать значения от 0 до 61440 с шагом 4096 (т.е. значения 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 и 61440).
VLAN Range	Введите начальный идентификатор диапазона идентификаторов VLAN, который необходимо добавить или удалить из области редактирования диапазонов VLAN, в поле Start . Введите конечный идентификатор диапазона идентификаторов VLAN, который необходимо добавить или удалить из области редактирования диапазонов VLAN, в поле End . Затем нажмите: <ul style="list-style-type: none"> • Add – чтобы добавить данный диапазон идентификаторов VLAN к списку связанных с данным экземпляром MST. • Remove – чтобы удалить данный диапазон идентификаторов VLAN из списка связанных с данным экземпляром MST. • Clear – чтобы удалить все сети VLAN из списка связанных с данным экземпляром MST.
Enabled VLAN(s)	В данном поле отображаются сети VLAN, связанные с данным экземпляром MST.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите данный переключатель, чтобы добавить данный порт к данному экземпляру MST.
Priority	Здесь можно определить приоритет для каждого из портов. Уровень приоритета определяет, какой из портов нужно отключить, когда на нескольких портах коммутатора образуется петля. Порты с более высоким значением приоритета отключаются первыми. Допустимый диапазон значений – от 0 до 255, по умолчанию устанавливается уровень приоритета 128.
Path Cost	Стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Данное значение рекомендуется выбирать в зависимости от скорости моста. Чем ниже скорость, тем выше стоимость – дополнительную информацию можно найти в табл. 24 на стр. 114 .
Add	Нажмите Add , чтобы сохранить данный экземпляр MST в оперативной памяти коммутатора. Это изменение будет утеряно в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Instance	В этом поле отображается идентификатор экземпляра MST.

Таблица 31 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
VLAN	В данном поле отображается идентификатор VID (или диапазоны идентификаторов VID), связанные с данным экземпляром MST.
Active Port	В данном поле отображаются порты, включенные в данный экземпляр MST.
Delete	В столбце Delete установите переключатели правил, которые нужно удалить, затем нажмите кнопку Delete .
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

11.9 Состояние протокола MSTP

Чтобы отобразить следующий экран состояния, нажмите в навигационной панели **Advanced Application > Spanning Tree Protocol**. Более подробную информацию о MSTP можно найти в [разд. 11.1.5 на стр. 116](#).



Данный экран доступен лишь в том случае, если на коммутаторе был включен протокол MSTP.

Рисунок 61 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP

Spanning Tree Protocol Status Configuration RSTP MRSTP MSTP

Spanning Tree Protocol: MSTP

CST

Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	8000-000000000000
Hello Time (second)	0	2
Max Age (second)	0	20
Forwarding Delay (second)	0	15
Cost to Bridge	0	0
Port ID	0x0000	0x0000
Configuration Name	001349000002	
Revision Number	0	
Configuration Digest	A317523DB32DA2D62	
Topology Changed Times	0	
Time Since Last Change	0	

Instance:

Instance	VLAN
0	1-4093

MSTI 1

Bridge	Regional Root	Our Bridge
Bridge ID	0000-000000000000	8001-000000000000
Internal Cost	0	0
Port ID	0x0000	0x0000

Поля экрана описаны в следующей таблице.

Таблица 32 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP

ПОЛЕ	ОПИСАНИЕ
Configuration	Нажмите Configuration , чтобы выбрать нужный режим STP. Для изменения настроек MSTP коммутатора нажмите на MSTP .
CST	В данном разделе описываются настройки общего покрывающего дерева.
Bridge	Root относится к основанию покрывающего дерева (корневой мост). Our Bridge – данный коммутатор. Данный коммутатор также может быть корневым мостом.
Bridge ID	Уникальный идентификатор данного моста, состоящий из уровня приоритета моста и MAC-адреса. Если коммутатор является корневым, то в полях Root и Our Bridge указывается один и тот же идентификатор.
Hello Time (second)	Временной интервал (в секундах), в течение которого корневой коммутатор передает конфигурационное сообщение.
Max Age (second)	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая конфигурационного сообщения, прежде чем он предпримет попытку произвести настройку заново.
Forwarding Delay (second)	Время (в секундах), в течение которого корневой коммутатор ожидает перед сменой состояний (то есть от Listening к Learning и затем к Forwarding).
Cost to Bridge	Стоимость пути от корневого порта на данном коммутаторе к корневому коммутатору.

Таблица 32 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP

ПОЛЕ	ОПИСАНИЕ
Port ID	Уровень приоритета и номер порта на коммутаторе, через который этот коммутатор должен связываться с корнем покрывающего дерева.
Configuration Name	В этом поле отображается имя конфигурации для данного региона MST.
Revision Number	В этом поле отображается номер версии для данного региона MST.
Configuration Digest	Кодификация конфигурации генерируется на основе информации о связывании VLAN-MSTI. В данном поле отображается состоящая из 16 октетов сигнатура, которая включается в блоки BPDU протокола MSTP. Кодификация отображается в данном поле лишь в том случае, если в системе включен протокол MSTP.
Topology Changed Times	Количество смен конфигурации покрывающего дерева.
Time Since Last Change	Время, прошедшее с последней смены конфигурации покрывающего дерева.
Instance:	В данных полях отображается информация о связывании MSTI с VLAN. Другими словами, какие виртуальные локальные сети работают в каждом из экземпляров покрывающего дерева.
Instance	В этом поле отображается идентификатор MSTI ID.
VLAN	В этом поле отображаются сети VLAN, связанные с указанным MSTI.
MSTI	Выберите экземпляр MST, настройки которого необходимо отобразить.
Bridge	Root определяет основание экземпляра покрывающего дерева MST. Our Bridge – данный коммутатор. Данный коммутатор также может быть корневым мостом.
Bridge ID	Уникальный идентификатор данного моста, состоящий из уровня приоритета моста и MAC-адреса. Если коммутатор является корневым, то в полях Root и Our Bridge указывается один и тот же идентификатор.
Internal Cost	Стоимость пути от корневого порта в данном экземпляре MST к корневому коммутатору региона.
Port ID	Уровень приоритета и номер порта на коммутаторе, через который этот коммутатор должен связываться с корнем экземпляра MST.

Управление пропускной способностью

В данной главе рассказывается, как ограничить максимальную пропускную способность с помощью меню **Bandwidth Control**.

12.1 Обзор управления пропускной способностью

Управление пропускной способностью подразумевает определение максимальной разрешенной пропускной способности для входящего и/или исходящего потоков трафика через порт.

12.1.1 CIR и PIR

Гарантированная скорость передачи информации (Committed Information Rate, CIR) представляет собой гарантированную пропускную способность для входящего трафика через порт. Пиковая скорость передачи информации (Peak Information Rate, PIR) представляет собой максимальную пропускную способность, которая может быть предоставлена для входящего трафика через порт при отсутствии перегрузок в сети.

Значения CIR и PIR должны быть установлены для всех портов, для которых используется общая пропускная способность канала каскадирования. При достижении значения CIR пакеты пересылаются со скоростью, которая может достигать PIR. В случае перегрузок в сети поступающие через входящий порт пакеты, занимающие пропускную способность сверх CIR, помечаются на отбрасывание.



Значение CIR должно быть меньше PIR.



Сумма значений CIR должна быть меньше или равна пропускной способности канала каскадирования.

12.2 Настройка управления пропускной способностью

Чтобы открыть показанный ниже экран, выберите в навигационной панели **Advanced Application > Bandwidth Control**.

Рисунок 62 Экран Advanced Application > Bandwidth Control

Port	Active	Ingress Rate		Active	Egress Rate
		Commit Rate	Peak Rate		
*	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>	<input type="text"/> 1 Kbps	<input type="checkbox"/>

Поля экрана описаны в следующей таблице.

Таблица 33 Экран Advanced Application > Bandwidth Control

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить управление пропускной способностью на коммутаторе.
Port	В этом поле отображается номер порта.
*	<p>Настройки в этой строке применяются ко всем портам.</p> <p>Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Ingress Rate	
Active	Установите этот переключатель, чтобы включить на этом порту ограничения гарантированной скорости.
Commit Rate	Укажите гарантированную пропускную способность в килобитах в секунду (кбит/с) для входящего потока трафика через этот порт. Гарантированная скорость должна быть меньше пиковой скорости (Peak Rate). Сумма значений гарантированной скорости должна быть меньше или равна пропускной способности канала каскадирования.
Active	Установите этот переключатель, чтобы включить на этом порту ограничения пиковой скорости.
Peak Rate	Укажите максимальную разрешенную пропускную способность в килобитах в секунду (кбит/с) для входящего потока трафика через этот порт.

Таблица 33 Экран Advanced Application > Bandwidth Control (продолжение)

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на этом порту ограничения скорости для исходящего трафика.
Egress Rate	Укажите максимальную разрешенную пропускную способность в килобитах в секунду (кбит/с) для исходящего потока трафика через этот порт.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Контроль широковещательных штормов

В этой главе описывается функция контроля широковещательных штормов и порядок ее настройки.

13.1 Настройка функции контроля широковещательных штормов

Функция контроля широковещательных штормов ограничивает количество широковещательных пакетов, пакетов мультивещания и DLF-пакетов (destination lookup failure), которые могут быть приняты за секунду времени через порты коммутатора. При достижении максимального допустимого количества широковещательных пакетов, пакетов мультивещания и/или DLF-пакетов все последующие пакеты отбрасываются. Включение этой функции позволяет снизить объем широковещательных пакетов, пакетов мультивещания и DLF-пакетов, поступающих в сеть. Имеется возможность ограничить для каждого порта количество пакетов каждого отдельного типа.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application > Broadcast Storm Control**.

Рисунок 63 Экран Advanced Application > Broadcast Storm Control

Port	Broadcast (pkt/s)	Multicast (pkt/s)	DLF (pkt/s)
*	<input type="checkbox"/> []	<input type="checkbox"/> []	<input type="checkbox"/> []
1	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]
2	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]
3	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]
4	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]
5	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]
6	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]
7	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]
8	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]	<input type="checkbox"/> [0]

Поля экрана описаны в следующей таблице.

Таблица 34 Экран Advanced Application > Broadcast Storm Control

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить контроль широковещательного трафика на коммутаторе. Снимите выделение с переключателя, если необходимо отключить эту функцию.
Port	В этом поле отображается номер порта.
*	<p>Настройки в этой строке применяются ко всем портам.</p> <p>Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Broadcast (pkt/s)	Выберите данную опцию и укажите количество широковещательных пакетов, которое может приниматься портом в секунду.
Multicast (pkt/s)	Выберите данную опцию и укажите количество мультивещательных пакетов, которое может приниматься портом в секунду.
DLF (pkt/s)	Выберите данную опцию и укажите количество DLF-пакетов (destination lookup failure), которое может приниматься портом в секунду.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Зеркальное копирование

В данной главе описаны экраны настройки зеркального копирования портов.

14.1 Настройка зеркального копирования портов

Зеркальное копирование портов позволяет копировать трафик на контрольный порт (тот, на который копируется трафик), чтобы можно было анализировать трафик на контролируемом порту, не вмешиваясь в поток.

Чтобы отобразить экран настроек зеркального копирования **Mirroring**, выберите в навигационной панели **Advanced Application > Mirroring**. Этот экран позволяет выбрать контрольный порт и определить поток трафика, который будет копироваться на контрольный порт.

Рисунок 64 Экран Advanced Application > Mirroring

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▼
1	<input type="checkbox"/>	Ingress ▼
2	<input type="checkbox"/>	Ingress ▼
3	<input type="checkbox"/>	Ingress ▼
4	<input type="checkbox"/>	Ingress ▼
5	<input type="checkbox"/>	Ingress ▼
6	<input type="checkbox"/>	Ingress ▼
7	<input type="checkbox"/>	Ingress ▼
8	<input type="checkbox"/>	Ingress ▼

Поля экрана описаны в следующей таблице.

Таблица 35 Экран Advanced Application > Mirroring

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, если необходимо включить фильтрацию зеркального копирования портов на коммутаторе. Снимите выделение с переключателя, если необходимо отключить эту функцию.
Monitor Port	Контрольный порт – это порт, на который копируется трафик с целью его анализа без вмешательства в поток трафика на исходном порту (портах). Введите номер контрольного порта.
Port	В этом поле отображается номер порта.
*	<p>Настройки в этой строке применяются ко всем портам.</p> <p>Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Mirrored	Выберите эту опцию, чтобы копировать трафик на порту.
Direction	Выберите направление трафика для зеркального копирования из ниспадающего списка. Выбрать можно Egress (исходящий), Ingress (входящий) или Both (весь трафик).
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Агрегация каналов

В этой главе рассказывается о логическом объединении (агрегации) нескольких физических каналов в один логический канал большей пропускной способности.

15.1 Обзор агрегации каналов

Агрегация (группирование) каналов – это объединение нескольких физических портов в один логический канал большей пропускной способности. Объединить несколько портов в один канал можно в том случае, если, например, дешевле использовать несколько каналов меньшей скорости, чем не на полную мощность загружать высокоскоростной, но более дорогой канал с одним портом.

Однако, чем больше портов будут подвергнуты агрегации, тем меньше доступных портов останется. Группой портов называется единый логический канал, объединяющий несколько портов.

Для формирования группы портов начальный порт каждой группы должен быть физически подключен.

Данный коммутатор поддерживает как статическую, так и динамическую агрегацию каналов.



В надлежащем образом спланированной сети рекомендуется использовать только статическую агрегацию каналов. Это обеспечивает более высокую стабильность сети и управление группами портов на коммутаторе.

Пример использования статического группирования портов можно найти в [разд. 15.6 на стр. 148](#).

15.2 Динамическая агрегация каналов

Поддержка статического и динамического группирования портов осуществляется коммутатором в соответствии со стандартом IEEE 802.3ad (протокол LACP).

Данный коммутатор поддерживает стандарт агрегации каналов IEEE802.3ad. Этот стандарт описывает протокол управления агрегацией каналов (LACP) – протокол, обеспечивающий динамическое создание и управление группами портов

При включении агрегации каналов по протоколу LACP на одном из портов этот порт может начать процесс автоматического согласования групп портов с устройством на другом конце. Протокол LACP также поддерживает избыточность портов, то есть если работающий порт выйдет из строя, то один из «резервных» портов начнет работать без вмешательства пользователя. Следует иметь в виду, что:

- Все порты должны быть подключены по схеме «точка-точка» к одному и тому же Ethernet-коммутатору, а также сконфигурированы в группу с использованием протокола LACP.
- Протокол LACP работает только на дуплексных каналах.
- Все порты, принадлежащие к одной группе, должны иметь одинаковый тип среды передачи, скорость, режим дуплекса и настройки управления потоком.

Настраивать группы портов или протокол LACP следует до подключения Ethernet-коммутатора, во избежание появления петель в сетевой топологии.

15.2.1 Идентификатор агрегации каналов

Идентификатор агрегации протокола LACP включает в себя¹:

Таблица 36 Идентификатор агрегации каналов: локальный коммутатор

ПРИОРИТЕТ СИСТЕМЫ	MAC-АДРЕС	КЛЮЧ	ПРИОРИТЕТ ПОРТА	НОМЕР ПОРТА
0000	00-00-00-00-00-00	0000	00	0000

Таблица 37 Идентификатор агрегации каналов: коммутатор-партнер

ПРИОРИТЕТ СИСТЕМЫ	MAC-АДРЕС	КЛЮЧ	ПРИОРИТЕТ ПОРТА	НОМЕР ПОРТА
0000	00-00-00-00-00-00	0000	00	0000

15.3 Состояние агрегации каналов

Выберите в навигационной панели **Advanced Application > Link Aggregation**. По умолчанию появится экран **Link Aggregation Status**. Дополнительную информацию можно найти в [разд. 15.1 на стр. 143](#).

1. Уровень приоритета порта и номер порта равны нулю, так как это агрегационный идентификатор для всей группы, а не отдельного порта.

Рисунок 65 Экран Advanced Application > Link Aggregation Status

Link Aggregation Status			Link Aggregation Setting	
Index	Enabled Ports	Synchronized Ports	Aggregator ID	Status
1	-	-	-	-
2	-	-	-	-
3	-	-	-	-
4	-	-	-	-
5	-	-	-	-
6	-	-	-	-

Поля экрана описаны в следующей таблице.

Таблица 38 Экран Advanced Application > Link Aggregation Status

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается идентификатор группы, который определяет группу портов, то есть логический канал, объединяющий несколько портов.
Enabled Port	Порты, настроенные в меню Link Aggregation как члены группы портов.
Synchronized Ports	Порты, в данный момент передающие данные как единый канал в этой группе портов.
Aggregator ID	Идентификатор агрегации каналов включает в себя: приоритет системы, MAC-адрес, ключ, приоритет порта и номер порта. Более подробную информацию об этом поле можно найти в разд. 15.2.1 на стр. 144 .
Status	В этом поле отображается способ добавления указанных портов в группу портов. Возможные значения: <ul style="list-style-type: none"> • Static – если порты настроены в качестве статических членов группы портов. • LACP – если порты были присоединены к группе портов посредством LACP.

15.4 Настройка агрегации каналов

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application > Link Aggregation > Link Aggregation Setting**. Дополнительную информацию об агрегации каналов можно найти в [разд. 15.1 на стр. 143](#).

Рисунок 66 Экран Advanced Application > Link Aggregation > Link Aggregation Setting

Group ID	Active
T1	<input type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>
T5	<input type="checkbox"/>
T6	<input type="checkbox"/>

Port	Group
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None

Поля экрана описаны в следующей таблице.

Таблица 39 Экран Advanced Application > Link Aggregation > Link Aggregation Setting

ПОЛЕ	ОПИСАНИЕ
Link Aggregation Setting	При включении статической агрегации каналов все настройки производятся на данном экране.
Group ID	В этом поле указан идентификатор группы агрегации каналов, то есть логического канала, объединяющего несколько портов.
Active	Установите этот переключатель, чтобы активировать группу портов.
Port	В этом поле отображается номер порта.
Group	Выберите группу портов, к которой принадлежит порт.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

15.5 Протокол управления агрегацией каналов LACP

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP**. Дополнительную информацию о динамической агрегации каналов можно найти в [разд. 15.2 на стр. 143](#).

Рисунок 67 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

Group ID	LACP Active
T1	<input type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>
T5	<input type="checkbox"/>
T6	<input type="checkbox"/>

Port	LACP Timeout
*	30 seconds
1	30 seconds
2	30 seconds
3	30 seconds
4	30 seconds
5	30 seconds
6	30 seconds
7	30 seconds
8	30 seconds

Поля экрана описаны в следующей таблице.

Таблица 40 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

ПОЛЕ	ОПИСАНИЕ
Link Aggregation Control Protocol	Примечание: Настройки на данном экране следует производить только при включении динамической агрегации каналов.
Active	Установите этот переключатель, чтобы включить протокол LACP.

Таблица 40 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (продолжение)

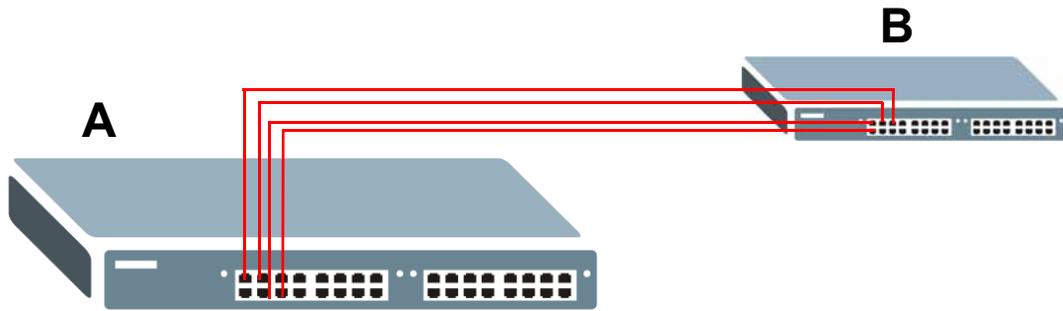
ПОЛЕ	ОПИСАНИЕ
System Priority	Приоритет системы протокола LACP – это число от 1 до 65 535. Коммутатор с наименьшим приоритетом системы (и наименьшим номером порта, если значения приоритета системы одинаковы) становится «сервером» протокола LACP. «Сервер» LACP управляет работой протокола LACP. Введите номер для установки приоритета активного порта, использующего протокол LACP. Чем меньше номер, тем выше уровень приоритета.
Group ID	В этом поле указан идентификатор группы агрегации каналов, то есть логического канала, объединяющего несколько портов.
LACP Active	Установите этот переключатель, чтобы включить протокол LACP для группы.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
LACP Timeout	Тайм-аут, определяющий временной промежуток от одного обмена пакетами LACP между отдельными портами до другого (в целях проверки работоспособности портов-партнеров в группе портов). Если порт не ответил после трех попыток, то он считается «отключенным» и удаляется из группы. Для загруженных сгруппированных каналов следует использовать короткий интервал (одна секунда), чтобы обеспечить скорейшее удаление отключенных портов из группы. Выберите значение (1 секунда или 30 секунд).
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

15.6 Пример статического группирования портов

В данном примере показано создание статической группы портов для портов 2-5.

- 1 Выполните физические подключения** – подключите все порты, которые должны войти в группу, к одному и тому же пункту назначения. На приведенном ниже рисунке показано подключение портов 2-5 коммутатора **A** к коммутатору **B**.

Рисунок 68 Пример группирования портов – физические подключения



- 2 **Настройте статическую группу портов** – нажмите **Advanced Application > Link Aggregation > Link Aggregation Setting**. На этом экране активируйте группу портов **T1** и выберите порты, которые должны быть включены в эту группу, как показано на следующем рисунке. После этого нажмите **Apply**.

Рисунок 69 Пример группирования портов – экран настройки

Link Aggregation Setting Status LACP

Group ID	Active
T1	<input checked="" type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>
T5	<input type="checkbox"/>
T6	<input type="checkbox"/>

Port	Group
1	None
2	T1
3	T1
4	T1
5	T1
6	None
7	None
8	None

На этом настройка группы портов 1 (**T1**) завершена; переходить на какие-либо другие экраны не требуется.

Аутентификация портов

В данной главе описаны методы аутентификации IEEE 802.1x и по MAC-адресам.

16.1 Обзор аутентификации портов

Механизм аутентификации портов позволяет проверять права доступа клиентов к портам коммутатора с использованием внешнего сервера (сервера аутентификации). Данный коммутатор поддерживает следующие методы аутентификации портов:

- **IEEE 802.1x²** – предусматривает проверку прав доступа к портам на сервере аутентификации с использованием имени пользователя и пароля, предоставленных пользователем.
- **По MAC-адресам** – предусматривает проверку прав доступа к портам с использованием MAC-адреса и пароля пользователя.

Проверка прав пользователя в каждом из способов аутентификации осуществляется с использованием протокола RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139). Дополнительную информацию о настройках сервера RADIUS можно найти в [разд. 23.1.2 на стр. 202](#).



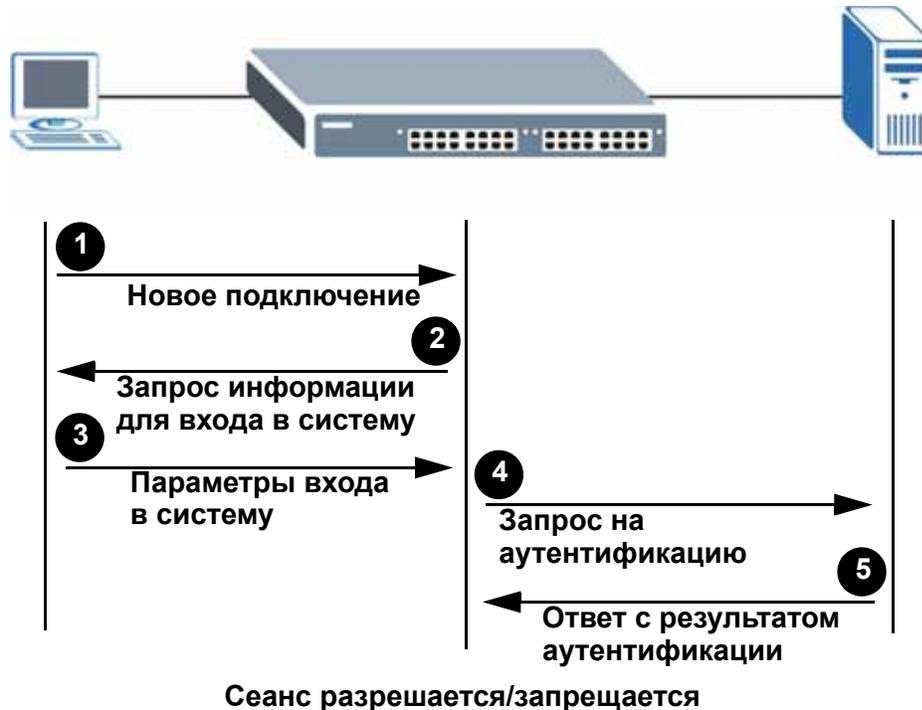
Если включить на одном и том же порту и аутентификацию по IEEE 802.1x, и аутентификацию по MAC-адресам, то коммутатор в первую очередь осуществляет аутентификацию по стандарту IEEE 802.1x. В случае невозможности осуществить аутентификацию пользователя по стандарту IEEE 802.1x доступ к порту будет запрещен.

2. На момент написания данного руководства стандарт IEEE 802.1x поддерживался не всеми операционными системами. Обратитесь к документации по операционной системе. Если операционная система не поддерживает стандарт 802.1x, может потребоваться установка программного обеспечения клиента 802.1x.

16.1.1 Аутентификация на основе IEEE 802.1x

Процесс проверки прав пользователя, подключающегося к порту с активированным механизмом аутентификации IEEE 802.1x, показан на следующем рисунке. Данный коммутатор запрашивает у клиента информацию для входа в систему в виде имени пользователя и пароля. После получения от клиента параметров входа в систему коммутатор отправляет запрос на аутентификацию на сервер RADIUS. Сервер RADIUS проверяет, обладает ли данный клиент правом доступа к данному порту.

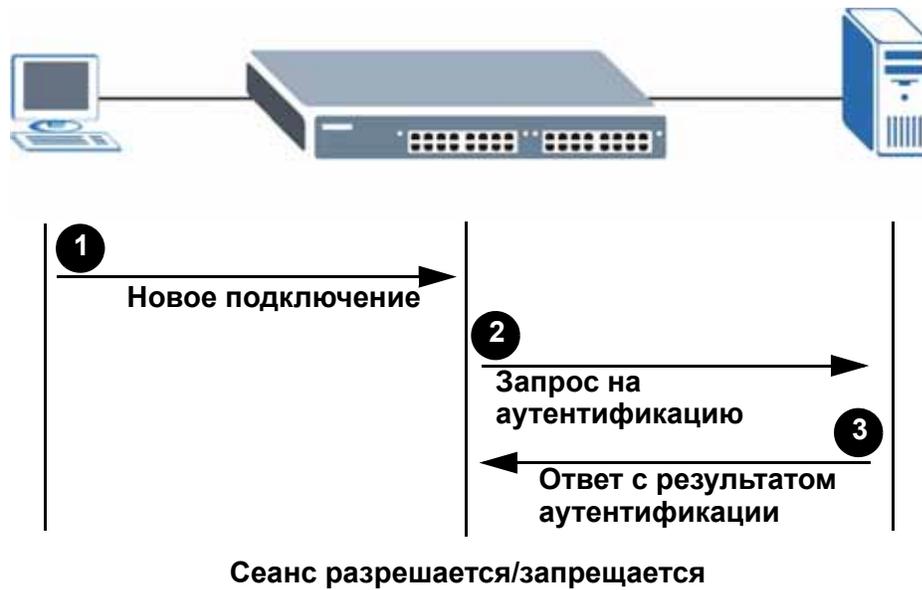
Рисунок 70 Процесс аутентификации на основе IEEE 802.1x



16.1.2 Аутентификация по MAC-адресам

Аутентификация по MAC-адресам работает практически так же, как и аутентификация по стандарту IEEE 802.1x. Основное различие заключается в том, что коммутатор не запрашивает у пользователя параметров входа. Параметрами входа являются MAC-адрес пользователя, подключающегося к порту коммутатора, а также пароль, настроенный на коммутаторе специально для аутентификации по MAC-адресам.

Рисунок 71 Процесс аутентификации по MAC-адресу



16.2 Настройка аутентификации портов

Чтобы включить аутентификацию портов, прежде всего необходимо активировать используемый метод или используемые методы аутентификации (как на коммутаторе, так и на портах), а затем настроить параметры сервера RADIUS на экране **Auth and Acct > Radius Server Setup**.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application > Port Authentication**.

Рисунок 72 Экран Advanced Application > Port Authentication



16.2.1 Включение функций безопасности стандарта IEEE 802.1x

С помощью данного экрана можно активировать функции безопасности стандарта IEEE 802.1x. На экране **Port Authentication** нажмите **802.1x**, чтобы отобразить показанный ниже экран настройки.

Рисунок 73 Экран Advanced Application > Port Authentication > 802.1x

Port	Active	Reauthentication	Reauthentication Timer
*	<input type="checkbox"/>	On	seconds
1	<input type="checkbox"/>	On	3600 seconds
2	<input type="checkbox"/>	On	3600 seconds
3	<input type="checkbox"/>	On	3600 seconds
4	<input type="checkbox"/>	On	3600 seconds
5	<input type="checkbox"/>	On	3600 seconds
6	<input type="checkbox"/>	On	3600 seconds
7	<input type="checkbox"/>	On	3600 seconds
8	<input type="checkbox"/>	On	3600 seconds

Поля экрана описаны в следующей таблице.

Таблица 41 Экран Advanced Application > Port Authentication > 802.1x

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы разрешить аутентификацию по стандарту 802.1x на коммутаторе. Примечание: Прежде чем приступить к настройке службы аутентификации по стандарту 802.1x на каждом порту, необходимо включить ее на коммутаторе.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы разрешить аутентификацию по стандарту 802.1x на этом порту. Прежде чем активировать аутентификацию по стандарту 802.1x на каждом порту, необходимо включить ее на коммутаторе.
Reauthentication	Укажите, требуется ли пользователю периодически вводить заново свое пользовательское имя и пароль, чтобы оставаться подключенным к порту.
Reauthentication Timer	Укажите, как часто клиенту требуется вводить заново свое имя пользователя и пароль, чтобы оставаться подключенным к порту.

Таблица 41 Экран Advanced Application > Port Authentication > 802.1x (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоа в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

16.2.2 Включение аутентификации по MAC-адресам

Данный экран используется для включения аутентификации по MAC-адресам. На экране **Port Authentication** нажмите на **MAC Authentication**, чтобы отобразить показанный ниже экран настройки.

Рисунок 74 Экран Advanced Application > Port Authentication > MAC Authentication

Port	Active
*	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

Поля экрана описаны в следующей таблице.

Таблица 42 Экран Advanced Application > Port Authentication > MAC Authentication

ПОЛЕ	ОПИСАНИЕ
Active	<p>Установите этот переключатель, чтобы разрешить аутентификацию по MAC-адресам на коммутаторе.</p> <p>Примечание: Прежде чем приступить к настройке аутентификации по MAC-адресам на каждом порту, необходимо включить ее на коммутаторе.</p>
Name Prefix	<p>Введите префикс имени, который будет добавляться ко всем MAC-адресам, отправляемым на сервер RADIUS для аутентификации. В поле можно ввести до 32 печатных символов ASCII.</p> <p>Если оставить это поле пустым, то на сервер RADIUS будет отправляться только MAC-адрес пользователя.</p>
Password	<p>Введите пароль, который коммутатор будет отправлять вместе с MAC-адресом пользователя на сервер RADIUS для аутентификации. В поле можно ввести до 32 печатных символов ASCII.</p>
Timeout	<p>Укажите период времени, по прошествии которого коммутатор разрешит пользователю с MAC-адресом, отвергнутым при аутентификации, повторить попытку аутентификации. Максимальное значение равно 3000 секунд.</p> <p>Когда пользователь не проходит аутентификацию по MAC-адресу, его MAC-адрес запоминается в таблице MAC-адресов с указанием статуса запрета. Указанный в данном поле период тайм-аута представляет собой время, в течение которого такой MAC-адрес будет находиться в таблице MAC-адресов; по прошествии этого времени запись удаляется. Если указать в этом поле значение тайм-аута 0, то удаление записей из таблицы MAC-адресов не производится.</p> <p>Примечание: В случае указания в поле Aging Time на экране Switch Setup меньшего значения оно имеет приоритет перед данным параметром. См. разд. 7.5 на стр. 81.</p>
Port	<p>В этом поле отображается номер порта.</p>
*	<p>С помощью этой строки можно настроить одновременно все порты. С помощью этой строки можно назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Active	<p>Установите этот переключатель, чтобы разрешить аутентификацию по MAC-адресам на этом порту. Прежде чем приступить к настройке аутентификации по MAC-адресам на каждом порту, необходимо включить ее на коммутаторе.</p>
Apply	<p>Нажмите Apply, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.</p>
Cancel	<p>Нажмите Cancel, чтобы начать настройку на этом экране заново.</p>

Средства безопасности портов

В данной главе описана настройка функций безопасности портов.

17.1 О средствах безопасности портов

Средства безопасности портов позволяют разрешить прохождение через порт коммутатора только пакетов с динамически полученными MAC-адресами и/или настроенными статическими MAC-адресами. Данный коммутатор может запомнить в общей сложности до 16 тыс. MAC-адресов, без ограничений на количество запоминаемых адресов на один порт (при условии, что общее количество не превышает 16 тыс.).

Для обеспечения максимальной безопасности порта необходимо отключить получение MAC-адресов и настроить для порта статический MAC-адрес (или MAC-адреса). Не рекомендуется отключать средства безопасности портов одновременно запоминанием MAC-адресов, так как это приведет к большому числу широковещательных пакетов. По умолчанию функция получения MAC-адресов остается активированной, даже если средства безопасности портов не включены.

17.2 Настройка средств безопасности портов

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application > Port Security**.

Рисунок 75 Экран Advanced Application > Port Security

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>

Apply Cancel

Поля экрана описаны в следующей таблице.

Таблица 43 Экран Advanced Application > Port Security

ПОЛЕ	ОПИСАНИЕ
Active	Установите данный переключатель, чтобы включить средства безопасности портов на коммутаторе.
Port	В этом поле отображается номер порта.
*	<p>Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Active	<p>Установите этот переключатель, чтобы включить средства безопасности для данного порта. Данный коммутатор пересылает пакеты, MAC-адрес(а) которых содержится в таблице MAC-адресов для этого порта. Пакеты с другими MAC-адресами отбрасываются.</p> <p>Снимите выделение с переключателя, если необходимо отключить эту функцию. Данный коммутатор будет пересылать все пакеты через этот порт.</p>
Address Learning	Функция получения MAC-адресов снижает объем исходящего широковещательного трафика. Чтобы получение MAC-адресов происходило для данного порта, порт должен быть активен и на нем должна быть включена функция получения адресов.

Таблица 43 Экран Advanced Application > Port Security (продолжение)

ПОЛЕ	ОПИСАНИЕ
Limited Number of Learned MAC Address	Это поле используется для ограничения допустимого количества (динамически) полученных MAC-адресов для порта. Например, если указать в этом поле для порта 2 значение «5», то в каждый момент времени одновременно получить доступ к порту 2 смогут лишь устройства с пятью полученными MAC-адресами. Шестому устройству придется ждать, пока один из этих пяти полученных MAC-адресов устареет. Параметр устаревания MAC-адресов можно определить в меню Switch Setup . Допустимый диапазон значений составляет от 0 до 16384. «0» означает отключение функции.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Классификация

В этой главе описывается настройка на коммутаторе функции классификации пакетов.

18.1 О классификации и управлении качеством обслуживания

Под управлением качеством обслуживания (QoS) понимается как способность сети доставлять данные с минимальной задержкой, так и применяемые в сети методы управления пропускной способностью. Если QoS не используется, то весь трафик имеет равную вероятность отбрасывания при возникновении перегрузок в сети. Это может привести к снижению производительности работы сети и сделать ее непригодной для критичных ко времени приложений, таких как видео по запросу.

При классификации трафик группируется на потоки данных по определенным критериям, таким как адрес источника, адрес назначения, номер порта источника, номер порта назначения и номер входящего порта. Например, можно настроить классификацию таким образом, чтобы в отдельный поток отбирался трафик порта определенного протокола (например, Telnet).

Настройка управления качеством обслуживания на коммутаторе позволяет сгруппировать и приоритезировать трафик приложений для точной настройки производительности сети. Настройка QoS включает в себя два отдельных этапа:

- 1 Настройка классификации для сортировки трафика между различными потоками.
- 2 Настройка правил политики, определяющих действия над классифицированными потоками трафика (настройка правил политики описана в [гл. 19 на стр. 167](#)).

18.2 Настройка классификации

Настройка классификации осуществляется на экране **Classifier**. После настройки классификации можно определить действия (политики), применяемые к отвечающим правилам трафику. Настройка правил политик описана в [гл. 19 на стр. 167](#).

Чтобы отобразить показанный ниже экран настройки, выберите в навигационной панели **Advanced Application > Classifier**.

Рисунок 76 Экран Advanced Application > Classifier

Поля экрана описаны в следующей таблице.

Таблица 44 Экран Advanced Application > Classifier

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить данное правило.
Name	Введите имя-описание данного правила, с помощью которого его можно идентифицировать.
Packet Format	Укажите формат пакетов. Возможные значения: All (все), 802.3 tagged (802.3 с тегами), 802.3 untagged (802.3 без тегов), Ethernet II tagged (Ethernet II с тегами) и Ethernet II untagged (Ethernet II без тегов). Значение 802.3 означает, что пакеты форматируются согласно стандартам IEEE 802.3. Значение Ethernet II означает, что пакеты форматируются согласно RFC 894, инкапсуляция Ethernet II.
Layer 2	В этом разделе приводятся поля, позволяющие настроить классификацию на уровне 2.
VLAN	Выберите Any , чтобы классифицировался трафик из любой сети VLAN, или выберите второй вариант и укажите идентификатор VLAN ID нужной сети в поле рядом.

Таблица 44 Экран Advanced Application > Classifier (продолжение)

ПОЛЕ	ОПИСАНИЕ
Priority	Выберите Any , чтобы классифицировался трафик с любым уровнем приоритета, или выберите второй вариант и укажите нужный уровень приоритета в поле рядом.
Ethernet Type	Выберите тип Ethernet, установив первый переключатель, или выберите вариант Other и введите номер типа Ethernet в шестнадцатеричном виде. Описание можно найти в табл. 46 на стр. 165 .
Source	
MAC Address	Выберите Any , чтобы правило применялось ко всем MAC-адресам. Чтобы указать определенный источник, выберите второй вариант и введите MAC-адрес в правильном формате (шесть пар шестнадцатеричных цифр).
Port	Введите номер порта, для которого будет действовать данное правило. Можно выбрать один из портов или все порты (Any).
Destination	
MAC Address	Выберите Any , чтобы правило применялось ко всем MAC-адресам. Чтобы указать определенный пункт назначения, выберите второй вариант и введите MAC-адрес в правильном формате (шесть пар шестнадцатеричных цифр).
Layer 3 В этом разделе приводятся поля, позволяющие настроить классификацию на уровне 3.	
DSCP	Выберите Any , чтобы классифицировался трафик с любым кодовым маркером DSCP, или выберите второй вариант и укажите номер DSCP (кодового маркера DiffServ) в диапазоне от 0 до 63 в поле рядом.
IP Protocol	Выберите тип IP-протокола, установив первый переключатель, или выберите вариант Other и введите номер протокола в десятичном виде. Дополнительную информацию можно найти в табл. 48 на стр. 165 . Для типа протокола TCP можно установить переключатель Establish Only . В этом случае коммутатор будет отбирать только пакеты, отправляемые для установления TCP-соединений.
Source	
IP Address/ Address Prefix	Введите IP-адрес источника в виде десятичных чисел, разделенных точками. Укажите префикс адреса, который представляет собой количество единиц в двоичной записи маски подсети. Маска подсети может быть представлена в виде 32-битного двоичного числа. Например, маску подсети «255.255.255.0» можно записать в двоичном виде как «11111111.11111111.11111111.00000000», и для нее количество единичных битов будет равно 24.
Socket Number	Примечание: Чтобы настроить номера сокетов, предварительно необходимо выбрать в поле IP Protocol значение UDP или TCP . Выберите Any , чтобы правило применялось для всех номеров портов протоколов TCP/UDP, или выберите второй вариант и введите номер порта протокола TCP/UDP.
Destination	
IP Address/ Address Prefix	Введите IP-адрес назначения в виде десятичных чисел, разделенных точками. Укажите префикс адреса, который представляет собой количество единиц в двоичной записи маски подсети. Маска подсети может быть представлена в виде 32-битного двоичного числа. Например, маску подсети «255.255.255.0» можно записать в двоичном виде как «11111111.11111111.11111111.00000000», и для нее количество единичных битов будет равно 24.

Таблица 44 Экран Advanced Application > Classifier (продолжение)

ПОЛЕ	ОПИСАНИЕ
Socket Number	Примечание: Чтобы настроить номера сокетов, предварительно необходимо выбрать в поле IP Protocol значение UDP или TCP . Выберите Any , чтобы правило применялось для всех номеров портов протоколов TCP/UDP, или выберите второй вариант и введите номер порта протокола TCP/UDP.
Add	Нажмите Add , чтобы добавить запись в итоговую таблицу ниже и сохранить изменения в оперативной памяти коммутатора. Эти настройки будут потеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clear	Нажмите Clear , чтобы вернуться к заводским настройкам.

18.3 Просмотр и редактирование настройки классификации

Чтобы просмотреть сводную информацию о настройках классификации, перейдите к итоговой таблице в нижней части экрана **Classifier**. Чтобы изменить настройки правила, нажмите на номере в поле **Index**.



В случае противоречия между двумя правилами приоритет имеет правило более высокого уровня.

Рисунок 77 Экран Advanced Application > Classifier: итоговая таблица

Index	Active	Name	Rule	Delete
1	Yes	Example	EtherType = IP; SrcMac = 00:50:ba:ad:4f:81; SrcPort = port 2;	<input type="checkbox"/>

Delete Cancel

Поля экрана описаны в следующей таблице.

Таблица 45 Экран Classifier: итоговая таблица

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер правила. Нажмите на этот номер, чтобы отредактировать правило.
Active	В этом поле отображается Yes , если правило активно, и No , если правило отключено.
Name	В этом поле отображается имя-описание для данного правила. Оно будет использоваться только для идентификации.
Rule	В этом поле отображаются сводные сведения по настройкам правила классификации.

Таблица 45 Экран Classifier: итоговая таблица

ПОЛЕ	ОПИСАНИЕ
Delete	Нажмите Delete , чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

Некоторые наиболее распространенные типы Ethernet и соответствующие номера протоколов приводятся в следующей таблице.

Таблица 46 Распространенные типы Ethernet и номера протоколов

ТИП ETHERNET	НОМЕР ПРОТОКОЛА
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Протоколом IP предусмотрено поле, называемое «Protocol», в котором указывается тип протокола IP. Некоторые наиболее распространенные типы протоколов и соответствующие номера протоколов приводятся в следующей таблице. Полный список можно найти по адресу: <http://www.iana.org/assignments/protocol-numbers>.

Таблица 47 Распространенные типы протокола IP и номера протоколов

ТИП ПРОТОКОЛА	НОМЕР ПРОТОКОЛА
ICMP	1
TCP	6
UDP	17
EGP	8
L2TP	115

Наиболее часто используемые порты протокола IP:

Таблица 48 Распространенные номера портов TCP и UDP

НОМЕР ПОРТА	НАЗВАНИЕ ПОРТА
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.4 Пример использования классификации

На следующем экране показан пример настройки классификации, в котором обнаруживается весь трафик от MAC-адреса 00:50:ba:ad:4f:81, поступающий через порт 2.

После настройки классификации можно настроить политику (на экране **Policy**), чтобы определить действия, выполняемые над этим потоком трафика.

Рисунок 78 Классификация: пример

The screenshot shows the 'Classifier' configuration window. It is divided into two main sections: Layer 2 and Layer 3. The 'Active' checkbox is checked. The 'Name' field contains 'Example'. The 'Packet Format' is set to 'All'. In the Layer 2 section, 'VLAN' is 'Any', 'Priority' is '0', and 'Ethernet Type' is 'All'. The 'Source' section is highlighted with a red oval: 'MAC Address' is selected with radio button, and the MAC address '00:50:ba:ad:4f:81' is entered in the field. 'Port' is set to '2'. The 'Destination' section has 'MAC Address' selected. In the Layer 3 section, 'DSCP' is 'Any', 'IP Protocol' is 'All', and 'Establish Only' is unchecked. The 'Source' and 'Destination' sections for Layer 3 have 'IP Address / Address Prefix' set to '0.0.0.0' and 'Socket Number' set to 'Any'. At the bottom, there are 'Add', 'Cancel', and 'Clear' buttons.

Правила политики

В данной главе описана настройка правил политики.

19.1 Обзор правил политики

С помощью классификации трафик делится на потоки в соответствии с установленными критериями (дополнительную информацию можно найти в [гл. 18 на стр. 161](#)). Правила политики обеспечивают надлежащую обработку потоков трафика в сети.

19.1.1 Дифференцированное обслуживание

Дифференцированное обслуживание (DiffServ) представляет собой модель на базе классов обслуживания (CoS), в которой пакеты маркируются таким образом, чтобы на пути следования маршрута на сетевых устройствах с поддержкой DiffServ они подвергались особой обработке на каждом конкретном переходе в зависимости от типа приложения и плотности трафика. Пакеты маркируются кодовыми маркерами DiffServ (DiffServ Code Points, DSCP), которые указывают на желаемый уровень обслуживания. Это позволяет промежуточным сетевым устройствам с поддержкой DiffServ обрабатывать пакеты различным образом в зависимости от маркера, без необходимости согласования путей или запоминания информации о состоянии для каждого потока. Кроме того, приложениям не требуется запрашивать конкретное обслуживание или выдавать предварительное уведомление о том, куда направляется трафик.

19.1.2 Маркер DSCP и обработка на каждом конкретном переходе

При использовании DiffServ в заголовок IP-пакетов добавляется новое поле DS (Differentiated Services), которое заменяет поле типа обслуживания ToS (Type of Service). Поле DS состоит из двухбитного неиспользуемого поля и 6-битного поля маркера DSCP, которое позволяет определить до 64 уровней обслуживания. Поле DS изображено на следующем рисунке.

Маркер DSCP обратно совместим с тремя битами приоритета в октете ToS, благодаря чему сетевое устройство с поддержкой ToS, но без поддержки DiffServ не будет конфликтовать с отображением маркера DSCP.

DSCP (6 бит)	Не используется (2 бита)
--------------	--------------------------

Значение DSCP определяет обработку при пересылке, так называемую обработку на каждом конкретном переходе (PHB, Per-Hop Behavior), которая осуществляется над каждым пакетом при прохождении по сети с поддержкой DiffServ. В зависимости от правила маркирования различные типы трафика могут подвергаться различным способам пересылки. Ресурсы могут быть распределены соответственно значениям DSCP и настроенным политикам.

19.2 Настройка правил политики

Прежде всего необходимо настроить классификацию на экране **Classifier**.

Дополнительную информацию можно найти в [разд. 18.2 на стр. 161](#).

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Applications > Policy Rule**.

Рисунок 79 Экран Advanced Application > Policy Rule

The screenshot shows the 'Policy Rule' configuration interface. It includes the following sections and fields:

- Active:** A checkbox to enable or disable the policy.
- Name:** A text input field for the policy name.
- Classifier(s):** A list box for selecting one or more classifiers.
- Parameters:**
 - General:** VLAN ID (text input), Egress Port (text input with '1' selected), Outgoing packet format for Egress port (radio buttons for Tag and Untag, with Tag selected), Priority (dropdown menu with '0' selected), DSCP (text input), and TOS (dropdown menu with '0' selected).
 - Metering:** Bandwidth (text input with 'kbps' unit), Out-of-Profile DSCP (text input).
- Action:**
 - Forwarding:** Radio buttons for No change (selected), Discard the packet, and Do not drop the matching frame previously marked for dropping.
 - Priority:** Radio buttons for No change (selected), Set the packet's 802.1 priority, Send the packet to priority queue, and Replace the 802.1 priority field with the IP TOS value.
 - Diffserv:** Radio buttons for No change (selected), Set the packet's TOS field, Replace the IP TOS field with the 802.1 priority value, and Set the Diffserv Codepoint field in the frame.
 - Outgoing:** Checkboxes for Send the packet to the mirror port, Send the packet to the egress port, Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port, and Set the packet's VLAN ID.
 - Metering:** A checkbox for Enable.
 - Out-of-profile action:** Checkboxes for Drop the packet, Change the DSCP value, Set Out-Drop Precedence, and Do not drop the matching frame previously marked for dropping.

At the bottom of the screen are three buttons: Add, Cancel, and Clear.

Поля экрана описаны в следующей таблице.

Таблица 49 Экран Advanced Application > Policy Rule

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить политику.
Name	Введите имя-описание для идентификации.
Classifier(s)	В этом поле отображаются активные правила классификации, настроенные на экране Classifier . Выберите правило классификации, к которому применяется данное правило политики. Чтобы выбрать несколько правил классификации, удерживайте при выборе нажатой клавишу [SHIFT].

Таблица 49 Экран Advanced Application > Policy Rule (продолжение)

ПОЛЕ	ОПИСАНИЕ
Parameters Настройки в следующих полях относятся к данной политике. Необходимо настроить только те поля, которые относятся в настроенным действиям в разделе Action .	
General	
VLAN ID	Укажите идентификационный номер VLAN.
Egress Port	Введите номер исходящего порта.
Outgoing packet format for Egress port	Выберите Tag , чтобы на указанном исходящем порту к пакетам добавлялся указанный идентификатор VID. В противном случае необходимо выбрать Untag .
Priority	Укажите уровень приоритета.
DSCP	Укажите значение DSCP (кодированного маркера DiffServ) в диапазоне от 0 до 63.
TOS	Укажите уровень приоритета типа обслуживания (TOS).
Metering	
	Имеется возможность настроить желаемую пропускную способность, выделяемую для потока трафика. Трафик, поступающий со скоростью сверх максимальной выделенной пропускной способности (в случаях перегрузки сети), называется внепрофильным трафиком.
Bandwidth	Укажите пропускную способность в килобитах в секунду (кбит/с). Введите значение в диапазоне от 1 до 1000000.
Out-of-Profile DSCP	Укажите значение DSCP (в диапазоне от 0 до 63), на которое должно заменяться значение DSCP у внепрофильного трафика.
Action Укажите действия, выполняемые коммутатором над соответствующим классифицированным потоком трафика.	
Forwarding	Выберите No change для пересылки пакетов. Выберите Discard the packet для отбрасывания пакетов. Выберите Do not drop the matching frame previously marked for dropping для сохранения кадров, ранее помеченных на отбрасывание.
Priority	Выберите No change , чтобы оставить приоритет кадров без изменения. Выберите Set the packet's 802.1 priority , чтобы заменить поле приоритета пакета по стандарту 802.1 на значение, указанное в поле Priority. Выберите Send the packet to priority queue , чтобы поместить пакеты в указанную очередь. Выберите Replace the 802.1 priority field with the IP TOS value , чтобы заменить поле приоритета пакета по стандарту 802.1 на значение, указанное в поле TOS .
Diffserv	Выберите No change , чтобы оставить поля TOS и/или DSCP пакетов без изменения. Выберите Set the packet's TOS field , чтобы установить для поля TOS значение, указанное в поле TOS . Выберите Replace the IP TOS with the 802.1 priority value , чтобы заменить поле TOS на значение, указанное в поле Priority . Выберите Set the Diffserv Codepoint field in the frame , чтобы установить для поля DSCP значение, указанное в поле DSCP .

Таблица 49 Экран Advanced Application > Policy Rule (продолжение)

ПОЛЕ	ОПИСАНИЕ
Outgoing	<p>Выберите Send the packet to the mirror port, чтобы передать пакет на зеркальный порт.</p> <p>Выберите Send the packet to the egress port, чтобы передать пакет на исходящий порт.</p> <p>Выберите Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port, чтобы передать на исходящий порт широковещательные, мультивещательные, DLF-кадры, а также помеченные на отбрасывание кадры и кадры CPU.</p> <p>Выберите Set the packet's VLAN ID, чтобы установить идентификатор VLAN пакета равным значению, указанному в поле VLAN ID.</p>
Metering	Выберите Enable , чтобы активировать ограничение пропускной способности для потоков трафика и затем настроить действия, выполняемые над внепрофильным трафиком.
Out-of-profile action	<p>Выберите действия, выполняемые над внепрофильным трафиком.</p> <p>Выберите Drop the packet для отбрасывания внепрофильного трафика.</p> <p>Выберите Change the DSCP value, чтобы заменить поле DSCP на значение, указанное в поле Out of profile DSCP.</p> <p>Выберите Set Out-Drop Precedence, чтобы пометить внепрофильный трафик и отбросить его в случае перегрузки сети.</p> <p>Выберите Do not drop the matching frame previously marked for dropping для постановки в очередь кадров, помеченных на отбрасывание.</p>
Add	Нажмите Add , чтобы добавить запись в итоговую таблицу ниже и сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clear	Нажмите Clear , чтобы вернуться к заводским настройкам.

19.3 Просмотр и редактирование настроек политики

Чтобы просмотреть сводную информацию о настройках политики, перейдите к итоговой таблице в нижней части экрана **Policy**. Чтобы изменить настройки правила, нажмите на номере в поле **Index**.

Рисунок 80 Экран Advanced Application > Policy Rule: итоговая таблица

Index	Active	Name	Classifier(s)	Delete
1	Yes	Test	Example,	<input type="checkbox"/>

Delete Cancel

Поля экрана описаны в следующей таблице.

Таблица 50 Политика: итоговая таблица

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается номер политики. Нажмите на этот номер, чтобы отредактировать политику.
Active	В этом поле отображается Yes , если политика активна, и No , если политика отключена.

Таблица 50 Политика: итоговая таблица (продолжение)

ПОЛЕ	ОПИСАНИЕ
Name	В этом поле отображается имя, назначенное для данной политики.
Classifier(s)	В этом поле отображаются имена правил классификации, к которым применяется данная политика.
Delete	Нажмите Delete , чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

19.4 Пример политики

На приведенном ниже рисунке показан пример экрана **Policy**, на котором настроена политика ограничения пропускной способности и отбрасывания внепрофильного трафика для потока трафика, классифицированного по правилу **Example** (см. [разд. 18.4](#) на стр. 166).

Рисунок 81 Пример политики

Policy

Active

Name

Classifier(s)

Parameters

VLAN ID

Egress Port

Outgoing packet format for Egress port Tag Untag

Priority

DSCP

TOS

General **Metering**

Bandwidth kbps

Out-of-Profile DSCP

Action

Forwarding

No change

Discard the packet

Do not drop the matching frame previously marked for dropping

Priority

No change

Set the packet's 802.1 priority

Send the packet to priority queue

Replace the 802.1 priority field with the IP TOS value

Diffserv

No change

Set the packet's TOS field

Replace the IP TOS field with the 802.1 priority value

Set the Diffserv Codepoint field in the frame

Outgoing

Send the packet to the mirror port

Send the packet to the egress port

Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port

Set the packet's VLAN ID

Metering

Enable

Out-of-profile action

Drop the packet

Change the DSCP value

Set Out-Drop Precedence

Do not drop the matching frame previously marked for dropping

Add Cancel Clear

Метод организации очередей

В данной главе описаны поддерживаемые методы организации очередей.

20.1 Обзор методов организации очередей

Организация очередей помогает решить проблему снижения производительности в случаях перегрузки сети. Для настройки алгоритмов организации очередей для исходящего трафика используется меню **Queuing Method**. Дополнительную информацию можно также найти в описании меню **Priority Queue Assignment** на экране **Switch Setup** и **802.1p Priority** на экране **Port Setup**.

Алгоритмы организации очередей позволяют коммутаторам поддерживать отдельные очереди для пакетов от каждого отдельного источника или потока, а также предотвращать присвоение всей пропускной способности одним источником.

20.1.1 Строгая очередь приоритетов (SP)

Алгоритм строгой очереди приоритетов SP обрабатывает очереди на основании только уровня приоритета. При поступлении трафика на коммутатор трафик с наивысшим уровнем приоритета (Q7) передается первым. Когда эта очередь заканчивается, начинает передаваться трафик со следующим уровнем приоритета Q6, пока эта очередь также не закончится, после чего начинает передаваться трафик с уровнем приоритета Q5, и так далее. Если очереди для трафика с высоким приоритетом никогда не заканчиваются, то трафик с низким приоритетом может не пройти через коммутатор. Алгоритм SPQ не может автоматически приспосабливаться к изменяющимся требованиям сети.

20.1.2 Взвешенная справедливая постановка в очередь (WFQ)

Алгоритм взвешенной справедливой постановки в очередь (WFQ) позволяет гарантировать для каждой очереди в случае перегрузки минимальную пропускную способность, определяемую весом (долей) очереди (числом, которое указывается в поле **Weight** – см. рис. 18.1). Алгоритм WFQ запускается только тогда, когда на порт приходит больше трафика, чем он может обработать. Очереди с большим весом получают более высокую гарантированную пропускную способность, чем очереди с малым весом. Этот механизм организации очереди эффективен потому, что он распределяет всю доступную пропускную способность между различными очередями трафика. По умолчанию

очередь Q0 имеет вес 1, очередь Q1 – вес 2, очередь Q2 – вес 3, и так далее. Гарантированная пропускная способность вычисляется следующим образом:

$$\frac{\text{Вес очереди}}{\text{Сумма весов очередей}} \times \text{Скорость порта}$$

Например, при настройках по умолчанию очередь Q0 на порту 1 получает гарантированную пропускную способность:

$$\frac{1}{1+2+3+4+5+6+7+8} \times 100 \text{ Мбит/с} = 3 \text{ Мбит/с}$$

20.1.3 Взвешенное циклическое обслуживание (WRR)

Алгоритм циклического обслуживания обрабатывает очереди по кругу и запускается только тогда, когда на порт приходит больше трафика, чем он может принять. Очереди выделяется некоторая доля пропускной способности вне зависимости от объема трафика, приходящего на этот порт. Затем эта очередь смещается в конец списка. Следующей очереди выделяется аналогичная доля пропускной способности, затем эта очередь тоже перемещается в конец списка; и так далее, в зависимости от количества используемых очередей. Алгоритм циклически повторяется, пока очередь не опустеет.

Алгоритм взвешенного циклического обслуживания (WRR) использует тот же метод, что и простое циклическое обслуживание, но он обрабатывает очереди на основе их уровня приоритета и веса очереди (число, которое вводится в поле **Weight**), а не фиксированной доли пропускной способности. Алгоритм WRR запускается только тогда, когда на порт приходит больше трафика, чем он может обработать. Очереди с большим весом обрабатываются быстрее, чем очереди с малым весом. Этот механизм организации очереди эффективен потому, что он распределяет всю доступную пропускную способность между различными очередями трафика и возвращается к очередям, которые еще не закончились.

20.2 Настройка метода организации очередей

Выберите в навигационной панели **Advanced Application > Queuing Method**.

Рисунок 82 Экран Advanced Application > Queuing Method

Port	Weight								GE Port SPQ Enable	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7		
*										None
1	1	2	3	4	5	6	7	8	-	
2	1	2	3	4	5	6	7	8	-	
3	1	2	3	4	5	6	7	8	-	
4	1	2	3	4	5	6	7	8	-	
5	1	2	3	4	5	6	7	8	-	
6	1	2	3	4	5	6	7	8	-	
7	1	2	3	4	5	6	7	8	-	

Поля экрана описаны в следующей таблице.

Таблица 51 Экран Advanced Application > Queuing Method

ПОЛЕ	ОПИСАНИЕ
Method	<p>Выберите SPQ (строгая очередь приоритетов), WFQ (взвешенная справедливая постановка в очередь) или WRR (взвешенное циклическое обслуживание).</p> <p>Алгоритм строгой очереди приоритетов обрабатывает очереди на основании только уровня приоритета. Когда опустошается очередь с наивысшим приоритетом, начинается обработка трафика в очереди со следующим уровнем приоритета. Самый высокий уровень приоритета – Q7, самый низкий – Q0.</p> <p>Алгоритм взвешенной справедливой постановки в очередь (WFQ) позволяет гарантировать для каждой очереди в случае перегрузки минимальную пропускную способность, определяемую весом (долей) очереди (числом, которое указывается в поле Weight). Очереди с большим весом получают более высокую гарантированную пропускную способность, чем очереди с малым весом.</p> <p>Алгоритм взвешенного циклического обслуживания обрабатывает очереди циклически в зависимости от их веса (число, которое вводится в поле веса Weight очереди). Очереди с большим весом обрабатываются быстрее, чем очереди с малым весом.</p>
FE Port SPQ Enable	<p>Данное поле используется только в случае выбора WFQ или WRR.</p> <p>Выберите очередь (от Q0 до Q7), начиная с которой (включительно) коммутатор будет использовать для портов Ethernet 10/100 Мбит/с алгоритм строгой очереди приоритетов. Например, если выбрать Q5, то коммутатор будет обслуживать трафик в очередях Q5, Q6 и Q7 с использованием алгоритма строгой очереди приоритетов.</p> <p>Чтобы в любом случае использовать для портов Ethernet 10/100 Мбит/с алгоритмы WFQ или WRR, выберите в данном поле значение None.</p>
Port	В этом поле отображается номер настраиваемого порта.

Таблица 51 Экран Advanced Application > Queuing Method (продолжение)

ПОЛЕ	ОПИСАНИЕ
*	<p>Настройки в этой строке применяются ко всем портам.</p> <p>Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Вес	В случае выбора метода WFQ или WRR в этих полях указываются веса очередей. Пропускная способность распределяется между очередями в зависимости от их веса.
GE Port SPQ Enable	<p>Данное поле используется только в случае выбора WFQ или WRR.</p> <p>Выберите очередь (от Q0 до Q7), начиная с которой (включительно) коммутатор будет использовать для портов Gigabit Ethernet алгоритм строгой очереди приоритетов. Например, если выбрать Q5, то коммутатор будет обслуживать трафик в очередях Q5, Q6 и Q7 с использованием алгоритма строгой очереди приоритетов.</p> <p>Чтобы в любом случае использовать для портов Gigabit Ethernet алгоритмы WFQ или WRR, выберите в данном поле значение None.</p>
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Стекирование VLAN

В данной главе описана настройка на коммутаторе стекирования VLAN. Более подробную информацию о виртуальных локальных сетях можно найти в главе о VLAN.

21.1 Обзор стекирования VLAN

С помощью стекирования VLAN провайдер услуг имеет возможность различать сети VLAN различных клиентов, даже если они имеют одинаковые (назначаемые клиентами) идентификаторы VLAN ID.

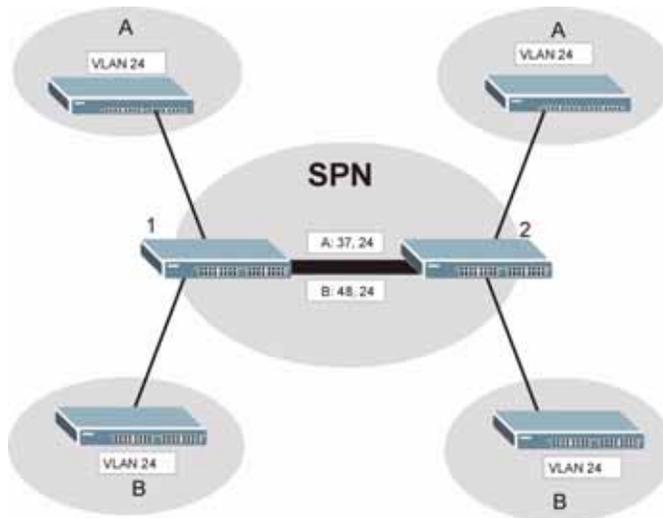
С помощью стекирования VLAN можно добавить внешний тег VLAN к кадрам с внутренними тегами IEEE 802.1Q при их поступлении в сеть. Посредством добавления тегов к уже имеющим теги кадрам (использования «двух тегов») провайдер услуг может управлять максимум 4 094 группами VLAN, каждая из которых может содержать до 4 094 клиентских сетей VLAN. Благодаря этому провайдер услуг может предоставлять дифференцированные услуги в зависимости от конкретной VLAN многим различным клиентам.

Клиентам провайдера услуг могут потребоваться различные виртуальные локальные сети для работы с несколькими приложениями. Клиенты провайдера услуг могут назначать свои собственные внутренние теги VLAN на портах для этих приложений. Каждому клиенту провайдер услуг может присвоить внешний тег VLAN. Таким образом, теги VLAN у различных клиентов не будут перекрываться, а трафик различных клиентов будет по-прежнему изолирован.

21.1.1 Пример стекирования VLAN

На приведенном ниже рисунке **A** и **B** являются клиентами провайдера услуг, использующими VPN-туннели между своими головными офисами и филиалами через сеть провайдера (SPN). Для своих групп VLAN оба клиента выбрали одинаковые теги VLAN. Провайдер услуг может разделить эти две сети VLAN в своей сети, добавляя тег 37 для клиента **A** и тег 48 для клиента **B** на граничном устройстве **1**, и затем удаляя эти теги на граничном устройстве **2** в момент выхода кадров из сети.

Рисунок 83 Пример стекирования VLAN



21.2 Роли портов при стекировании VLAN

Каждый из портов при стекировании VLAN может выполнять одну из трех «ролей»: **Normal** (обычный порт), **Access Port** (порт доступа) и **Tunnel** (туннель, только для гигабитных портов).

- Значение **Normal** соответствует «обычной» (без использования стекирования VLAN) коммутации кадров IEEE 802.1Q.
- Значение **Access Port** устанавливается для входящих портов на граничных устройствах провайдера услуг (1 и 2 на рисунке с примером стекирования VLAN). При этом входящие кадры обрабатываются как «не имеющие тегов», что дает возможность добавить второй тег VLAN (внешний тег VLAN).



На портах, для которых выбраны режимы **Normal** или **Access Port**, должно быть ОТКЛЮЧЕНО добавление тегов **Tx Tagging** для статических VLAN.

- Значение **Tunnel Port** (доступное только для гигабитных портов) устанавливается для исходящих портов на граничном устройстве сети провайдера услуг. Все принадлежащие клиенту сети VLAN могут быть агрегированы в одну VLAN провайдера услуг (с использованием внешнего тега VLAN, определенного по SP VID).



На портах, для которых выбран режим **Tunnel Port**, должно быть **ВКЛЮЧЕНО** добавление тегов **Tx Tagging** для статических VLAN.

21.3 Формат тега VLAN

Тег VLAN (при стекировании VLAN провайдером услуг или использовании клиентских сетей IEEE 802.1Q) включает в себя следующие три поля.

Таблица 52 Формат тега VLAN

Type	Priority	VID
------	----------	-----

Type представляет собой стандартный код типа Ethernet, который идентифицирует кадр и указывает, несет ли кадр информацию тега IEEE 802.1Q. **SP TPID** (идентификатор протокола тега провайдера услуг) представляет собой тип тега для стекирования VLAN провайдером услуг. Многие производители используют значения 0x8100 или 0x9100.

TPID (идентификатор протокола тега) представляет собой тег клиентской сети IEEE 802.1Q.

- Если порт при стекировании VLAN имеет роль **Access Port**, то коммутатор добавляет тег **SP TPID** ко всем входящим кадрам на граничных устройствах провайдера услуг (1 и 2 на рисунке с примером стекирования VLAN).
- Если порт при стекировании VLAN имеет роль **Tunnel**, то коммутатор добавляет тег **SP TPID** только к тем входящим кадрам на граничных устройствах провайдера услуг (1 и 2 на рисунке с примером стекирования VLAN), у которых **SP TPID** отличается от настроенного на коммутаторе. (Если **SP TPID** входящего кадра совпадает с настроенным на коммутаторе, то коммутатор тег не добавляет).

Priority определяется стандартом IEEE 802.1p и позволяет провайдерам услуг приоритезировать трафик в зависимости от класса обслуживания (CoS), оплаченного клиентом.

- На коммутаторе уровни приоритета для внутренних тегов IEEE 802.1Q настраиваются на экране **Port Setup**.
- «0» соответствует самому низкому приоритету, «7» – самому высокому.

VID представляет собой идентификатор VLAN ID. **SP VID** – это идентификатор VID для второго тега VLAN (провайдера услуг).

21.3.1 Формат кадра

Ниже показаны форматы кадра для кадра Ethernet без тега, для кадра с одним тегом 802.1Q (клиентским) и с двумя тегами 802.1Q (провайдера услуг).

Выделенные поля соответствуют настраиваемым на коммутаторе на экране **VLAN Stacking**.

Таблица 53 Формат кадра с одним и двумя тегами 802.11Q

						DA	SA	Len/ Etype	Data	FCS	Кадр Ethernet без тегов
			DA	SA	TPID	Priority	VID	Len/ Etype	Data	FCS	Кадр с клиентским тегом IEEE 802.1Q
DA	SA	SPTPID	Priority	VID	TPID	Priority	VID	Len/ Etype	Data	FCS	Кадр с двумя тегами

Таблица 54 Кадр 802.1Q

DA	Адрес назначения	Priority	Приоритет 802.1p
SA	Адрес источника	Len/ Etype	Длина и тип кадра Ethernet
(SP)TPID	Идентификатор протокола тега (провайдера услуг)	Data	Данные кадра
VID	VLAN ID	FCS	Контрольная последовательность кадра

21.4 Настройка стекирования VLAN

Чтобы отобразить следующий экран, нажмите **Advanced Applications > VLAN Stacking**.

Рисунок 84 Экран Advanced Application > VLAN Stacking

VLAN Stacking

Active

SP TPID 0x8100 Others (Hex)

Port	Role	SPVID	Priority
*	Normal	<input type="text"/>	0
1	Access Port	1	0
2	Access Port	1	0
3	Access Port	1	0
4	Access Port	1	0
5	Access Port	1	0
6	Access Port	1	0
7	Access Port	1	0
8	Access Port	1	0

Apply Cancel

Поля экрана описаны в следующей таблице.

Таблица 55 Экран Advanced Application > VLAN Stacking

ПОЛЕ	ОПИСАНИЕ
Active	Установите данный переключатель, чтобы включить на коммутаторе стекирование VLAN.
SP TPID	SP TPID представляет собой стандартный код типа Ethernet, идентифицирующий кадр и указывающий, несет ли кадр информацию тега IEEE 802.1Q. Выберите 0x8100 или 0x9100 из ниспадающего списка или выберите пункт Others и введите четырехзначное число в шестнадцатеричном виде в диапазоне от 0x0000 до 0xFFFF. 0x указывает на запись в шестнадцатеричном виде. Эти два символа не следует вводить в текстовое поле Others .
Port	Номер порта – определяет настраиваемый порт.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Role	Выберите Normal , чтобы коммутатор игнорировал получаемые (или передаваемые) через данный порт кадры с тегами стекирования VLAN. В этом случае настройки в SPVID и Priority игнорируются. Выберите Access Port , чтобы коммутатор добавлял тег SP TPID ко всем входящим кадрам, принимаемым через данный порт. Значение Access Port необходимо выбрать для входящих портов на границе сети провайдера услуг. Значение Tunnel Port (доступное только для гигабитных портов) устанавливается для исходящих портов на граничном устройстве сети провайдера услуг. Для поддержки стекирования VLAN на порту данный порт должен быть способен пропускать через себя кадры длиной 1526 байт (1522 байта + 4 байта для второго тега).
SPVID	SPVID представляет собой идентификатор VLAN провайдера услуг (внешний тег VLAN). Введите идентификатор провайдера услуг (в диапазоне от 1 до 4094) для кадров, принимаемых через данный порт. Дополнительную информацию об идентификаторах VLAN можно найти в гл. 8 на стр. 91 .
Priority	На коммутаторе уровни приоритета для внутренних тегов IEEE 802.1Q настраиваются на экране Port Setup . «0» соответствует самому низкому приоритету, «7» – самому высокому.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Мультивещание

В данной главе описана настройка различных функций мультивещания.

22.1 Обзор мультивещания

Обычно передача IP-пакетов происходит одним из двух способов: в режиме одноадресной передачи (от 1 отправителя к 1 получателю) или в режиме широковещания (от 1 отправителя всем получателям в сети). Мультивещание (или групповая передача) обеспечивает доставку IP-пакетов определенной группе хостов в сети.

Межсетевой протокол управления группами (Internet Group Management Protocol, IGMP) представляет собой протокол сетевого уровня, используемый для определения принадлежности к группе мультивещания. Для передачи пользовательских данных он не используется. Информацию о протоколе IGMP версий 1, 2 и 3 можно найти соответственно в стандартах RFC 1112, RFC 2236 и RFC 3376.

22.1.1 IP-адреса мультивещания

В IPv4 адрес мультивещания позволяет устройству отправлять пакеты определенной группе хостов (группе мультивещания) в отличной подсети. IP-адрес мультивещания определяет группу получателей трафика, а не конкретное получающее устройство. В качестве IP-адресов мультивещания используются IP-адреса класса D (от 224.0.0.0 до 239.255.255.255). Некоторые IP-адреса мультивещания зарезервированы IANA для особых целей (более подробную информацию можно найти на сайте IANA).

22.1.2 Фильтрация IGMP

Функция фильтрации IGMP позволяет определять, к каким группам IGMP сможет присоединиться абонент на порту. Таким образом можно контролировать предоставление функций мультивещания (например, рассылку контента) в зависимости от тарифных планов и типов подписки.

В коммутаторе можно настроить отбрасывание запросов присоединения к группам мультивещания на уровне отдельного порта, для чего необходимо настроить профиль фильтрации IGMP и привязать этот профиль к конкретному порту.

22.1.3 Отслеживание многоадресного трафика IGMP

Данный коммутатор может пассивно отслеживать IGMP-пакеты, передаваемые между маршрутизаторами/коммутаторами IP-мультивещания и хостами IP-мультивещания, чтобы получать информацию об участии в группах IP-мультивещания. Он проверяет IGMP-пакеты, проходящие через него, считывает информацию о регистрации в группах, а затем соответствующим образом настраивает мультивещание. Функция отслеживания многоадресного трафика (IGMP snooping) позволяет коммутатору автоматически считывать информацию о группах мультивещания, избавляя от необходимости настраивать их вручную.

Данный коммутатор направляет мультивещательный трафик, предназначенный для групп мультивещания (которые были выявлены функцией отслеживания многоадресного трафика IGMP или введены вручную), на порты, являющиеся членами соответствующей группы. Функция отслеживания многоадресного трафика IGMP не создает дополнительного сетевого трафика, что позволяет значительно снизить объем мультивещательного трафика, проходящего через коммутатор.

22.1.4 Отслеживание многоадресного трафика IGMP и сети VLAN

Данный коммутатор может отслеживать многоадресный трафик IGMP максимум в 16 виртуальных локальных сетях VLAN. На коммутаторе можно настроить режим автоматического получения информации об участии в группе мультивещания для любых сетей VLAN. При этом коммутатор будет выполнять отслеживание многоадресного трафика IGMP в первых 16 виртуальных локальных сетях VLAN, от которых были получены пакеты IGMP. Такой режим называется автоматическим (auto). Кроме того, можно указать конкретные виртуальные локальные сети VLAN, для которых необходимо выполнять отслеживание многоадресного трафика IGMP. Такой режим называется фиксированным (fixed). В фиксированном режиме коммутатор получает информацию об участии в группах мультивещания только в таких виртуальных локальных сетях VLAN, которые были явным образом добавлены как VLAN отслеживания многоадресного трафика IGMP.

22.2 Состояние мультивещания

Чтобы отобразить следующий экран, нажмите **Advanced Applications > Multicast**. На этом экране отображается информация о группах мультивещания. Более подробную информацию о мультивещании можно найти в [разд. 22.1 на стр. 185](#).

Рисунок 85 Экран Advanced Application > Multicast



Multicast Status		Multicast Setting	
Index	VID	Port	Multicast Group

Поля экрана описаны в следующей таблице.

Таблица 56 Экран Multicast Status

ПОЛЕ	ОПИСАНИЕ
Index	Порядковый номер записи.
VID	В этом поле отображается идентификатор VLAN-сети мультивещания.
Port	В этом поле отображается номер порта, принадлежащего группе мультивещания.
Multicast Group	В этом поле отображаются IP-адреса группы мультивещания.

22.3 Настройка мультивещания

Чтобы отобразить показанный ниже экран, нажмите **Advanced Applications > Multicast > Multicast Setting**. Более подробную информацию о мультивещании можно найти в [разд. 22.1 на стр. 185](#).

Рисунок 86 Экран Advanced Application > Multicast > Multicast Setting

Multicast Setting Multicast Status IGMP Snooping VLAN IGMP Filtering Profile MVR

IGMP Snooping

Active

Host Timeout

Leave Timeout

802.1p Priority

IGMP Filtering

Active

Unknown Multicast Frame Flooding Drop

Reserved Multicast Group Flooding Drop

Port	Immed. Leave	Group Limited	Max Group Num.	IGMP Filtering Profile	IGMP Querier Mode
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Default	Auto
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto

Apply Cancel

Поля экрана описаны в следующей таблице.

Таблица 57 Экран Advanced Application > Multicast > Multicast Setting

ПОЛЕ	ОПИСАНИЕ
IGMP Snooping	Данные параметры позволяют настроить отслеживание многоадресного трафика IGMP.
Active	Выбор Active активирует отслеживание многоадресного трафика IGMP, при котором трафик группы мультивещания пересылается только на порты, входящие в соответствующую группу.
Host Timeout	Укажите время в секундах (от 1 до 16 711 450), по истечении которого коммутатор удаляет запись об участии в группе IGMP при отсутствии сообщений Report от порта.
Leave Timeout	Введите значение тайм-аута Leave для IGMP в секундах (от 1 до 16 711 450). Он определяет время, которое коммутатор выжидает после получения IGMP-сообщения Leave от хоста перед удалением записи об участии в группе IGMP.
802.1p Priority	Выберите приоритет (0-7), который устанавливается коммутатором для исходящих управляющих пакетов IGMP. Выбор No-Change оставляет приоритет без изменения.
IGMP Filtering	<p>Выбор Active активирует функцию фильтрации IGMP, с помощью которой можно определять, к каким группам IGMP сможет присоединяться абонент на порту.</p> <p>Примечание: При включении фильтрации IGMP необходимо создать и назначить профили фильтрации IGMP тем портам, которым необходимо разрешить присоединение к группам мультивещания.</p>
Unknown Multicast Frame	Выберите действие, выполняемое коммутатором при получении неизвестного кадра мультивещания. Drop – отбрасывание кадра. Flooding – пересылка кадра на все порты.
Reserved Multicast Group	Адреса мультивещания (в диапазоне с 224.0.0.0 по 224.0.0.255) зарезервированы для использования в локальном масштабе. Например, 224.0.0.1 предназначен для всех хостов в данной подсети, 224.0.0.2 – для всех маршрутизаторов мультивещания в данной подсети и т.д. Пакеты с IP-адресами назначения из данного диапазона маршрутизатором не пересылаются. Дополнительную информацию можно найти на сайте IANA. Выберите действие, выполняемое коммутатором при получении кадра с зарезервированным адресом мультивещания. Drop – отбрасывание кадра. Flooding – пересылка кадра на все порты.
Port	В этом поле отображается номер порта.
*	<p>Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта.</p> <p>Примечание: Изменения в данной строке сразу же копируются на все порты.</p>
Immed. Leave	<p>Выбор данной опции заставляет коммутатор удалять данный порт из дерева мультивещания сразу же при получении через данный порт Leave-сообщения протокола IGMP версии 2.</p> <p>Эту опцию следует выбирать лишь в том случае, когда к порту подключен только один хост.</p>

Таблица 57 Экран Advanced Application > Multicast > Multicast Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
Group Limited	Выбор данной опции позволяет ограничить число групп мультивещания, к которым разрешено присоединиться данному порту.
Max Group Num.	Введите число групп мультивещания, к которым разрешено присоединиться данному порту. После регистрации порта в указанном количестве групп мультивещания все последующие Join-сообщения IGMP от данного порта отбрасываются.
IGMP Filtering Profile	Выберите имя профиля фильтрации IGMP, который будет использоваться для данного порта. Значение Default запрещает порту присоединение к любым группам мультивещания. Создание профилей фильтрации IGMP осуществляется на экране Multicast > Multicast Setting > IGMP Filtering Profile .
IGMP Querier Mode	Query-порт IGMP коммутатор рассматривает в качестве порта, к которому подключен маршрутизатор (или сервер) мультивещания IGMP. Join- и Leave-пакеты IGMP коммутатор направляет на Query-порт IGMP. Значение Auto заставляет коммутатор назначать порту статус Query-порта IGMP при получении Query-пакетов IGMP. Значение Fixed заставляет коммутатор постоянно использовать данный порт в качестве Query-порта IGMP. Данное значение следует выбрать в том случае, когда к порту подключается сервер мультивещания IGMP. Значение Edge заставляет коммутатор отменить для данного порта статус Query-порта IGMP. Данный коммутатор не сохраняет каких-либо записей о подключении маршрутизатора IGMP к данному порту. Join- и Leave-пакеты IGMP на этот порт коммутатором не пересылаются.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

22.4 VLAN отслеживания многоадресного трафика IGMP

Выберите в навигационной панели **Advanced Applications > Multicast**. Нажмите на ссылку **Multicast Setting** и затем на **IGMP Snooping VLAN**, чтобы отобразить показанный ниже экран. Дополнительную информацию о VLAN отслеживания многоадресного трафика IGMP можно найти в [разд. 22.1.4 на стр. 186](#).

Рисунок 87 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

Поля экрана описаны в следующей таблице.

Таблица 58 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

ПОЛЕ	ОПИСАНИЕ
Mode	<p>Выберите auto, чтобы коммутатор автоматически получал информацию об участии в группе мультивещания для любых сетей VLAN.</p> <p>Выберите fixed, чтобы коммутатор получал информацию об участии в группе мультивещания только для указанных ниже сетей VLAN.</p> <p>Как в автоматическом режиме auto, так и в фиксированном режиме fixed коммутатор способен получить информацию максимум о 16 виртуальных локальных сетях VLAN (включая максимум три сети VLAN, настроенные на экране MVR). Так, если на экране MVR была настроена одна VLAN-сеть мультивещания, на данном экране можно настроить не более 15 сетей VLAN.</p> <p>Данный коммутатор отбрасывает любые управляющие сообщения IGMP, которые не принадлежат одной из этих 16 сетей VLAN.</p> <p>Примечание: Предварительно необходимо включить отслеживание многоадресного трафика IGMP на экране Multicast Setting.</p>
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
VLAN	В данном разделе можно добавить сети VLAN, для которых коммутатор будет осуществлять отслеживание многоадресного трафика IGMP.
Name	Введите имя-описание VLAN, с помощью которого ее можно идентифицировать.
VID	<p>Введите идентификатор статической VLAN; допустимое значение находится в диапазоне от 1 до 4094.</p> <p>Примечание: Не допускается использовать тот же идентификатор VLAN ID, что и на экране MVR.</p>

Таблица 58 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите Add , чтобы добавить запись в итоговую таблицу ниже и сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы сбросить поля к предыдущим значениям.
Clear	Нажатие на данную кнопку позволяет очистить поля.
Index	Номер записи VLAN отслеживания многоадресного трафика IGMP в таблице.
Name	В этом поле отображается имя-описание группы VLAN.
VID	В этом поле отображается идентификационный номер группы VLAN.
Delete	В столбце Delete установите переключатели правил, которые нужно удалить, затем нажмите кнопку Delete .
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

22.5 Профиль фильтрации IGMP

Профиль фильтрации IGMP определяет диапазон групп мультивещания, к которым могут присоединиться подключенные к коммутатору пользователи. Профиль содержит диапазон IP-адресов мультивещания, к которым необходимо разрешить подключение пользователей. Профили назначаются конкретным портам (на экране **Multicast Setting**). Подключающиеся через эти порты пользователи могут присоединяться к группам мультивещания, указанным в профиле. Каждому порту может быть назначен только один профиль. Один и тот же профиль допускается назначать нескольким портам.

Чтобы отобразить показанный ниже экран, нажмите **Advanced Applications > Multicast > Multicast Setting > IGMP Filtering Profile**.

Рисунок 88 Экран Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

The screenshot displays the 'IGMP Filtering Profile' configuration interface. At the top, there's a header with 'IGMP Filtering Profile' and 'Multicast Setting'. Below this is a 'Profile Setup' section containing three input fields: 'Profile Name', 'Start Address' (pre-filled with 224.0.0.0), and 'End Address' (pre-filled with 224.0.0.0). Underneath these fields are 'Add' and 'Clear' buttons. A table below lists existing profiles. The table has columns for 'Profile Name', 'Start Address', 'End Address', 'Delete Profile', and 'Delete Rule'. One profile named 'Default' is shown with 'Start Address' 0.0.0.0, 'End Address' 0.0.0.0, and checkboxes for 'Delete Profile' and 'Delete Rule'. At the bottom of the screen are 'Delete' and 'Cancel' buttons.

Поля экрана описаны в следующей таблице.

Таблица 59 Экран Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

ПОЛЕ	ОПИСАНИЕ
Profile Name	Введите имя-описание профиля, с помощью которого его можно идентифицировать. Чтобы настроить дополнительные правила для уже добавленного профиля, необходимо ввести имя профиля и указать другие диапазоны IP-адресов мультивещания.
Start Address	Введите начальный адрес диапазона IP-адресов мультивещания, который необходимо включить в профиль фильтрации IGMP.
End Address	Введите конечный адрес диапазона IP-адресов мультивещания, который необходимо включить в профиль фильтрации IGMP. Чтобы добавить единственный IP-адрес мультивещания, укажите его и в поле Start Address , и в поле End Address .
Add	Нажмите Add , чтобы сохранить профиль в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Clear	Нажмите Clear , чтобы вернуться к заводским настройкам.
Profile Name	В этом поле отображается имя-описание профиля.
Start Address	В этом поле отображается начальный адрес диапазона IP-адресов мультивещания.
End Address	В этом поле отображается конечный адрес диапазона IP-адресов мультивещания.
Delete	Чтобы удалить профиль и все связанные с ним правила, выберите нужный профиль в столбце Delete Profile и нажмите на кнопку Delete . Чтобы удалить правило или правила из профиля, выберите нужные правила в столбце Delete Rule и нажмите на кнопку Delete .
Cancel	Нажатие на кнопку Cancel снимает выделения с переключателей в столбцах Delete Profile/Delete Rule .

22.6 Обзор MVR

Механизм регистрации VLAN-сети мультивещания (Multicast VLAN Registration, MVR) предназначен для случаев, когда требуется передавать мультивещательный трафик через Ethernet-сеть провайдера услуг, имеющую конфигурацию кольца (например, для приложений «мультимедиа по требованию» – MoD).

MVR позволяет определить одну VLAN-сеть мультивещания, которая будет доступна различным абонентским сетям VLAN в сети. Даже изолированные по различным абонентским сетям VLAN устройства могут подписываться и отписываться от потока мультивещания во VLAN-сети мультивещания. Благодаря этому обеспечивается оптимальное использование пропускной способности за счет предотвращения дублирования мультивещательного трафика в абонентских сетях VLAN, а также упрощается управление группами мультивещания.

MVR реагирует только на управляющие Join- и Leave-запросы IGMP от групп мультивещания, которые были настроены в MVR. Join- и Leave-запросы от других групп мультивещания управляются отслеживанием IGMP.

Пример сети показан на следующем рисунке. Информация об абонентских сетях VLAN (1, 2 и 3) скрыта от сервера потокового мультимедиа S. Кроме того, информация о VLAN-сети мультивещания видима только коммутатору и серверу S.

Рисунок 89 Пример сети с поддержкой MVR



22.6.1 Типы портов MVR

В MVR портом источника называется порт коммутатора, который отправляет и принимает трафик мультивещания из VLAN-сети мультивещания, тогда как порт приемника может только принимать трафик мультивещания. После настройки на коммутаторе создается таблица пересылки, которая соотносит поток мультивещания с соответствующей группой мультивещания.

22.6.2 Режимы MVR

Для коммутатора можно выбрать либо динамический режим, либо режим совместимости MVR.

В динамическом режиме коммутатор отправляет Leave- и Join-сообщения IGMP на другие устройства мультивещания (такие как маршрутизаторы или серверы мультивещания) во VLAN-сети мультивещания. Благодаря этому устройства мультивещания могут обновлять таблицу пересылки мультивещательного трафика и включать или отключать пересылку трафика мультивещания на порты приемников.

В режиме совместимости коммутатор не пересылает никаких запросов IGMP. В этом случае настройки пересылки на устройствах мультивещания во VLAN-сети мультивещания необходимо устанавливать вручную.

22.6.3 Как работает механизм MVR

Приведенный ниже рисунок иллюстрирует пример с мультивещанием телевизионного контента, когда абонентское устройство (такое как компьютер) в сети VLAN 1 принимает через коммутатор трафик мультивещания от сервера потокового мультимедиа S. Через порт, настроенный на коммутаторе в качестве порта приемника, возможно подключение нескольких абонентских устройств.

При выборе абонентом телевизионного канала компьютер **A** отправляет на коммутатор IGMP-запрос на присоединение к соответствующей группе мультивещания. Если IGMP-запрос соответствует одному из настроенных на коммутаторе адресов групп мультивещания MVR, в таблице пересылки коммутатора создается запись. В ней абонентская VLAN включается в список пунктов назначения для пересылки указанного трафика мультивещания.

Если абонент переключается на другой канал или выключает компьютер, на коммутатор направляется Leave-сообщение IGMP для выхода из группы мультивещания. Данный коммутатор направляет запрос в сеть VLAN 1 через порт приемника (в данном случае это порт каскадирования коммутатора). Если к данному порту в той же абонентской VLAN подключено еще хотя бы одно абонентское устройство, порт приемника по-прежнему останется в списке пунктов назначения для пересылки трафика мультивещания. В противном случае коммутатор удаляет порт приемника из таблицы пересылки.

Рисунок 90 Пример с мультивещанием телевидения посредством MVR



22.7 Общая настройка MVR

Создать VLAN-сети мультивещания и выбрать для каждой VLAN-сети мультивещания порты приемников и порт источника можно на экране **MVR**. Чтобы отобразить показанный ниже экран, нажмите **Advanced Applications > Multicast > Multicast Setting > MVR**.



Данный коммутатор позволяет определить максимум три VLAN-сети мультивещания и максимум 256 правил.



При создании на данном экране VLAN-сети мультивещания коммутатор автоматически создает статическую VLAN (с тем же идентификатором VID).

Рисунок 91 Экран Advanced Application > Multicast > Multicast Setting > MVR

The screenshot shows the MVR configuration interface. At the top, there are tabs for 'MVR', 'Multicast Setting', and 'Group Configuration'. The configuration fields are as follows:

- Active:** A checkbox that is currently unchecked.
- Name:** An empty text input field.
- Multicast VLAN ID:** An empty text input field.
- 802.1p Priority:** A dropdown menu currently set to '0'.
- Mode:** Two radio buttons, 'Dynamic' (selected) and 'Compatible'.

Below the configuration fields is a table for port configuration:

Port	Source Port	Receiver Port	None	Tagging
*		None		<input type="checkbox"/>
1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
6	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
7	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
8	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

At the bottom of the table, there are 'Add' and 'Cancel' buttons. Below the table is a summary table with columns: VLAN, Active, Name, Mode, Source Port, Receiver Port, 802.1p, and Delete. At the very bottom, there are 'Delete' and 'Cancel' buttons.

Поля экрана описаны в следующей таблице.

Таблица 60 Экран Advanced Application > Multicast > Multicast Setting > MVR

ПОЛЕ	ОПИСАНИЕ
Active	Выберите данный переключатель для включения MVR, чтобы использовать одну единственную VLAN-сеть мультивещания для различных абонентских VLAN в сети.
Name	Введите имя-описание (до 32 отображаемых ASCII-символов), по которому можно идентифицировать эту запись.
Multicast VLAN ID	Введите идентификатор сети VLAN (от 1 до 4094) для VLAN-сети мультивещания.
802.1p Priority	Выберите приоритет (0-7), на который коммутатор заменяет приоритет в исходящих управляющих пакетах IGMP (принадлежащих к данной VLAN-сети мультивещания).
Mode	Укажите режим MVR для коммутатора. Можно выбрать значения Dynamic (динамический) и Compatible (режим совместимости). Dynamic – сообщения IGMP отправляются на все порты источников MVR во VLAN-сети мультивещания. Compatible – сообщения IGMP коммутатором не отправляются.
Port	В этом поле отображается номер порта коммутатора.

Таблица 60 Экран Advanced Application > Multicast > Multicast Setting > MVR

ПОЛЕ	ОПИСАНИЕ
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Source Port	Выберите данную опцию, чтобы назначить данный порт в качестве порта источника MVR, который осуществляет отправку и прием трафика мультивещания. Все порты источников должны принадлежать к одной VLAN-сети мультивещания.
Receiver Port	Выберите данную опцию, чтобы назначить данный порт в качестве порта приемника MVR, который только принимает трафик мультивещания.
None	Выберите данную опцию, если данный порт не участвует в механизме MVR. Через такой порт трафик мультивещания MVR не передается и не принимается.
Tagging	Выберите данный переключатель, если ко всем передаваемым через порт исходящим кадрам должен добавляться тег идентификатора VLAN.
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
VLAN	В этом поле отображается идентификатор VLAN-сети мультивещания.
Active	Данное поле показывает, включена ли поддержка группы мультивещания.
Name	В этом поле отображается имя-описание для данной настройки.
Mode	В этом поле отображается режим MVR.
Source Port	В этом поле отображаются номера портов источников.
Receiver Port	В этом поле отображаются номера портов приемников.
802.1p	В этом поле отображается уровень приоритета.
Delete	Чтобы удалить VLAN-сети мультивещания, выберите нужные сети в столбце Delete и нажмите на кнопку Delete .
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

22.8 Настройка группы MVR

Данные мультивещания, направляемые в группу мультивещания, могут принимать все порты источников и порты приемников, принадлежащие группе мультивещания.

IP-адреса группы мультивещания MVR настраиваются на экране **Group Configuration**. Нажмите на ссылку **Group Configuration** на экране **MVR**.



Порт может принадлежать нескольким VLAN-сетям мультивещания. Однако, IP-адреса различных групп мультивещания не должны перекрываться.

Рисунок 92 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

Поля экрана описаны в следующей таблице.

Таблица 61 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

ПОЛЕ	ОПИСАНИЕ
Multicast VLAN ID	Выберите из ниспадающего списка идентификатор VLAN-сети мультивещания (настроенный на экране MVR).
Name	Введите имя-описание для идентификации.
Start Address	Введите начальный IP-адрес группы мультивещания в виде десятичных чисел, разделенных точками. Более подробную информацию об IP-адресах мультивещания можно найти в разд. 22.1.1 на стр. 185 .
End Address	Введите конечный IP-адрес группы мультивещания в виде десятичных чисел, разделенных точками. Если в группу мультивещания необходимо внести только один адрес, введите в это поле тот же IP-адрес, что и в поле Start Address . Более подробную информацию об IP-адресах мультивещания можно найти в разд. 22.1.1 на стр. 185 .
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
MVLAN	В этом поле отображается идентификатор VLAN-сети мультивещания.
Name	В этом поле отображается имя-описание для данной настройки.
Start Address	В этом поле отображается начальный IP-адрес группы мультивещания.
End Address	В этом поле отображается конечный IP-адрес группы мультивещания.

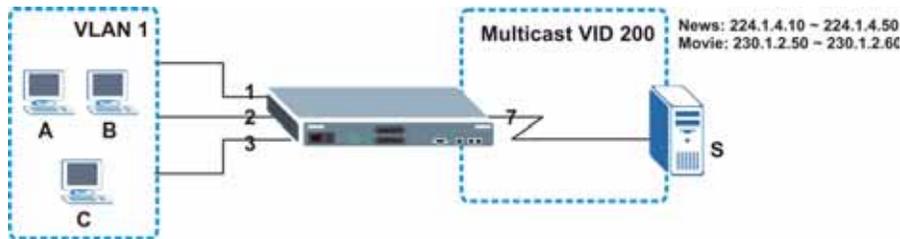
Таблица 61 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration (продолжение)

ПОЛЕ	ОПИСАНИЕ
Delete	Для удаления из таблицы выбранных записей выберите Delete Group и нажмите Delete .
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей в таблице.

22.8.1 Пример настройки MVR

На приведенном ниже рисунке показан пример сети, в которой порты 1, 2 и 3 коммутатора принадлежат VLAN 1. Кроме того, порт 7 принадлежит к группе мультивещания с идентификатором VID 200 для получения трафика мультивещания (каналы **News** и **Movie**) от удаленного сервера потокового мультимедиа, S. Компьютеры A, B и C в сети VLAN 1 могут принимать трафик.

Рисунок 93 Пример настройки MVR



Для определения настроек MVR на коммутаторе необходимо создать группу мультивещания на экране **MVR** и назначить порты приемников и источников.

Рисунок 94 Пример настройки MVR

Port	Source Port	Receiver Port	None	Tagging
*		None		<input type="checkbox"/>
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
6	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
8	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

Чтобы коммутатор пересылал трафик группы мультивещания абонентам, необходимо определить настройки группы мультивещания на экране **Group Configuration**. На следующем рисунке показан пример настройки двух групп мультивещания (**News** и **Movie**) для VLAN-сети мультивещания 200.

Рисунок 95 Пример настройки групп MVR

Group Configuration MVR

Multicast VLAN ID: 200

Name	Start Address	End Address
Movie	230.1.2.50	230.1.2.60

Add Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200	News	224.1.4.10	224.1.4.50	<input type="checkbox"/>	<input type="checkbox"/>

Delete Cancel

Рисунок 96 Пример настройки групп MVR

Group Configuration MVR

Multicast VLAN ID: 200

Name	Start Address	End Address
	0.0.0.0	0.0.0.0

Add Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200	Movie	230.1.2.50	230.1.2.60	<input type="checkbox"/>	<input type="checkbox"/>
	News	224.1.4.10	224.1.4.50	<input type="checkbox"/>	<input type="checkbox"/>

Delete Cancel

Аутентификация и учет

В данной главе описана настройка функций аутентификации и учета на коммутаторе.

23.1 Аутентификация, авторизация и учет

Аутентификацией называется процесс идентификации пользователя и проверки его прав доступа к коммутатору. Данный коммутатор позволяет проводить аутентификацию пользователей с использованием учетных записей, настроенных в самом коммутаторе. Кроме того, коммутатор позволяет использовать внешний сервер аутентификации в целях аутентификации большого количества пользователей.

Авторизацией называется процесс определения действий, которые допустимо выполнять пользователю. Различным пользовательским учетным записям могут быть назначены более высокие или более низкие уровни привилегий. Например, у пользователя А может быть право на создание новых учетных записей на коммутаторе, тогда как у пользователя В такого права не будет. Авторизация пользователей может осуществляться коммутатором с использованием учетных записей, настроенных на самом коммутаторе, или с использованием внешнего сервера в целях авторизации большого количества пользователей.

Учетом называется процесс регистрации действий пользователей. Данный коммутатор позволяет отслеживать вход пользователей, выход пользователей, выполняемые ими команды и другие действия с использованием внешнего сервера. В рамках учета могут также регистрироваться системные действия, такие как время загрузки и выключения коммутатора.

Внешние серверы, выполняющие функции аутентификации, авторизации и учета, сокращенно называются серверами AAA. В качестве внешних серверов аутентификации, авторизации и учета данный коммутатор поддерживает серверы RADIUS (Remote Authentication Dial-In User Service, см. [разд. 23.1.2 на стр. 202](#)) и TACACS+ (Terminal Access Controller Access-Control System Plus, см. [разд. 23.1.2 на стр. 202](#)).

Рисунок 97 Сервер AAA



23.1.1 Локальные учетные записи пользователей

Локальное хранение профилей пользователей на коммутаторе дает коммутатору возможность обходиться при аутентификации и авторизации пользователей без внешнего сервера AAA в сети. Однако, возможное количество пользователей при таком способе аутентификации ограничено (см. [гл. 30 на стр. 269](#)).

23.1.2 RADIUS и TACACS+

RADIUS и TACACS+ представляют собой протоколы безопасности, которые используются для аутентификации пользователей путем обращения к внешнему серверу вместо внутренней базы данных пользователей устройства, которая ограничена емкостью памяти этого устройства (внешний сервер может также использоваться в дополнение к внутренней базе данных). В целом аутентификация с использованием RADIUS и TACACS+ позволяет идентифицировать неограниченное количество пользователей с помощью единой централизованной службы.

Некоторые основные различия между протоколами RADIUS и TACACS+ приводятся в следующей таблице.

Таблица 62 RADIUS и TACACS+

	RADIUS	TACACS+
Транспортный протокол	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Шифрование	Шифрование пароля, отправляемого для аутентификации.	Шифрование всей коммуникации между клиентом (коммутатором) и сервером TACACS.

23.2 Экраны настройки функций аутентификации и учета

Чтобы включить функции аутентификации и/или учета на коммутаторе, необходимо прежде всего указать настройки сервера аутентификации (RADIUS и/или TACACS+), а затем настроить приоритеты аутентификации и учета.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application > Auth and Acct**.

Рисунок 98 Экран Advanced Application > Auth and Acct



23.2.1 Настройка сервера RADIUS

Настройки сервера RADIUS вводятся на показанном ниже экране. Дополнительную информацию о серверах RADIUS можно найти в [разд. 23.1.2 на стр. 202](#), а информацию об атрибутах RADIUS, используемых функциями аутентификации и учета данного коммутатора – в [разд. 23.3 на стр. 211](#). Чтобы отобразить показанный ниже экран, нажмите на ссылке **RADIUS Server Setup** на экране **Authentication and Accounting**.

Рисунок 99 Экран Advanced Application > Auth and Acct > RADIUS Server Setup

RADIUS Server Setup Auth and Acct

Authentication Server

Mode:

Timeout: seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>	<input type="text"/>	<input type="checkbox"/>

Apply Cancel

Accounting Server

Timeout: seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="1813"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text" value="0.0.0.0"/>	<input type="text" value="1813"/>	<input type="text"/>	<input type="checkbox"/>

Apply Cancel

Поля экрана описаны в следующей таблице.

Таблица 63 Экран Advanced Application > Auth and Acct > RADIUS Server Setup

ПОЛЕ	ОПИСАНИЕ
Authentication Server	В данном разделе вводятся настройки аутентификации с использованием RADIUS.
Mode	Данное поле используется лишь при настройке нескольких серверов RADIUS. В случае выбора index-priority коммутатор будет пытаться осуществить аутентификацию с использованием первого настроенного сервера RADIUS; при отсутствии ответа коммутатор обратится ко второму серверу RADIUS. В случае выбора round-robin запросы на аутентификацию будут направляться серверам RADIUS поочередно.
Timeout	Укажите период в секундах, в течение которого коммутатор будет ожидать ответа на запрос от сервера RADIUS. В случае выбора режима index-priority и использования двух серверов RADIUS значение тайм-аута делится между двумя серверами RADIUS. Например, если установить период тайм-аута равным 30 секундам, коммутатор будет ожидать ответа от первого сервера RADIUS в течение 15 секунд, после чего направит запрос на второй сервер RADIUS.

Таблица 63 Экран Advanced Application > Auth and Acct > RADIUS Server Setup

ПОЛЕ	ОПИСАНИЕ
Index	Порядковый номер записи о сервере RADIUS (только для чтения).
IP Address	Введите IP-адрес внешнего сервера RADIUS в виде десятичных чисел, разделенных точками.
UDP Port	По умолчанию аутентификация на сервере RADIUS производится через порт 1812 . Изменять это значение не следует, за исключением тех случаев, когда об этом попросит администратор сети.
Shared Secret	Укажите пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера RADIUS и коммутатора. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере RADIUS и коммутаторе.
Delete	При необходимости удалить из коммутатора существующую запись о сервере RADIUS установите данный переключатель. Удаление записи произойдет после нажатия на кнопку Apply .
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Accounting Server	В данном разделе вводятся настройки учета с использованием RADIUS.
Timeout	Укажите период в секундах, в течение которого коммутатор будет ожидать ответа на запрос от сервера учета RADIUS.
Index	Порядковый номер записи о сервере учета RADIUS (только для чтения).
IP Address	Введите IP-адрес внешнего сервера учета RADIUS в виде десятичных чисел, разделенных точками.
UDP Port	По умолчанию учет на сервере RADIUS производится через порт 1813 . Изменять это значение не следует, за исключением тех случаев, когда об этом попросит администратор сети.
Shared Secret	Укажите пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера учета RADIUS и коммутатора. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере учета RADIUS и коммутаторе.
Delete	При необходимости удалить из коммутатора существующую запись о сервере учета RADIUS установите данный переключатель. Удаление записи произойдет после нажатия на кнопку Apply .
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

23.2.2 Настройка сервера TACACS+

Настройки сервера TACACS+ вводятся на показанном ниже экране. Более подробную информацию о серверах TACACS+ можно найти в [разд. 23.1.2 на стр. 202](#). Чтобы отобразить показанный ниже экран, нажмите на ссылке **TACACS+ Server Setup** на экране **Authentication and Accounting**.

Рисунок 100 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup

TACACS+ Server Setup
Auth and Acct

Authentication Server

Mode:

Timeout: seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="49"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text" value="0.0.0.0"/>	<input type="text" value="49"/>	<input type="text"/>	<input type="checkbox"/>

Accounting Server

Timeout: seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="49"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text" value="0.0.0.0"/>	<input type="text" value="49"/>	<input type="text"/>	<input type="checkbox"/>

Поля экрана описаны в следующей таблице.

Таблица 64 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup

ПОЛЕ	ОПИСАНИЕ
Authentication Server	В данном разделе вводятся настройки аутентификации с использованием TACACS+.
Mode	<p>Данное поле используется лишь при настройке нескольких серверов TACACS+.</p> <p>В случае выбора index-priority коммутатор будет пытаться осуществить аутентификацию с использованием первого настроенного сервера TACACS+; при отсутствии ответа коммутатор обратится ко второму серверу TACACS+.</p> <p>В случае выбора round-robin запросы на аутентификацию будут направляться серверам TACACS+ поочередно.</p>
Timeout	<p>Укажите период в секундах, в течение которого коммутатор будет ожидать ответа на запрос от сервера TACACS+.</p> <p>В случае выбора режима index-priority и использования двух серверов TACACS+ значение тайм-аута делится между двумя серверами TACACS+. Например, если установить период тайм-аута равным 30 секундам, коммутатор будет ожидать ответа от первого сервера TACACS+ в течение 15 секунд, после чего направит запрос на второй сервер TACACS+.</p>
Index	Порядковый номер записи о сервере TACACS+ (только для чтения).
IP Address	Введите IP-адрес внешнего сервера TACACS+ в виде десятичных чисел, разделенных точками.
TCP Port	По умолчанию аутентификация на сервере TACACS+ производится через порт 49 . Изменять это значение не следует, за исключением тех случаев, когда об этом попросит администратор сети.

Таблица 64 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup

ПОЛЕ	ОПИСАНИЕ
Shared Secret	Укажите пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера TACACS+ и коммутатора. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере TACACS+ и коммутаторе.
Delete	При необходимости удалить из коммутатора существующую запись о сервере TACACS+ установите данный переключатель. Удаление записи произойдет после нажатия на кнопку Apply .
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Accounting Server	В данном разделе вводятся настройки учета с использованием TACACS+.
Timeout	Укажите период в секундах, в течение которого коммутатор будет ожидать ответа на запрос от сервера учета TACACS+.
Index	Порядковый номер записи о сервере учета TACACS+ (только для чтения).
IP Address	Введите IP-адрес внешнего сервера учета TACACS+ в виде десятичных чисел, разделенных точками.
TCP Port	По умолчанию учет на сервере TACACS+ производится через порт 49 . Изменять это значение не следует, за исключением тех случаев, когда об этом попросит администратор сети.
Shared Secret	Укажите пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера учета TACACS+ и коммутатора. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере учета TACACS+ и коммутаторе.
Delete	При необходимости удалить из коммутатора существующую запись о сервере учета TACACS+ установите данный переключатель. Удаление записи произойдет после нажатия на кнопку Apply .
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

23.2.3 Настройка аутентификации и учета

Настройка функций аутентификации и учета коммутатора осуществляется на следующем экране. Чтобы отобразить показанный ниже экран, нажмите на ссылке **Auth and Acct Setup** на экране **Authentication and Accounting**.

Рисунок 101 Экран Advanced Application > Auth and Acct > Auth and Acct Setup

Auth and Acct Setup Auth and Acct

Authentication

Type	Method 1	Method 2	Method 3
Privilege Enable	local	-	-
Login	local	-	-

Accounting

Update Period: minutes

Type	Active	Broadcast	Mode	Method	Privilege
System	<input type="checkbox"/>	<input type="checkbox"/>	-	radius	-
Exec	<input type="checkbox"/>	<input type="checkbox"/>	start-stop	radius	-
Dot1x	<input type="checkbox"/>	<input type="checkbox"/>	start-stop	radius	-
Commands	<input type="checkbox"/>	<input type="checkbox"/>	stop-only	tacacs+	0

Apply Cancel

Поля экрана описаны в следующей таблице.

Таблица 65 Экран Advanced Application > Auth and Acct > Auth and Acct Setup

ПОЛЕ	ОПИСАНИЕ
Authentication	В данном разделе определяются способы аутентификации пользователей, пытающихся получить доступ к коммутатору.
Privilege Enable	<p>В данных полях можно определить, к какой базе данных должен обращаться коммутатор (в первую, вторую и третью очередь) для аутентификации уровня привилегий учетных записей администраторов (пользователей, управляющих коммутатором).</p> <p>Привилегии доступа для учетных записей в случае использования локальной аутентификации (local) определяются при помощи команд (см. Справочник по интерфейсу командной строки). TACACS+ и RADIUS представляют собой внешние серверы. Прежде чем установить приоритет, убедитесь, что соответствующая база данных правильно настроена.</p> <p>Для аутентификации привилегий доступа администраторов на коммутаторе можно указать до трех методов. Данный коммутатор пытается использовать каждый из методов в том порядке, в котором они указаны (сначала Method 1, затем Method 2 и наконец Method 3). В поле Method 1 обязательно должен быть выбран один из методов. Если коммутатор должен обращаться и к другим источникам для проверки привилегий доступа, их необходимо указать в полях Method 2 и Method 3.</p> <p>В случае выбора local для проверки уровня привилегий коммутатор будет обращаться к настроенным на нем записям.</p> <p>В случае выбора radius или tacacs+ проверка уровня привилегий будет осуществляться коммутатором с помощью внешних серверов.</p>

Таблица 65 Экран Advanced Application > Auth and Acct > Auth and Acct Setup

ПОЛЕ	ОПИСАНИЕ
Login	<p>В данных полях можно определить, к какой базе данных должен обращаться коммутатор (в первую, вторую и третью очередь) для аутентификации учетных записей администраторов (пользователей, управляющих коммутатором). Локальные учетные записи пользователей настраиваются на экране Access Control > Logins. TACACS+ и RADIUS представляют собой внешние серверы. Прежде чем установить приоритет, убедитесь, что соответствующая база данных правильно настроена.</p> <p>Для аутентификации учетных записей администраторов на коммутаторе можно указать до трех методов. Данный коммутатор пытается использовать каждый из методов в том порядке, в котором они указаны (сначала Method 1, затем Method 2 и наконец Method 3). В поле Method 1 обязательно должен быть выбран один из методов. Если коммутатор должен обращаться и к другим источникам для проверки учетных записей администраторов, их необходимо указать в полях Method 2 и Method 3.</p> <p>В случае выбора local для проверки учетных записей администраторов коммутатор будет обращаться к записям, настроенным на экране Access Control > Logins.</p> <p>В случае выбора radius аутентификацию учетных записей администраторов коммутатор осуществляет через сервер RADIUS.</p> <p>В случае выбора tacacs+ аутентификацию учетных записей администраторов коммутатор осуществляет через сервер TACACS+.</p>
Accounting	В данном разделе вводятся настройки функции учета для коммутатора.
Update Period	Периодичность в минутах, с которой коммутатор отправляет на сервер учета обновленную информацию. Данное значение используется лишь в том случае, если для параметров Exec или Dot1x выбран вариант start-stop .
Type	<p>Данный коммутатор поддерживает передачу на сервер(ы) учета следующих типов событий:</p> <ul style="list-style-type: none"> • System – в случае выбора данного варианта коммутатор будет передавать информацию о следующих системных событиях: загрузка системы, отключение системы, включение учета на системе, отключение учета на системе. • Exec – в случае выбора данного варианта коммутатор будет передавать информацию о входе и выходе администратора и системы через консольный порт, Telnet или SSH. • Dot1x – в случае выбора данного варианта коммутатор будет передавать информацию о начале клиентами сеансов IEEE 802.1x (аутентификация на коммутаторе), завершении сеансов, а также промежуточных обновлениях о состоянии сеансов. • Commands – в случае выбора данного варианта коммутатор будет передавать информацию о выполнении на коммутаторе команд с уровнем привилегий, равным или выше указанного.
Active	Установите этот переключатель, чтобы активировать функцию учета для указанных типов событий.
Broadcast	<p>Установите данный переключатель, чтобы учетная информация передавалась коммутатором сразу на все настроенные серверы учета.</p> <p>Если данный переключатель не установлен, но было настроено два сервера учета, коммутатор отправляет информацию на первый сервер учета; при отсутствии ответа информация отправляется на второй сервер учета.</p>
Mode	<p>Данный коммутатор поддерживает два режима регистрации событий входа в систему. Выберите:</p> <ul style="list-style-type: none"> • start-stop – чтобы коммутатор отправлял информацию на сервер учета при начале сеанса, в течение пользовательского сеанса (если он превышает период Update Period) и при завершении сеанса пользователем. • stop-only – чтобы коммутатор отправлял информацию на сервер учета только после завершения сеанса пользователем.

Таблица 65 Экран Advanced Application > Auth and Acct > Auth and Acct Setup

ПОЛЕ	ОПИСАНИЕ
Method	Выберите метод (RADIUS или TACACS+) для учета событий определенного типа. Для регистрации событий типа Commands поддерживается только метод TACACS+.
Privilege	Данное поле настраивается только для событий типа Commands . Выберите пороговый уровень привилегий для команд, информация о которых будет направляться коммутатором на сервер учета. В этом случае коммутатор будет передавать учетную информацию в случае выполнения на коммутаторе команд, уровень привилегий которых равен или превышает указанный.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

23.2.4 Специальный атрибут производителя

Стандартом RFC 2865 определен метод обмена специфичной для производителя информацией между сервером RADIUS и сетевым устройством доступа (например, коммутатором). Для расширения функциональных возможностей сервера RADIUS компания может использовать специальные атрибуты производителя (VSA).

Данный коммутатор поддерживает атрибуты VSA, которые, в зависимости от результатов аутентификации пользователя, позволяют выполнять следующие действия:

- Ограничивать пропускную способность для входящего или исходящего трафика через порт, к которому подключен пользователь.
- Назначать уровни привилегий учетным записям (более подробную информацию об уровнях привилегий учетных записей можно найти в [Справочнике по интерфейсу командной строки](#)) для пользователей, прошедших аутентификацию.

Атрибут VSA включает в себя следующие поля:

- **Vendor-ID**: Идентификационный номер, назначенный компании уполномоченной организацией по распределению нумерации в сети Интернет (IANA). ZyXEL присвоен идентификатор 890.
- **Vendor-Type**: Определяемый производителем атрибут, идентифицирующий изменяемый параметр.
- **Vendor-data**: Значение, которое необходимо присвоить параметру.



Порядок настройки атрибутов VSA для пользователей, проходящий аутентификацию на сервере RADIUS, можно найти в документации к соответствующему серверу RADIUS.

Атрибуты VSA, поддерживаемые коммутатором, описаны в следующей таблице.

Таблица 66 Поддерживаемые атрибуты VSA

ФУНКЦИЯ	АТРИБУТ
Назначение пропускной способности для входящего трафика	Vendor-Id = 890 Vendor-Type = 1 Vendor-data = скорость входящего трафика (кбит/с в десятичном формате)
Назначение пропускной способности для исходящего трафика	Vendor-Id = 890 Vendor-Type = 2 Vendor-data = скорость исходящего трафика (кбит/с в десятичном формате)
Назначение привилегий	Vendor-ID = 890 Vendor-Type = 3 Vendor-Data = " shell:priv-lvl=N " или Vendor-ID = 9 (CISCO) Vendor-Type = 1 (CISCO-AVPAIR) Vendor-Data = " shell:priv-lvl=N " где N – уровень привилегий (от 0 до 14). Примечание: Если для учетной записи на сервере или серверах RADIUS и на коммутаторе установлены различные уровни привилегий, пользователю назначается уровень привилегий из той базы данных (RADIUS или локальной), которая первой была использована коммутатором для аутентификации пользователя.

23.2.4.1 Атрибут протокола туннелирования

С помощью атрибутов протокола туннелирования на сервере RADIUS (см. документацию к серверу RADIUS) можно назначить порт коммутатора виртуальной локальной сети VLAN с использованием аутентификации на основе IEEE 802.1x. Настройки VLAN порта – фиксированные, без тегов. При этом также назначается идентификатор VID порта. Значения, которые необходимо настроить, описаны в следующей таблице. Значения, выделенные в таблице полужирным шрифтом, являются фиксированными в соответствии с RFC 3580.

Таблица 67 Поддерживаемые атрибуты протокола туннелирования

ФУНКЦИЯ	АТРИБУТ
Назначение сети VLAN	Tunnel-Type = VLAN(13) Tunnel-Medium-Type = 802(6) Tunnel-Private-Group-ID = VLAN ID Примечание: На коммутаторе необходимо создать сеть VLAN с указанным идентификатором VID.

23.3 Поддерживаемые атрибуты RADIUS

Атрибуты RADIUS представляют собой данные, используемые для определения специального порядка аутентификации, а также учетные элементы пользовательского профиля, сохраняемые на сервере RADIUS. В данном приложении перечислены атрибуты RADIUS, поддерживаемые коммутатором.

Более подробную информацию об атрибутах RADIUS, используемых для аутентификации, можно найти в RFC 2865. Описание атрибутов RADIUS, используемых для учета, можно найти в RFC 2866 и RFC 2869.

В данном приложении перечислены атрибуты, используемые коммутатором для функций аутентификации и учета. В тех случаях, когда с атрибутом связан особый формат, приводится описание формата.

23.3.1 Атрибуты, используемые для аутентификации

В приведенных ниже разделах перечислены атрибуты, передаваемые коммутатором на сервер RADIUS при осуществлении аутентификации.

23.3.1.1 Атрибуты, используемые при аутентификации привилегированного доступа

User-Name

– формат атрибута User-Name: **\$enab#\$**, где # представляет собой уровень привилегий (1-14)

User-Password

NAS-Identifier

NAS-IP-Address

23.3.1.2 Атрибуты, используемые для входа пользователей

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

23.3.1.3 Атрибуты, используемые для аутентификации на основе IEEE 802.1x

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

– Данное значение на коммутаторе устанавливается равным **Ethernet(15)**.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

23.3.2 Атрибуты, используемые для учета

В приведенных ниже разделах перечислены атрибуты, передаваемые коммутатором на сервер RADIUS при использовании функций учета.

23.3.2.1 Атрибуты, используемые для учета системных событий

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID

– Формат идентификатора Acct-Session-Id: **дата+время+8-значный порядковый номер**, например, 2007041917210300000001. (дата: 2007/04/19, время: 17:21:03, порядковый номер: 00000001)

Acct-Delay-Time

23.3.2.2 Атрибуты, используемые для учета событий выполнения команд (Exec)

Передаваемые атрибуты и момент времени, когда они передаются, перечислены в следующей таблице (различия между событиями Exec, связанными с выполнением команд с консоли или через Telnet/SSH заключается в том, для событий через Telnet/SSH используется атрибут Calling-Station-Id):

Таблица 68 Атрибуты RADIUS – события Exec при выполнении команд с консоли

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
User-Name	Д	Д	Д
NAS-Identifier	Д	Д	Д
NAS-IP-Address	Д	Д	Д
Service-Type	Д	Д	Д
Acct-Status-Type	Д	Д	Д
Acct-Delay-Time	Д	Д	Д
Acct-Session-Id	Д	Д	Д
Acct-Authentic	Д	Д	Д
Acct-Session-Time		Д	Д
Acct-Terminate-Cause			Д

Таблица 69 Атрибуты RADIUS – события Exec при выполнении команд через Telnet/SSH

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
User-Name	Д	Д	Д
NAS-Identifier	Д	Д	Д
NAS-IP-Address	Д	Д	Д
Service-Type	Д	Д	Д
Calling-Station-Id	Д	Д	Д
Acct-Status-Type	Д	Д	Д
Acct-Delay-Time	Д	Д	Д

Таблица 69 Атрибуты RADIUS – события Exec при выполнении команд через Telnet/SSH

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
Acct-Session-Id	Д	Д	Д
Acct-Authentic	Д	Д	Д
Acct-Session-Time		Д	Д
Acct-Terminate-Cause			Д

23.3.2.3 Атрибуты, используемые для учета событий IEEE 802.1x

Используемые атрибуты перечислены в следующей таблице с указанием момента времени, когда они передаются:

Таблица 70 Атрибуты RADIUS – события Exec при выполнении команд с консоли

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
User-Name	Д	Д	Д
NAS-IP-Address	Д	Д	Д
NAS-Port	Д	Д	Д
Class	Д	Д	Д
Called-Station-Id	Д	Д	Д
Calling-Station-Id	Д	Д	Д
NAS-Identifier	Д	Д	Д
NAS-Port-Type	Д	Д	Д
Acct-Status-Type	Д	Д	Д
Acct-Delay-Time	Д	Д	Д
Acct-Session-Id	Д	Д	Д
Acct-Authentic	Д	Д	Д
Acct-Input-Octets		Д	Д
Acct-Output-Octets		Д	Д
Acct-Session-Time		Д	Д
Acct-Input-Packets		Д	Д
Acct-Output-Packets		Д	Д
Acct-Terminate-Cause			Д
Acct-Input-Gigawords		Д	Д
Acct-Output-Gigawords		Д	Д

Защита от подмены IP-адресов

Функция защиты от подмены IP-адресов позволяет отфильтровывать несанкционированные пакеты DHCP и ARP в сети.

24.1 Обзор функции защиты от подмены IP-адресов

Для защиты от подмены IP-адресов применяется таблица привязок, позволяющая различать санкционированные и несанкционированные DHCP- и ARP-пакеты. При привязке используются следующие атрибуты:

- MAC-адрес
- VLAN ID
- IP-адрес
- Номер порта

При получении коммутатором пакета DHCP или ARP производится поиск соответствующих MAC-адреса, идентификатора VLAN ID, IP-адреса и номера порта в таблице привязок. При наличии привязки коммутатор пересылает пакет. Если привязки не найдено, пакет коммутатором отбрасывается.

Таблица привязок строится коммутатором посредством отслеживания пакетов DHCP (динамическая привязка) и на основе информации, предоставленной администратором вручную (статическая привязка).

Функция защиты от подмены IP-адресов включает в себя следующие функции:

- Статическая привязка. Используется для создания статических связей в таблице привязок.
- Отслеживание DHCP. Используется для отфильтровывания несанкционированных пакетов DHCP в сети и для динамического построения таблицы привязок.
- Инспекция ARP-пакетов. Используется для отфильтровывания несанкционированных пакетов ARP.

Чтобы использовать динамическую привязку для отфильтровывания несанкционированных ARP-пакетов (типичная ситуация), перед включением инспекции ARP-пакетов необходимо включить отслеживание DHCP.

24.1.1 Обзор отслеживания DHCP

Функция отслеживания DHCP позволяет отфильтровывать несанкционированные DHCP-пакеты в сети и динамически строить таблицу привязок. Благодаря этому можно защитить клиентов от получения IP-адресов от несанкционированных серверов DHCP.

24.1.1.1 Доверенные и не заслуживающие доверия порты

Функция отслеживания DHCP делит все порты на доверенные и не заслуживающие доверия. Данная настройка не зависит от аналогичной настройки доверенных/не заслуживающих доверия портов для функции инспекции ARP-пакетов. Кроме того, можно определить максимальное количество пакетов DHCP, которое может приниматься через каждый из портов (доверенных или не заслуживающих доверия) за секунду.

Доверенные порты подключаются к серверам DHCP или другим коммутаторам. Пакеты DHCP, поступающие через доверенные порты, коммутатор отбрасывает лишь в том случае, если скорость их поступления слишком высока. По информации от доверенных портов коммутатор строит динамическую таблицу привязок.



Если включить отслеживание DHCP и не определить ни одного доверенного порта, коммутатор будет отбрасывать все запросы DHCP.

Не заслуживающие доверия порты подключаются к абонентам. Пакеты DHCP от не заслуживающих доверия портов отбрасываются коммутатором в следующих случаях:

- Пакет представляет собой пакет сервера DHCP (например, OFFER, ACK или NACK).
- MAC-адрес источника и IP-адрес источника в пакете не соответствуют ни одной из существующих привязок.
- Пакет представляет собой пакет типа RELEASE или DECLINE, и MAC-адрес источника и порт источника не соответствуют ни одной из существующих привязок.
- Скорость поступления пакетов DHCP слишком высока.

24.1.1.2 База данных отслеживания DHCP

Таблица привязок хранится коммутатором в энергозависимой памяти. В случае перезапуска коммутатора он загружает статические привязки из постоянной памяти, однако динамические привязки при этом теряются, т.е. устройства в сети должны повторно направлять DHCP-запросы. В связи с этим рекомендуется настроить базу данных отслеживания DHCP.

База данных отслеживания DHCP позволяет хранить динамические привязки для функций отслеживания DHCP и инспекции ARP-пакетов в файле на внешнем сервере TFTP. Если база данных отслеживания DHCP была настроена, коммутатор загружает динамические привязки из базы данных отслеживания DHCP после перезапуска коммутатора.

Можно настроить имя и расположение файла на внешнем сервере TFTP. Файл имеет следующий формат:

Рисунок 102 Формат файла базы данных отслеживания DHCP

```

<начальная-контрольная-сумма>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<привязка-1> <контрольная-сумма-1>
<привязка-2> <контрольная-сумма-1-2>
...
...
<привязка-n> <контрольная-сумма-1-2-..-n>
END

```

Значение <начальная-контрольная-сумма> позволяет различать привязки, сохраненные в последнем обновлении, от привязок из предыдущих обновлений. Каждая привязка включает в себя 72 байта, пробел и еще одну контрольную сумму, которая используется для проверки привязки в процессе считывания. Если вычисленная контрольная сумма не совпадает с контрольной суммой в файле, данная и все последующие привязки игнорируются.

24.1.1.3 Информация в поле Option 82 при ретрансляции DHCP

Данный коммутатор способен добавлять информацию к тем запросам DHCP, которые им не отбрасываются. Благодаря этому сервер DHCP может получить больше информации об источнике запроса. Данный коммутатор способен добавлять следующую информацию:

- Идентификатор слота (1 байт), идентификатор порта (1 байт), и идентификатор VLAN (2 байта)
- Имя системы (до 32 байт)

Данная информация помещается в поле информации агента поля Option 82 заголовка DHCP в кадрах клиентских запросов DHCP. Дополнительную информацию о поле Option 82 при ретрансляции DHCP можно найти в [гл. 28 на стр. 255](#).

При ответе сервера DHCP коммутатор удаляет информацию из поля информации агента перед пересылкой ответа к первоначальному источнику запроса.

Данные параметры могут быть настроены для каждой исходной VLAN. Они не зависят от настроек ретрансляции DHCP ([гл. 28 на стр. 255](#)).

24.1.1.4 Настройка отслеживания DHCP

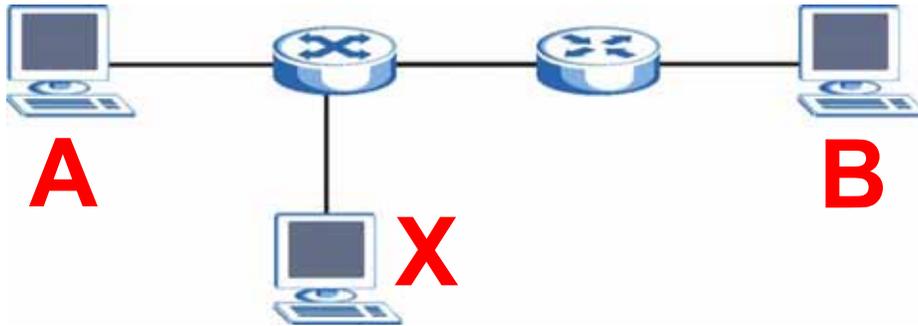
Чтобы настроить на коммутаторе функцию отслеживания DHCP, выполните следующие действия.

- 1 Включите функцию отслеживания DHCP на коммутаторе.
- 2 Включите функцию отслеживания DHCP для каждой VLAN, и настройте значение для поля Option 82 при ретрансляции DHCP.
- 3 Настройте доверенные и не заслуживающие доверия порты, а также укажите максимальное количество пакетов DHCP в секунду, принимаемое через каждый из портов.
- 4 Настройте статические привязки.

24.1.2 Обзор функции инспекции ARP-пакетов

Инспекция ARP-пакетов используется для отфильтровывания несанкционированных пакетов ARP. Это позволяет предотвратить многие виды атак класса «man-in-the-middle», таких как описанная в следующем примере.

Рисунок 103 Пример: атака «Man-in-the-middle»



В данном примере компьютер **В** пытается установить соединение с компьютером **А**. Компьютер **Х** находится в том же широковещательном домене, что и компьютер **А**, и перехватывает ARP-запрос для разрешения адреса компьютера **А**. После этого компьютер **Х**:

- Выдает себя компьютером **А** и отвечает компьютеру **В**.
- Выдает себя компьютером **В** и отправляет сообщение компьютеру **А**.

В результате весь обмен данными между компьютером **А** и компьютером **В** происходит через компьютер **Х**. Компьютер **Х** получает возможность читать и изменять информацию, передаваемую между этими двумя компьютерами.

24.1.2.1 Инспекция ARP-пакетов и фильтры MAC-адресов

При обнаружении коммутатором несанкционированного ARP-пакета им автоматически создается фильтр MAC-адресов, блокирующий трафик от MAC-адреса и сети VLAN, от которых поступил несанкционированный ARP-пакет. Период активности фильтра MAC-адресов на коммутаторе можно настраивать.

Такие фильтры MAC-адресов отличаются от обычных фильтров MAC-адресов (см. [гл. 10 на стр. 111](#)).

- Они сохраняются только в энергозависимой памяти.
- В памяти они находятся в другой области, не вместе с обычными фильтрами MAC-адресов.
- Эти фильтры видны только на экранах и в командах функции инспекции ARP-пакетов **ARP Inspection**, и не видны на экранах и в командах фильтров MAC-адресов **MAC Address Filter**.

24.1.2.2 Доверенные и не заслуживающие доверия порты

Функция инспекции ARP-пакетов делит все порты на доверенные и не заслуживающие доверия. Данная настройка не зависит от аналогичной настройки доверенных/не заслуживающих доверия портов для функции отслеживания DHCP.

Пакеты ARP, приходящие через доверенные порты, коммутатором не отбрасываются ни по какой причине.

Пакеты ARP, приходящие через не заслуживающие доверия порты, отбрасываются коммутатором в том случае, если информация об отправителе в ARP-пакете не совпадает ни с одной из существующих привязок.

24.1.2.3 Системный журнал Syslog

При пересылке или отбрасывании пакетов ARP коммутатор может отправлять сообщения системного журнала syslog на указанный сервер syslog (гл. 32 на стр. 293). В целях большей эффективности коммутатор может консолидировать сообщения контрольного журнала и отправлять их партиями.

24.1.2.4 Настройка инспекции ARP-пакетов

Чтобы настроить на коммутаторе функцию инспекции ARP-пакетов, выполните следующие действия.

- 1 Настройте отслеживание DHCP. См. [разд. 24.1.1.4 на стр. 217](#).



Рекомендуется включить отслеживание DHCP как минимум за один день до включения инспекции ARP-пакетов, чтобы у коммутатора было достаточно времени для построения таблицы привязок.

- 2 Включите функцию инспекции ARP-пакетов в каждой сети VLAN.
- 3 Настройте доверенные и не заслуживающие доверия порты, а также укажите максимальное количество пакетов ARP в секунду, принимаемое через каждый из портов.

24.2 Защита от подмены IP-адресов

На данном экране можно просмотреть существующие привязки для функций отслеживания DHCP и инспекции ARP-пакетов. На основе привязок функции отслеживания DHCP и инспекции ARP-пакетов различают санкционированные и несанкционированные пакеты. Таблица привязок строится коммутатором посредством отслеживания пакетов DHCP (динамическая привязка) и на основе информации, предоставленной администратором вручную (статическая привязка). Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard**.

Рисунок 104 Экран Advanced Application > IP Source Guard

IP Source Guard						
Static Binding DHCP Snooping ARP Inspection						
Index	MAC Address	IP Address	Lease	Type	VID	Port
1	a1:12:12:12:12:01	172.23.37.222	inifinity	static	1	18

Поля экрана описаны в следующей таблице.

Таблица 71 Экран Advanced Application > IP Source Guard

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер каждой привязки.
MAC Address	В этом поле отображается MAC-адрес источника для привязки.
IP Address	В этом поле отображается IP-адрес, назначенный для MAC-адреса в привязке.
Lease	В этом поле отображается количество дней, часов, минут и секунд, в течение которого действует привязка; например, 2d3h4m5s означает, что привязка действует в течение 2 дней, 3 часов, 4 минут и 5 секунд. Для привязки, действительной в течение неограниченного времени (например, статической привязки), в этом поле отображается infinity .
Type	В этом поле отображается способ получения коммутатором информации о привязке. static : привязка создана с использованием информации, предоставленной администратором вручную. dhcp-snooping : привязка создана в результате отслеживания пакетов DHCP.
VID	В этом поле отображается идентификатор VLAN для привязки.
Port	В этом поле отображается номер порта для привязки. Если данное поле пустое, привязка действует для всех портов.

24.3 Статическая привязка для защиты от подмены IP-адресов

На данном экране можно управлять статическими привязками для функций отслеживания DHCP и инспекции ARP-пакетов. Статические привязки идентифицируются по MAC-адресу и идентификатору VLAN ID. Для каждой комбинации MAC-адреса и идентификатора VLAN ID можно создать только одну статическую привязку. При попытке создать статическую привязку с теми же MAC-адресом и идентификатором VLAN ID, что и у существующей статической привязки, новая информация заменяет предыдущую. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > Static Binding**.

Рисунок 105 Экран Advanced Application > IP Source Guard > Static Binding

Поля экрана описаны в следующей таблице.

Таблица 72 Экран Advanced Application > IP Source Guard > Static Binding

ПОЛЕ	ОПИСАНИЕ
MAC Address	Введите MAC-адрес источника для привязки.
IP Address	Введите IP-адрес, назначенный для MAC-адреса в привязке.
VLAN	Введите идентификатор VLAN ID для привязки.
Port	Укажите порты для привязки. Если привязка относится к одному порту, выберите первый переключатель и введите номер порта в соответствующее поле справа. Если данная привязка относится ко всем портам, выберите переключатель Any .
Add	Нажмите на данную кнопку, чтобы добавить указанную статическую привязку или обновить существующую.
Cancel	Нажмите на данную кнопку, чтобы сбросить значения из последней выбранной статической привязке или, если ничего не было выбрано, очистить перечисленные выше поля.
Clear	Нажмите на данную кнопку, чтобы очистить перечисленные выше поля.
Index	В этом поле отображается порядковый номер каждой привязки.
MAC Address	В этом поле отображается MAC-адрес источника для привязки.
IP Address	В этом поле отображается IP-адрес, назначенный для MAC-адреса в привязке.
Lease	В этом поле отображается период действия привязки.
Type	В этом поле отображается способ получения коммутатором информации о привязке. static : привязка создана с использованием информации, предоставленной администратором вручную.
VLAN	В этом поле отображается идентификатор VLAN для привязки.
Port	В этом поле отображается номер порта для привязки. Если данное поле пустое, привязка действует для всех портов.

Таблица 72 Экран Advanced Application > IP Source Guard > Static Binding

ПОЛЕ	ОПИСАНИЕ
Delete	Установите переключатель и нажмите на Delete , чтобы удалить выбранную запись.
Cancel	Нажмите на данную кнопку, чтобы снять выделение с переключателей Delete .

24.4 Отслеживание DHCP

На данном экране можно просмотреть различные статистические данные по базе данных отслеживания DHCP. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > DHCP Snooping**.

Рисунок 106 Экран Advanced Application > IP Source Guard > DHCP Snooping

DHCP Snooping		Configure	IPSG
Database Status			
Description	Status		
Agent URL			
Write delay timer	300	seconds	
Abort timer	300	seconds	
Agent running	None		
Delay timer expiry	Not Running		
Abort timer expiry	Not Running		
Last succeeded time	None		
Last failed time	None		
Last failed reason	No failure recorded		
		Times	
Total attempts	0		
Startup failures	0		
Successful transfers	0		
Failed transfers	0		
Successful reads	0		
Failed reads	0		
Successful writes	0		
Failed writes	0		
Database detail			
Description	Status		
First successful access	None		
Last ignored bindings counters			
Binding collisions	0		
Invalid interfaces	0		
Parse failures	0		
Expired leases	0		
Unsupported vlans	0		
Last ignored time	None		
Total ignored bindings counters			
Binding collisions	0		
Invalid interfaces	0		
Parse failures	0		
Expired leases	0		
Unsupported vlans	0		

Поля экрана описаны в следующей таблице.

Таблица 73 Экран Advanced Application > IP Source Guard > DHCP Snooping

ПОЛЕ	ОПИСАНИЕ
Database Status	
	В данном разделе отображаются текущие настройки базы данных отслеживания DHCP. Их можно изменить на экране DHCP Snooping Configure . См. разд. 24.5 на стр. 226 .
Agent URL	В данном поле отображается месторасположение базы данных отслеживания DHCP.
Write delay timer	В данном поле отображается, как долго (в секундах) коммутатор пытается выполнить конкретное обновление базы данных отслеживания DHCP перед отказом от дальнейших попыток.
Abort timer	В данном поле отображается, как долго (в секундах) коммутатор выжидает перед обновлением базы данных отслеживания DHCP после изменения текущих привязок.
	В этом разделе отображается информация о текущем обновлении и следующем обновлении базы данных отслеживания DHCP.
Agent running	В этом поле отображается статус текущего обновления или доступа к базе данных отслеживания DHCP. none : коммутатор не обращается к базе данных отслеживания DHCP. read : коммутатор осуществляет загрузку динамических привязок из базы данных отслеживания DHCP. write : коммутатор осуществляет обновление базы данных отслеживания DHCP.
Delay timer expiry	В данном поле отображается, сколько еще (в секундах) коммутатор будет пытаться выполнить текущее обновление перед отказом от дальнейших попыток. Если коммутатор в данный момент не выполняет обновления базы данных отслеживания DHCP, в этом поле отображается Not Running .
Abort timer expiry	В данном поле отображается, через какой промежуток времени (в секундах) коммутатор выполнит очередное обновление базы данных отслеживания DHCP. Если текущие привязки с момента последнего обновления не изменялись, в этом поле отображается Not Running .
	В данном разделе отображается информация о последнем обновлении коммутатором базы данных отслеживания DHCP.
Last succeeded time	В этом поле отображается время последнего успешного обновления коммутатором базы данных отслеживания DHCP.
Last failed time	В этом поле отображается время последнего неудавшегося обновления коммутатором базы данных отслеживания DHCP.
Last failed reason	В этом поле отображается причина последнего неудавшегося обновления коммутатором базы данных отслеживания DHCP.
	В данном разделе отображается историческая информация о количестве успешных и неудавшихся попыток считывания или обновления коммутатором базы данных отслеживания DHCP.
Total attempts	В этом поле отображается общее количество попыток обращения коммутатором к базе данных отслеживания DHCP по любым причинам.
Startup failures	В данном поле отображается количество случаев, когда коммутатору не удалось создать или считать базу данных отслеживания DHCP при запуске коммутатора или настройки нового URL для базы данных отслеживания DHCP.

Таблица 73 Экран Advanced Application > IP Source Guard > DHCP Snooping

ПОЛЕ	ОПИСАНИЕ
Successful transfers	В данном поле отображается количество случаев успешного считывания привязок или обновления привязок коммутатором в базе данных отслеживания DHCP.
Failed transfers	В данном поле отображается количество случаев неудавшегося считывания привязок или обновления привязок коммутатором в базе данных отслеживания DHCP.
Successful reads	В этом поле отображается количество успешных считываний привязок коммутатором из базы данных отслеживания DHCP.
Failed reads	В этом поле отображается количество неудавшихся считываний привязок коммутатором из базы данных отслеживания DHCP.
Successful writes	В этом поле отображается количество успешных обновлений привязок коммутатором в базе данных отслеживания DHCP.
Failed writes	В этом поле отображается количество неудавшихся обновлений привязок коммутатором в базе данных отслеживания DHCP.
Database detail	
First successful access	В этом поле отображается время первого обращения коммутатора к базе данных отслеживания DHCP по любой причине.
Last ignored bindings counters	В этом разделе отображается количество случаев и причины, по которым коммутатором были проигнорированы привязки при последней попытке считывания привязок из базы данных отслеживания DHCP. Эти счетчики можно сбросить посредством перезапуска коммутатора или с использованием команд интерфейса командной строки. См. Справочник по интерфейсу командной строки.
Binding collisions	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине наличия в коммутаторе привязки с тем же самым MAC-адресом и идентификатором VLAN ID.
Invalid interfaces	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине того, что номер порта соответствует доверенному интерфейсу или больше не существует.
Parse failures	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине невозможности для коммутатора выделить данные для привязки из базы данных привязок DHCP.
Expired leases	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине окончания срока аренды.
Unsupported vlans	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине прекращения существования сети с указанным VLAN ID.
Last ignored time	В этом поле отображается время последнего игнорирования коммутатором привязок из базы данных отслеживания DHCP по любой причине.
Total ignored bindings counters	В этом разделе отображается количество случаев и причины, по которым коммутатором были проигнорированы привязки при считывании привязок из базы данных отслеживания DHCP за все время. Эти счетчики можно сбросить посредством перезапуска коммутатора или с использованием команд интерфейса командной строки. См. Справочник по интерфейсу командной строки.
Binding collisions	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине наличия в коммутаторе привязки с тем же самым MAC-адресом и идентификатором VLAN ID.

Таблица 73 Экран Advanced Application > IP Source Guard > DHCP Snooping

ПОЛЕ	ОПИСАНИЕ
Invalid interfaces	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине того, что номер порта соответствует доверенному интерфейсу или больше не существует.
Parse failures	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине невозможности для коммутатор выделить данные для привязки из базы данных привязок DHCP.
Expired leases	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине окончания срока аренды.
Unsupported vlans	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине прекращения существования сети с указанным VLAN ID.

24.5 Настройка отслеживания DHCP

С помощью данного экрана можно включить отслеживание DHCP на коммутаторе (но не на конкретных VLAN), указать сеть VLAN, в которой располагается DHCP-сервер по умолчанию, а также настроить базу данных отслеживания DHCP. База данных отслеживания DHCP позволяет хранить текущие привязки на защищенном внешнем сервере TFTP, чтобы они были доступны после перезапуска. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Рисунок 107 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure

Поля экрана описаны в следующей таблице.

Таблица 74 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure

ПОЛЕ	ОПИСАНИЕ
Active	<p>Установите этот переключатель, чтобы включить на коммутаторе функцию отслеживания DHCP. После этого необходимо включить функцию отслеживания DHCP в конкретной сети VLAN и указать доверенные порты.</p> <p>Примечание: Если включить отслеживание DHCP и не определить ни одного доверенного порта, коммутатор будет отбрасывать все запросы DHCP.</p>
DHCP Vlan	<p>Выберите идентификатор VLAN ID, если коммутатор должен пересылать пакеты DHCP к серверам DHCP в конкретной VLAN.</p> <p>Примечание: Для этой VLAN необходимо будет также включить отслеживание DHCP.</p> <p>Чтобы помочь серверам DHCP различать запросы DHCP от различных сетей VLAN, на экране DHCP Snooping VLAN Configure можно включить использование поля Option82 (разд. 24.5.2 на стр. 229).</p> <p>Выберите Disable, если от коммутатора не требуется пересылки пакетов DHCP в конкретную сеть VLAN.</p>
Database	<p>Если значение Timeout interval превышает значение Write delay interval, то следующее плановое обновление может произойти до успешного завершения или тайм-аута текущего обновления. В этом случае коммутатор выжидает с началом следующего обновления до завершения текущего.</p>
Agent URL	<p>Введите расположение базы данных отслеживания DHCP. Расположение должно быть указано в следующем виде: ftfp://{имя домена или IP-адрес}/каталог, если необходимо/имя файла; например, ftfp://192.168.10.1/database.txt.</p>
Timeout interval	<p>Введите, как долго (от 10 до 65535 секунд) коммутатор будет пытаться выполнить конкретное обновление базы данных отслеживания DHCP перед отказом от дальнейших попыток.</p>
Write delay interval	<p>Введите, как долго (от 10 до 65535 секунд) коммутатор будет выжидать перед обновлением базы данных отслеживания DHCP после первого изменения текущих привязок с момента обновления. После определения времени следующего обновления все дополнительные изменения в текущих привязках включаются в это обновление автоматически.</p>
Renew DHCP Snooping URL	<p>Введите расположение базы данных отслеживания DHCP и нажмите на Renew, чтобы коммутатор загрузил ее. Таким образом можно загрузить динамические привязки из другой базы данных отслеживания DHCP, чем указанная в поле Agent URL.</p> <p>При загрузке динамических привязок из базы данных отслеживания DHCP коммутатор предварительно не отбрасывает существующие динамические привязки. В случае конфликта коммутатор сохраняет динамические привязки в энергозависимой памяти и изменяет показания счетчика Binding collisions на экране DHCP Snooping (разд. 24.4 на стр. 222).</p>

Таблица 74 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

24.5.1 Настройка портов отслеживания DHCP

На данном экране можно определить порты как доверенные и не заслуживающие доверия для функции отслеживания DHCP.



Если включить отслеживание DHCP и не определить ни одного доверенного порта, коммутатор будет отбрасывать все запросы DHCP.

Кроме того, можно определить максимальное количество пакетов DHCP, которое может приниматься через каждый из портов (доверенных или не заслуживающих доверия) за секунду. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Рисунок 108 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port

Port	Server Trusted state	Rate (pps)
*	Untrusted	
1	Untrusted	0
2	Untrusted	0
3	Untrusted	0
4	Untrusted	0
5	Untrusted	0
6	Untrusted	0
7	Untrusted	0
8	Untrusted	0

Поля экрана описаны в следующей таблице.

Таблица 75 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port

ПОЛЕ	ОПИСАНИЕ
Port	В этом поле отображается номер порта. При настройке порта * эти настройки применяются ко всем портам.
Server Trusted state	<p>Выберите, будет ли данный порт считаться доверенным (Trusted) или не заслуживающим доверия (Untrusted).</p> <p>Доверенные порты подключаются к серверам DHCP или другим коммутаторам, поэтому коммутатор отбрасывает пакеты DHCP от доверенных портов лишь в том случае, если скорость их поступления слишком высока.</p> <p>Не заслуживающие доверия порты подключаются к абонентам, и коммутатор отбрасывает пакеты DHCP от не заслуживающих доверия портов в следующих случаях:</p> <ul style="list-style-type: none"> • Пакет представляет собой пакет сервера DHCP (например, OFFER, ACK или NACK). • MAC-адрес источника и IP-адрес источника в пакете не соответствуют ни одной из существующих привязок. • Пакет представляет собой пакет типа RELEASE или DECLINE, и MAC-адрес источника и порт источника не соответствуют ни одной из существующих привязок. • Скорость поступления пакетов DHCP слишком высока.
Rate (pps)	Укажите максимальное число пакетов DHCP (1-2048), которое коммутатор может принимать через каждый из портов за секунду. Все пакеты DHCP сверх указанного лимита коммутатором отбрасываются. Значение 0 позволяет отключить данный лимит, что рекомендуется сделать для доверенных портов.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

24.5.2 Настройка VLAN отслеживания DHCP

На данном экране можно включить отслеживание DHCP в каждой из VLAN и указать, должен ли коммутатор добавлять информацию агента ретрансляции DHCP в поле option 82 (гл. 28 на стр. 255) к запросам DHCP, которые коммутатор ретранслирует к серверу DHCP для каждой из VLAN. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

Рисунок 109 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN

Поля экрана описаны в следующей таблице.

Таблица 76 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN

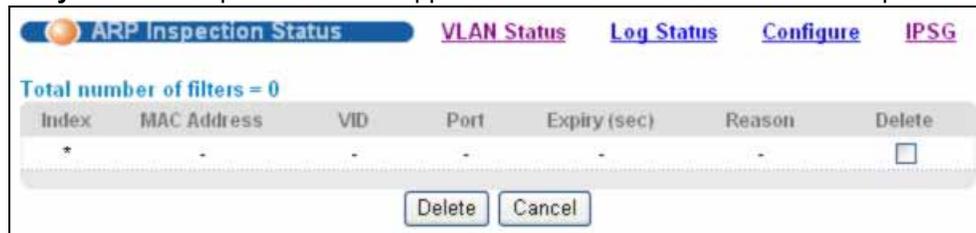
ПОЛЕ	ОПИСАНИЕ
Show VLAN	В данном разделе определяются виртуальные локальные сети VLAN, которые будут настраиваться в разделе ниже.
Start VID	Введите идентификатор начала диапазона для сетей VLAN, которые будут настраиваться в разделе ниже.
End VID	Введите идентификатор конца диапазона для сетей VLAN, которые будут настраиваться в разделе ниже.
Apply	Нажмите на данную кнопку, чтобы отобразить введенный диапазон сетей VLAN в разделе ниже.
VID	В данном поле отображаются идентификаторы VLAN ID каждой из сетей VLAN из выбранного выше диапазона. При настройке VLAN-сети * эти настройки применяются ко всем сетям VLAN.
Enabled	<p>Выберите Yes, чтобы включить отслеживание DHCP в данной сети VLAN. Также необходимо включить функцию отслеживания DHCP на коммутаторе и указать доверенные порты.</p> <p>Примечание: Если включить отслеживание DHCP и не определить ни одного доверенного порта, коммутатор будет отбрасывать все запросы DHCP.</p>
Option82	Установите этот переключатель, чтобы коммутатор добавлял номер слота, номер порта и идентификатор VLAN ID к запросам DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN. Сеть VLAN DHCP указывается на экране DHCP Snooping Configure . См. разд. 24.5 на стр. 226 .
Information	Установите этот переключатель, чтобы коммутатор добавлял имя системы к запросам DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN. Имя системы указывается на экране General Setup . См. гл. 7 на стр. 77 . Сеть VLAN DHCP указывается на экране DHCP Snooping Configure . См. разд. 24.5 на стр. 226 .

Таблица 76 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

24.6 Состояние инспекции ARP-пакетов

На данном экране можно посмотреть текущий список фильтров MAC-адресов, созданных коммутатором в связи с обнаружением несанкционированных пакетов ARP. При обнаружении коммутатором несанкционированного ARP-пакета им автоматически создается фильтр MAC-адресов, блокирующий трафик от MAC-адреса и сети VLAN, от которых поступил несанкционированный ARP-пакет. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection**.

Рисунок 110 Экран Advanced Application > IP Source Guard > ARP Inspection

Поля экрана описаны в следующей таблице.

Таблица 77 Экран Advanced Application > IP Source Guard > ARP Inspection

ПОЛЕ	ОПИСАНИЕ
Total number of filters	В данном поле отображается общее количество фильтров MAC-адресов, созданных коммутатором в связи с обнаружением несанкционированных пакетов ARP.
Index	В этом поле отображается порядковый номер фильтра MAC-адресов.
MAC Address	В этом поле отображается MAC-адрес источника для фильтра MAC-адресов.
VID	В этом поле отображается идентификатор VLAN для фильтра MAC-адресов.
Port	В этом поле отображается порт источника для отброшенного пакета ARP.
Expiry (sec)	В этом поле отображается период времени (в секундах), в течение которого фильтр MAC-адресов будет действовать на коммутаторе. Запись можно удалить вручную (Delete).

Таблица 77 Экран Advanced Application > IP Source Guard > ARP Inspection

ПОЛЕ	ОПИСАНИЕ
Reason	В этом поле отображается причина, по которой был отброшен пакет ARP. MAC+VLAN: MAC-адрес и идентификатор VLAN ID не найдены в таблице привязок. IP: MAC-адрес и идентификатор VLAN ID найдены в таблице привязок, но IP-адрес недействителен. Port: MAC-адрес, идентификатор VLAN ID и IP-адрес найдены в таблице привязок, но номер порта недействителен.
Delete	Установите переключатель и нажмите на Delete , чтобы удалить выбранную запись.
Delete	Нажмите на данную кнопку, чтобы удалить выбранные записи.
Cancel	Нажмите на данную кнопку, чтобы снять выделение с переключателей Delete .

24.6.1 Состояние сети VLAN для инспекции ARP-пакетов

На данном экране можно просмотреть различные статистические данные по пакетам ARP в каждой из сетей VLAN. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Рисунок 111 Экран ARP Inspection VLAN Status

Поля экрана описаны в следующей таблице.

Таблица 78 Экран ARP Inspection VLAN Status

ПОЛЕ	ОПИСАНИЕ
Show VLAN range	В данном разделе определяются виртуальные локальные сети VLAN, которые будут отображаться в разделе ниже.
Enabled VLAN	Выберите этот переключатель, чтобы отобразить в разделе ниже все виртуальные локальные сети VLAN, на которых включена инспекция ARP-пакетов.
Selected VLAN	Выберите данный переключатель, чтобы отобразить в разделе ниже все виртуальные локальные сети VLAN из указанного диапазона. После этого введите наименьший идентификатор VLAN ID (в поле Start VID) и наибольший идентификатор VLAN ID (в поле End VID) для требуемого диапазона.
Apply	Нажмите на данную кнопку, чтобы отобразить введенный диапазон сетей VLAN в разделе ниже.

Таблица 78 Экран ARP Inspection VLAN Status

ПОЛЕ	ОПИСАНИЕ
VID	В данном поле отображаются идентификаторы VLAN ID каждой из сетей VLAN из выбранного выше диапазона.
Received	В этом поле отображается общее количество ARP-пакетов, полученных из данной VLAN с момента последнего перезапуска коммутатора.
Request	В этом поле отображается общее количество ARP-пакетов типа Request, полученных из данной VLAN с момента последнего перезапуска коммутатора.
Reply	В этом поле отображается общее количество ARP-пакетов типа Reply, полученных из данной VLAN с момента последнего перезапуска коммутатора.
Forwarded	В этом поле отображается общее количество ARP-пакетов, направленных коммутатором в данную VLAN с момента последнего перезапуска коммутатора.
Dropped	В этом поле отображается общее количество ARP-пакетов для данной VLAN, отброшенных коммутатором с момента последнего перезапуска коммутатора.

24.6.2 Состояние журнала инспекции ARP-пакетов

На данном экране можно просмотреть сообщения контрольного журнала, сгенерированные пакетами ARP, которые еще не были отправлены на сервер syslog. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Рисунок 112 Экран Advanced Application > IP Source Guard > ARP Inspection > Log Status



Поля экрана описаны в следующей таблице.

Таблица 79 Экран Advanced Application > IP Source Guard > ARP Inspection > Log Status

ПОЛЕ	ОПИСАНИЕ
Clearing log status table	Нажатие на Apply позволяет удалить все сообщения контрольного журнала, сгенерированные пакетами ARP, которые еще не были отправлены на сервер syslog.
Total number of logs	В данном поле отображается количество сообщений контрольного журнала, сгенерированных пакетами ARP, которые еще не были отправлены на сервер syslog. В случае отбрасывания одного или нескольких сообщений контрольного журнала из-за недоступности буфера соответствующие записи помечаются как overflow , с указанием текущего количества отброшенных сообщений.
Index	В этом поле отображается порядковый номер сообщения контрольного журнала.
Port	В этом поле отображается порт источника пакета ARP.
VID	В этом поле отображается идентификатор VLAN источника пакета ARP.
Sender MAC	В этом поле отображается MAC-адрес источника пакета ARP.
Sender IP	В этом поле отображается IP-адрес источника пакета ARP.
Num Pkts	В этом поле отображается количество пакетов ARP, консолидированных в данном сообщении контрольного журнала. Данный коммутатор консолидирует в одно сообщение идентичные сообщения контрольного журнала, сгенерированные пакетами ARP, за установленный период консолидации. Это период настраивается на экране ARP Inspection Configure . См. разд. 24.7 на стр. 235 .
Reason	В этом поле отображается причина, по которой было сгенерировано сообщение контрольного журнала. dhcp deny : ARP-пакет был отброшен из-за нарушения динамической привязки MAC-адреса и идентификатора VLAN ID. static deny : ARP-пакет был отброшен из-за нарушения статической привязки MAC-адреса и идентификатора VLAN ID. deny : ARP-пакет был отброшен из-за отсутствия статической привязки MAC-адреса и идентификатора VLAN ID. dhcp permit : Коммутатор переслал ARP-пакет, так как была найдена динамическая привязка. static permit : Коммутатор переслал ARP-пакет, так как была найдена статическая привязка. На экране ARP Inspection VLAN Configure можно настроить коммутатор таким образом, чтобы он генерировал сообщения контрольного журнала при отбрасывании или пересылке пакетов ARP в зависимости от идентификатора VLAN ID пакета ARP. См. разд. 24.7.2 на стр. 238 .
Time	В этом поле отображается время, в которое было сгенерировано сообщение контрольного журнала.

24.7 Настройка инспекции ARP-пакетов

На данном экране производится настройка функции инспекции ARP-пакетов на коммутаторе. Кроме того, можно настроить период времени, в течение которого коммутатор хранит записи об отброшенных пакетах ARP, а также определить глобальные параметры контрольного журнала функции инспекции ARP-пакетов. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Рисунок 113 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure

Поля экрана описаны в следующей таблице.

Таблица 80 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на коммутаторе функцию инспекции ARP-пакетов. После этого необходимо включить функцию инспекции ARP-пакетов в конкретной сети VLAN и указать доверенные порты.
Filter Aging Time	
Filter aging time	Данная настройка не влияет на существующие фильтры MAC-адресов. Введите период времени (1-2147483647 секунд), в течение которого фильтр MAC-адресов будет действовать на коммутаторе с момента обнаружения коммутатором несанкционированного пакета ARP. По истечению этого времени фильтр MAC-адресов автоматически удаляется коммутатором. Чтобы фильтр MAC-адреса действовал постоянно, необходимо ввести в это поле значение 0.
Log Profile	

Таблица 80 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure

ПОЛЕ	ОПИСАНИЕ
Log buffer size	<p>Введите максимальное количество сообщений контрольного журнала (0-1024), которые могут быть сгенерированы пакетами ARP до отправки на сервер syslog. Данное значение должно соответствовать указанным значениям параметров Syslog rate и Log interval.</p> <p>Если количество сообщений контрольного журнала на коммутаторе превысит это значение, коммутатор остановит запись сообщений контрольного журнала и будет только подсчитывать количество записей, которые были отброшены из-за нехватки места в буфере. Для очистки контрольного журнала и сброса данного счетчика нажмите на Clearing log status table на экране ARP Inspection Log Status. См. разд. 24.6.2 на стр. 233.</p>
Syslog rate	<p>Введите максимальное количество сообщений syslog, которые коммутатор может передать на сервер syslog в одной партии. Данное количество выражается в виде скорости, так как периодичность отправки партий устанавливается параметром Log Interval. Для использования этой функции необходимо настроить сервер syslog (гл. 32 на стр. 293). Чтобы коммутатор не отправлял сообщения контрольного журнала, генерируемые пакетами ARP, на сервер syslog, введите в данное поле значение 0.</p> <p>Взаимосвязь между параметрами Syslog rate и Log interval иллюстрируют следующие примеры:</p> <ul style="list-style-type: none"> • 4 недействительных пакета ARP в секунду, Syslog rate равен 5, Log interval равен 1: коммутатор будет отправлять 4 сообщения syslog каждую секунду. • 6 недействительных пакетов ARP в секунду, Syslog rate равен 5, Log interval равен 2: коммутатор будет отправлять 10 сообщения syslog каждые 2 секунды.
Log interval	<p>Введите периодичность (0-86400 секунд), с которой коммутатор будет отправлять партии сообщений syslog на сервер syslog. Чтобы сообщения отправлялись коммутатором на сервер syslog немедленно, введите в это поле значение 0. Пример взаимосвязи между параметрами Syslog rate и Log interval приводится в описании параметра Syslog rate.</p>
Apply	<p>Нажмите Apply, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.</p>
Cancel	<p>Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.</p>

24.7.1 Настройка портов для инспекции ARP-пакетов

На данном экране можно определить порты как доверенные и не заслуживающие доверия для функции инспекции ARP-пакетов. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Рисунок 114 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > Port

Port	Trusted State	Limit	
		Rate (pps)	Burst interval (seconds)
*	Untrusted		
1	Untrusted	15	1
2	Untrusted	15	1
3	Untrusted	15	1
4	Untrusted	15	1
5	Untrusted	15	1
6	Untrusted	15	1
7	Untrusted	15	1
8	Untrusted	15	1

Поля экрана описаны в следующей таблице.

Таблица 81 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > Port

ПОЛЕ	ОПИСАНИЕ
Port	В этом поле отображается номер порта. При настройке порта * эти настройки применяются ко всем портам.
Trusted State	<p>Выберите, будет ли данный порт считаться доверенным (Trusted) или не заслуживающим доверия (Untrusted).</p> <p>Пакеты ARP, приходящие через доверенные порты, коммутатором не отбрасываются ни по какой причине.</p> <p>От не заслуживающих доверия портов коммутатор отбрасывает ARP-пакеты в следующих случаях:</p> <ul style="list-style-type: none"> Информация об отправителе в ARP-пакете не совпадает с одной из существующих привязок. Скорость поступления пакетов ARP слишком высока. Можно указать максимальную скорость, с которой будут приниматься ARP-пакеты через не заслуживающие доверия порты.
Limit	Для доверенных портов данные настройки безразличны
Rate (pps)	Укажите максимальную скорость (0-2048 пакетов в секунду), с которой коммутатор будет принимать ARP-пакеты через каждый из портов. Все пакеты ARP сверх указанного лимита коммутатором отбрасываются. Значение 0 позволяет отключить данный лимит.
Burst interval (seconds)	Под этим значением понимается период времени, в течение которого контролируется скорость поступления ARP-пакетов через каждый порт. Например, если скорость установлена равной 15 пакетам в секунду, а данный интервал – 1 секунде, то коммутатор принимает максимум 15 ARP-пакетов за каждый из интервалов продолжительностью в одну секунду. Если интервал установить равным 5 секундам, то коммутатор будет принимать максимум 75 ARP-пакетов в течение каждого пятисекундного интервала. Введите продолжительность интервала оценки (1-15 секунд).

Таблица 81 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > Port (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

24.7.2 Настройка сети VLAN для инспекции ARP-пакетов

На данном экране можно включить инспекцию ARP-пакетов для каждой виртуальной локальной сети и указать, должен ли коммутатор генерировать сообщения контрольного журнала при получении пакетов ARP от каждой из сетей VLAN. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Рисунок 115 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN

Поля экрана описаны в следующей таблице.

Таблица 82 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN

ПОЛЕ	ОПИСАНИЕ
VLAN	В данном разделе определяются виртуальные локальные сети VLAN, которые будут настраиваться в разделе ниже.
Start VID	Введите идентификатор начала диапазона для сетей VLAN, которые будут настраиваться в разделе ниже.
End VID	Введите идентификатор конца диапазона для сетей VLAN, которые будут настраиваться в разделе ниже.
Apply	Нажмите на данную кнопку, чтобы отобразить введенный диапазон сетей VLAN в разделе ниже.
VID	В данном поле отображаются идентификаторы VLAN ID каждой из сетей VLAN из выбранного выше диапазона. При настройке VLAN-сети * эти настройки применяются ко всем сетям VLAN.

Таблица 82 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Enabled	Выберите Yes , чтобы включить инспекцию ARP-пакетов в данной сети VLAN. Выберите No , чтобы отключить инспекцию ARP-пакетов в данной сети VLAN.
Log	Укажите, должен ли коммутатор генерировать сообщения контрольного журнала при получении пакетов ARP от данной VLAN. None : коммутатор не генерирует никаких сообщений контрольного журнала при получении пакетов ARP от данной VLAN. Deny : коммутатор генерирует сообщения контрольного журнала при отбрасывании пакета ARP от данной VLAN. Permit : коммутатор генерирует сообщения контрольного журнала при пересылке пакетов ARP от данной VLAN. All : коммутатор генерирует сообщения контрольного журнала при каждом получении пакетов ARP от данной VLAN.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

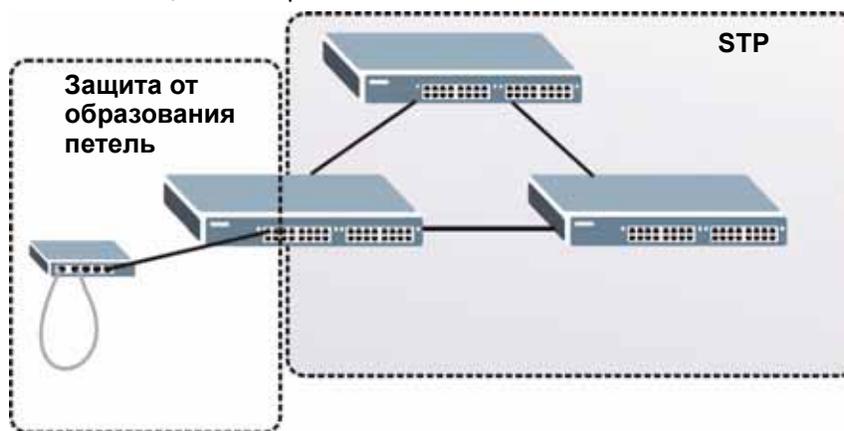
Защита от образования петель

В данной главе описана настройка на коммутаторе механизма защиты от образования петель на границе сети.

25.1 Обзор функции защиты от образования петель

Функция защиты от образования петель позволяет настроить на коммутаторе отключение определенного порта при обнаружении ситуации, когда отправляемые через этот порт пакеты возвращаются на коммутатор. Для защиты от образования петель в опорной сети можно использовать протокол покрывающего дерева (STP), однако STP не обеспечивает защиты от петель, которые могут возникнуть на границе сети.

Рисунок 116 Защита от образования петель и STP



Функция защиты от образования петель предназначена специально для устранения проблем на границе сети. Проблема может возникнуть при подключении порта к коммутатору, на котором образовалась петля. Петля образуется в результате человеческой ошибки. Она возникает, когда два порта коммутатора оказываются соединенными одним кабелем. При рассылке коммутатором с петлей широковещательных сообщений они возвращаются на коммутатор и повторно ретранслируются снова и снова, вызывая широковещательный шторм.

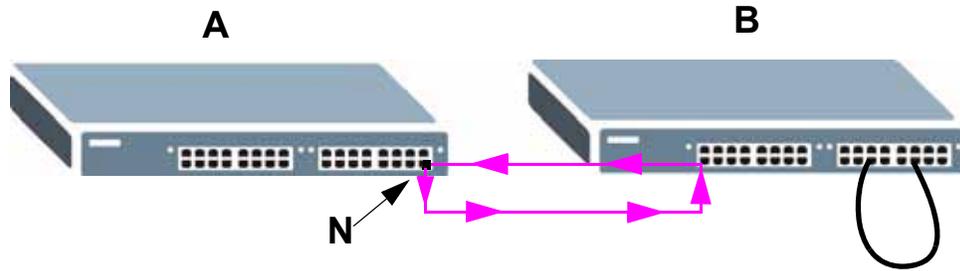
При подключении коммутатора (без петли) к коммутатору с петлей проблемы последнего отражаются на первом следующим образом:

- Он будет принимать широковещательные сообщения, рассылаемые коммутатором с петлей.

- Он будет получать собственные широковещательные сообщения, так как они будут возвращаться по петле к нему. После этого эти сообщения будут ретранслироваться коммутатором повторно.

На приведенном ниже рисунке показано подключение порта **N** на коммутаторе **A** к коммутатору **B**. На коммутаторе **B** образовалась петля. При выходе широковещательных или мультивещательных сообщений из порта **N** и их поступлении на коммутатор **B** эти сообщения вновь направляются на порт **N** коммутатора **A**, после их ретрансляции коммутатором **B**.

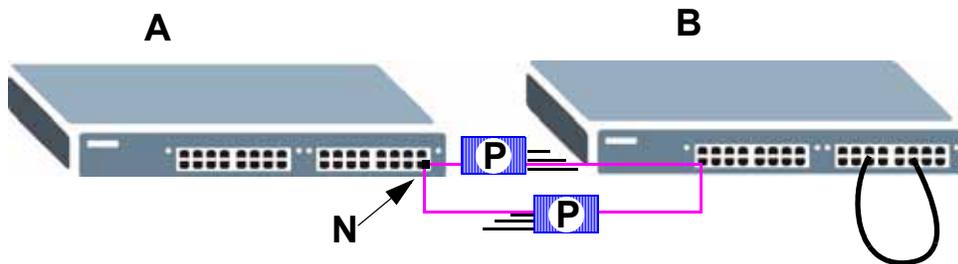
Рисунок 117 Коммутатор с петлей



Функция защиты от образования петель проверяет, не подключен ли порт с активированной функцией к коммутатору с петлей. Для этого она периодически рассылает пробные пакеты и проверяет, не возвращаются ли эти пакеты через тот же самый порт. При обнаружении такого события коммутатор отключает порт, который подключен к коммутатору с петлей.

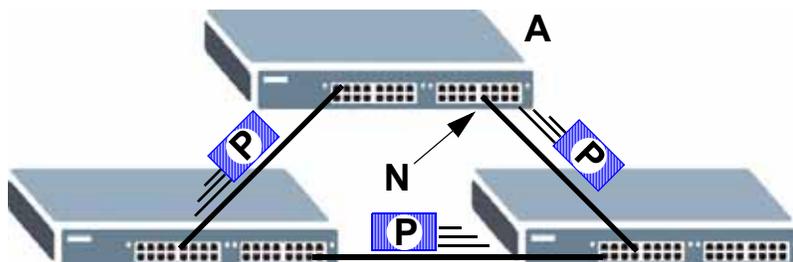
На приведенном ниже рисунке показан коммутатор **A** с активированной на порту **N** функцией защиты от образования петель, который отправляет пробный пакет **P** на коммутатор **B**. Так как на коммутаторе **B** имеется петля, пробный пакет **P** возвращается на порт **N** коммутатора **A**. Для защиты остальной части сети от коммутатора с петлей данный коммутатор отключает порт **N**.

Рисунок 118 Защита от образования петель – пробный пакет



Данный коммутатор также отключит порт **N**, если пробный пакет вернется на коммутатор **A** через любой другой порт. Другими словами, функция защиты от образования петель защищает также от обычных петель в сети. На приведенном ниже рисунке показан пример с тремя коммутаторами, образующими петлю. На рисунке также показан путь пробного пакета, отправляемого функцией защиты от образования петель. В данном примере пробный пакет отправляется из **N** и возвращается на другой порт. Если на порту **N** включена функция защиты от образования петель, коммутатор отключит порт **N** после обнаружения пробного пакета, вернувшегося на коммутатор.

Рисунок 119 Защита от образования петель – петля в сети



После устранения проблемы с петлей в сети отключенный порт можно снова активировать через Web-конфигуратор (см. [разд. 7.7 на стр. 87](#)) или интерфейс командной строки (см. [Справочник по интерфейсу командной строки](#)).

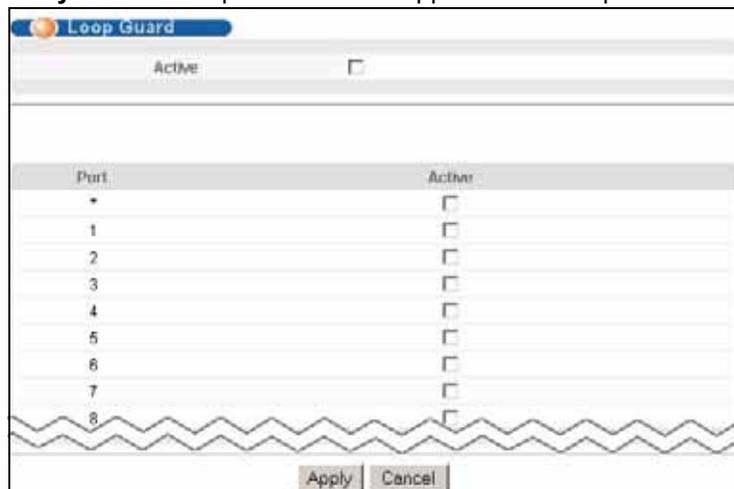
25.2 Настройка защиты от образования петель

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application > Loop Guard**.



Функция защиты от образования петель не может быть включена на портах, для которых включен протокол покрывающего дерева (RSTP, MRSTP или MSTP).

Рисунок 120 Экран Advanced Application > Loop Guard



Поля экрана описаны в следующей таблице.

Таблица 83 Экран Advanced Application > Loop Guard

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить защиту от образования петель на коммутаторе. При отключении порта в результате действия функции защиты от образования петель коммутатор генерирует сообщения syslog, сообщения внутреннего контрольного журнала, а также «ловушки» SNMP.
Port	В этом поле отображается номер порта.
*	С помощью этой строки можно настроить одновременно все порты. С помощью этой строки можно назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить защиту от образования петель для данного порта. Данный коммутатор будет отправлять пробные пакеты через этот порт для проверки, не подключен ли он к коммутатору с петлей. В случае обнаружения подключения данного порта к коммутатору с петлей данный коммутатор отключит этот порт. Снимите выделение с переключателя, если необходимо отключить эту функцию защиты от образования петель.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Статические маршруты

В данной главе описана настройка статических маршрутов.

26.1 Настройка статических маршрутов

Взаимодействие данного коммутатора с управляющими компьютерами осуществляется через IP-подключение (например, с использованием HTTP, telnet, SSH или SNMP). С помощью статических IP-маршрутов коммутатор может отвечать удаленным станциям управления, недоступным через шлюз по умолчанию. Кроме того, статические маршруты могут использоваться коммутатором для отправки данных на сервер или устройство, недоступные через шлюз по умолчанию, например, для передачи «ловушек» SNMP или использования команды ping при проверке IP-подключения.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application > Static Routing**.

Рисунок 121 Экран IP Application > Static Routing

Поля экрана, используемые для создания статического маршрута, описаны в следующей таблице.

Таблица 84 Экран IP Application > Static Routing

ПОЛЕ	ОПИСАНИЕ
Active	В этом поле можно активировать/деактивировать данный статический маршрут.
Name	Введите имя-описание (до 10 отображаемых ASCII-символов), по которому можно идентифицировать эту запись.

Таблица 84 Экран IP Application > Static Routing (продолжение)

ПОЛЕ	ОПИСАНИЕ
Destination IP Address	Сетевой IP-адрес конечного пункта назначения. Маршрутизация всегда основывается на номере сети. Если нужно указать маршрут к конкретному хосту, в поле ввода маски подсети необходимо ввести маску 255.255.255.255, и тогда в качестве номера сети можно использовать идентификатор требуемого хоста.
IP Subnet Mask	Введите маску подсети для данного направления.
Gateway IP Address	Введите IP-адрес шлюза. Шлюз – это ближайший сосед коммутатора, который направляет пакет к пункту его назначения. Шлюз должен быть маршрутизатором в том же сегменте, что и коммутатор.
Metric	Метрика отражает «стоимость» передачи для целей маршрутизации. В IP-маршрутизации в качестве меры стоимости используется счетчик пройденных узлов, с минимальным значением 1 для сетей, соединенных напрямую. Введите число, примерно отражающее стоимость данного канала. Это число не обязательно должно быть точным, но оно должно находиться в диапазоне от 1 до 15. На практике обычно подходит 2 или 3.
Add	Нажмите Add , чтобы сохранить новый статический маршрут в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоа в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clear	Нажмите Clear , чтобы вернуться к заводским настройкам.
Index	В этом поле отображается порядковый номер маршрута. Нажмите на него, чтобы редактировать запись статического маршрута.
Active	В этом поле стоит Yes , если статический маршрут активирован, и No , если он отключен.
Name	В этом поле отображается имя-описание маршрута. Оно будет использоваться только для идентификации.
Destination Address	В этом поле отображается сетевой IP-адрес конечного пункта назначения.
Subnet Mask	В этом поле отображается маска подсети для данного направления.
Gateway Address	В этом поле отображается IP-адрес шлюза. Шлюз – это ближайший сосед коммутатора, который направляет пакет к пункту его назначения.
Metric	В этом поле отображается «стоимость» передачи для целей маршрутизации.
Delete	Нажмите Delete , чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

Дифференцированное обслуживание

В данной главе описана настройка на коммутаторе механизмов дифференцированного обслуживания (DiffServ).

27.1 Обзор механизма DiffServ

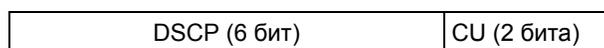
Механизмы управления качеством обслуживания (QoS) позволяют установить приоритеты для потоков трафика из источника в пункт назначения. Все пакеты в потоке получают одинаковый приоритет. Чтобы установить различные приоритеты для различных типов пакетов, можно использовать классы обслуживания (CoS).

DiffServ представляет собой модель на базе классов обслуживания (CoS), в которой пакеты маркируются таким образом, чтобы на пути следования маршрута на сетевых устройствах с поддержкой DiffServ они подвергались особой обработке на каждом конкретном переходе в зависимости от типа приложения и плотности трафика. Пакеты маркируются кодовыми маркерами DiffServ (DiffServ Code Points, DSCP), которые указывают на желаемый уровень обслуживания. Это позволяет промежуточным сетевым устройствам с поддержкой DiffServ обрабатывать пакеты различным образом в зависимости от маркера, без необходимости согласования путей или запоминания информации о состоянии для каждого потока. Кроме того, приложениям не требуется запрашивать конкретное обслуживание или выдавать предварительное уведомление о том, куда направляется трафик.

27.1.1 Маркер DSCP и обработка на каждом конкретном переходе

При использовании DiffServ в заголовок IP-пакетов добавляется новое поле DS (Differentiated Services), которое заменяет поле типа обслуживания ToS (Type of Service). Поле DS содержит 6-битное поле маркера DSCP, которое позволяет определить до 64 уровней обслуживания, а оставшиеся 2 бита на данный момент не используются (currently unused, CU). Поле DS изображено на следующем рисунке.

Рисунок 122 DiffServ: поле Differentiated Service



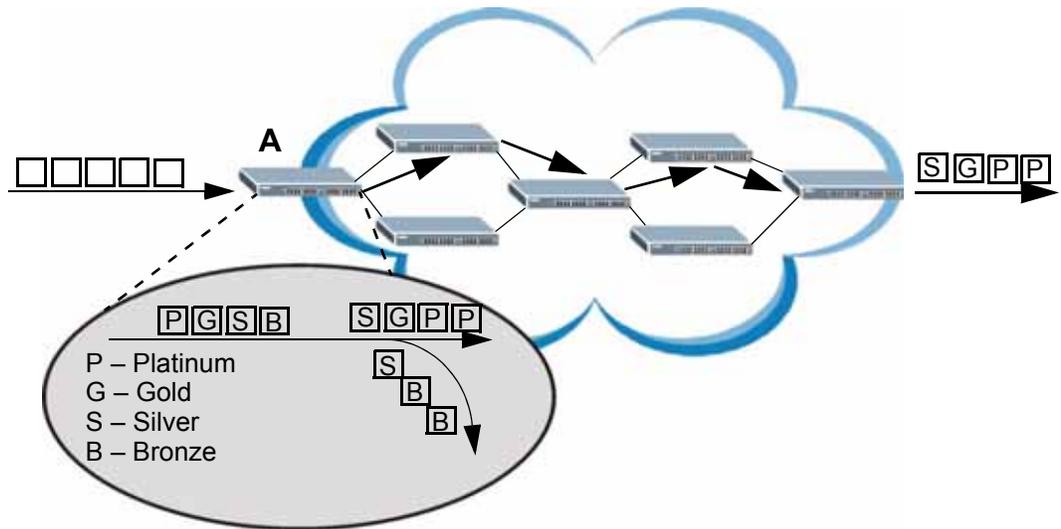
Маркер DSCP обратно совместим с тремя битами приоритета в октете ToS, благодаря чему сетевое устройство с поддержкой ToS, но без поддержки DiffServ не будет конфликтовать с отображением маркера DSCP.

Значение DSCP определяет так называемую обработку на каждом конкретном переходе (PHB, Per-Hop Behavior), которая осуществляется над каждым пакетом при пересылке по сети с поддержкой DiffServ. В зависимости от правила маркирования различные типы трафика могут получать различные приоритеты пересылки. Ресурсы могут быть распределены соответственно значениям DSCP и настроенным политикам.

27.1.2 Пример сети с поддержкой DiffServ

Пример простой сети с поддержкой DiffServ, состоящей из нескольких подключенных напрямую сетевых устройств с поддержкой DiffServ, показан на следующем рисунке. Граничный узел (A на рис. 123) в сети DiffServ классифицирует (помечает маркером DSCP) входящие пакеты, разделяя их на различные потоки трафика (**Platinum**, **Gold**, **Silver**, **Bronze**) на основе настроенных правил маркирования. После этого сетевой администратор может применять к потокам трафика различные политики. Один из примеров такой политики – назначение более высокого приоритета отбрасывания одному из потоков трафика по сравнению с другими. В нашем примере у пакетов потока трафика **Bronze** вероятность отбрасывания при перегрузках в процессе движения по сети DiffServ больше, чем у пакетов потока трафика **Platinum**.

Рисунок 123 Сеть с поддержкой DiffServ



27.2 Ограничение трафика с использованием маркеров TRTSM

Функция ограничения трафика позволяет ограничить скорость входящего или исходящего трафика в зависимости от класса трафика с использованием определяемых пользователем критериев. Методы ограничения трафика оценивают потоки трафика на основе определяемых пользователем критериев и идентифицируют трафик как отвечающий критериям, превышающий критерии или нарушающий критерии.

Маркеры TRTCM (Two Rate Three Color Marker, определенные в RFC 2698) – один из типов ограничения трафика, в котором идентификация пакетов осуществляется на основании сравнения с двумя установленным пользователем скоростями: гарантированной скорости передачи информации (CIR) и пиковой скорости передачи информации (PIR). CIR определяет среднюю скорость, с которой пакеты допускаются в сеть. Значение PIR выбирается большим или равным CIR. Значения CIR и PIR базируются на гарантированной и максимальной пропускной способности, соответственно, согласованных между провайдером услуг и клиентом.

При использовании метода Two Rate Three Color (две скорости, три цвета) поступающие пакеты оцениваются и маркируются одним из трех цветов, определяющие приоритеты при отбрасывании пакетов. Высокий уровень приоритета при отбрасывании пакетов обозначается красным, средний уровень – желтым, а низкий – зеленым. После настройки TRTCM и включения DiffServ над пакетами с цветовой маркировкой выполняются следующие действия:

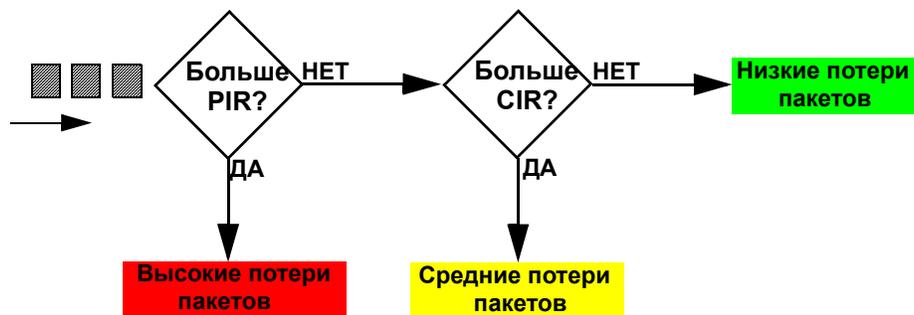
- Красные пакеты (с высоким приоритетом отбрасывания) отбрасываются.
- Желтые пакеты (со средним приоритетом отбрасывания) отбрасываются в случае перегрузки в сети.
- Зеленые пакеты (с низким приоритетом отбрасывания) пересылаются.

TRTCM может работать в одном из двух режимов: без учета цвета и с учетом цвета. В режиме без учета цвета (color-blind) маркировка пакетов осуществляется посредством их оценки относительно параметров PIR и CIR, независимо от предыдущей маркировки. В режиме с учетом цвета (color-aware) маркировка пакетов осуществляется с учетом как текущего цвета, так и оценки относительно параметров PIR и CIR. Если пакеты не попадают под маркировку ни одним из цветов, они передаются в неизменном виде.

27.2.1 TRTCM – режим без учета цвета

Все пакеты оцениваются по скорости PIR. Пакеты, поступающие со скоростью выше PIR, помечаются красным. В противном случае пакеты оцениваются по скорости CIR. Пакеты, поступающие со скоростью выше CIR, помечаются желтым. Все остальные пакеты (поступающие со скоростью ниже CIR) помечаются зеленым.

Рисунок 124 TRTCM – режим без учета цвета

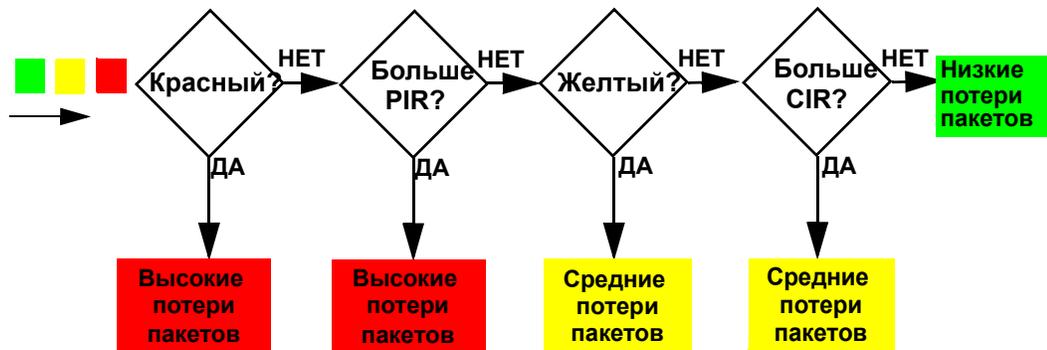


27.2.2 TRTSM – режим с учетом цвета

В режиме с учетом цвета при оценке пакетов учитывается ранее назначенный приоритет отбрасывания. TRTSM может увеличить приоритет отбрасывания пакетов, однако не может его уменьшить. Пакеты, ранее помеченные красным или желтым, могут быть промаркированы цветом с тем же самым или более высоким приоритетом отбрасывания.

Пакеты, промаркированные красным (с высоким приоритетом отбрасывания), остаются красными без оценки относительно параметров PIR и CIR. Пакеты, промаркированные желтым, могут быть промаркированы красным или остаться желтыми, в связи с чем они оцениваются только относительно PIR. Только пакеты, промаркированные зеленым, оцениваются относительно PIR и затем, если их скорость меньше PIR, оцениваются относительно CIR.

Рисунок 125 TRTSM – режим с учетом цвета



27.3 Активация механизма DiffServ

Включение DiffServ позволяет применять правила маркирования или отображение приоритетов IEEE 802.1p на выбранных портах.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application > DiffServ**.

Рисунок 126 Экран IP Application > DiffServ

Port	Active
*	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

Поля экрана описаны в следующей таблице.

Таблица 85 Экран IP Application > DiffServ

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить поддержку DiffServ на коммутаторе.
Port	В этом поле отображается порядковый номер порта коммутатора.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите переключатель Active , чтобы включить DiffServ для соответствующего порта.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

27.3.1 Настройка маркировки TRTCM

Настройка маркировки TRTCM осуществляется на следующем экране. Чтобы отобразить показанный ниже экран, нажмите на экране **DiffServ** ссылку **2-rate 3 Color Marker**.



Включить одновременно TRTSM и управление пропускной способностью невозможно.

Рисунок 127 Экран IP Application > DiffServ > 2-rate 3 Color Marker

Port	Active	Commit Rate	Peak Rate	DSCP				
				green	yellow	red		
*	<input type="checkbox"/>	<input type="text"/>	Kbps	<input type="text"/>	Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
1	<input type="checkbox"/>	0	Kbps	0	Kbps	26	28	30
2	<input type="checkbox"/>	0	Kbps	0	Kbps	26	28	30
3	<input type="checkbox"/>	0	Kbps	0	Kbps	26	28	30
4	<input type="checkbox"/>	0	Kbps	0	Kbps	26	28	30
5	<input type="checkbox"/>	0	Kbps	0	Kbps	26	28	30
6	<input type="checkbox"/>	0	Kbps	0	Kbps	26	28	30
7	<input type="checkbox"/>	0	Kbps	0	Kbps	26	28	30
8	<input type="checkbox"/>	0	Kbps	0	Kbps	26	28	30

Поля экрана описаны в следующей таблице.

Таблица 86 Экран IP Application > DiffServ > 2-rate 3 Color Marker

ПОЛЕ	ОПИСАНИЕ
Active	<p>Установите этот переключатель, чтобы включить на коммутаторе маркировку TRTSM (Two Rate Three Color Marker). Данный коммутатор оценивает и маркирует пакеты с использованием настроек TRTSM.</p> <p>Примечание: Чтобы коммутатор отбрасывал пакеты с красной маркировкой (высоким приоритетом отбрасывания), необходимо также включить DiffServ на коммутаторе и на отдельных портах.</p>
Mode	<p>Выберите color-blind, чтобы коммутатор обрабатывал все поступающие пакеты как не имеющие цветовой маркировки. При этом все поступающие пакеты оцениваются на основе параметров CIR и PIR.</p> <p>Выберите color-aware, чтобы пакеты маркировались с учетом предыдущей маркировки. При этом все поступающие оцениваются на основе существующей цветовой маркировки. Поступающие пакеты без цветовой маркировкой проходят через коммутатор.</p>
Port	В этом поле отображается порядковый номер порта коммутатора.

Таблица 86 Экран IP Application > DiffServ > 2-rate 3 Color Marker (продолжение)

ПОЛЕ	ОПИСАНИЕ
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы активировать TRTSM на порту.
Commit Rate	Укажите гарантированную скорость передачи информации (CIR) для данного порта.
Peak Rate	Укажите пиковую скорость передачи информации (PIR) для данного порта.
DSCP	В данном разделе можно указать, какие значения кодовых маркеров DSCP должны назначаться пакетам в зависимости от их цвета, который они получают в результате обработки TRTSM.
green	Укажите значение DSCP, которое назначается пакетам с низким приоритетом отбрасывания.
yellow	Укажите значение DSCP, которое назначается пакетам со средним приоритетом отбрасывания.
red	Укажите значение DSCP, которое назначается пакетам с высоким приоритетом отбрасывания.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоа в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

27.4 Настройка отображения маркеров DSCP на приоритеты IEEE 802.1p

Настройка отображения маркеров DSCP на приоритеты IEEE 802.1p позволяет коммутатору определять приоритеты всего трафика по значению входящих маркеров DSCP, согласно таблице отображения маркеров DiffServ на приоритеты IEEE 802.1p.

Отображение маркеров DSCP на приоритеты IEEE802.1P по умолчанию показано в следующей таблице.

Таблица 87 Отображение маркеров DSCP на приоритеты IEEE 802.1p по умолчанию

ЗНАЧЕНИЕ DSCP	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

27.4.1 Настройка DSCP

Чтобы изменить отображение маркеров DSCP на приоритеты IEEE 802.1p, выберите **DSCP Setting** на экране **DiffServ**. Появится экран, показанный ниже.

Рисунок 128 Экран IP Application > DiffServ > DSCP Setting

The screenshot shows a configuration screen titled "DSCP Setting" with a subtitle "DSCP to 802.1p Mapping". It features a table with 64 rows (DSCP values 0 to 63) and 8 columns (IEEE 802.1p priority values 0 to 7). Each cell contains a dropdown menu. At the bottom, there are "Apply" and "Cancel" buttons.

DSCP	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2
3	3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4	4
5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6
7	7	7	7	7	7	7	7	7

Поля экрана описаны в следующей таблице.

Таблица 88 Экран IP Application > DiffServ > DSCP Setting

ПОЛЕ	ОПИСАНИЕ
0 ... 63	Идентификационные номера классификации DSCP. Чтобы определить отображение на приоритет IEEE 802.1p, выберите уровень приоритета в ниспадающем списке.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

В данной главе описана настройка функции DHCP.

28.1 Обзор DHCP

Протокол динамической конфигурации хоста DHCP (Dynamic Host Configuration Protocol, документы RFC 2131 и RFC 2132) позволяет отдельным компьютерам получать настройки TCP/IP с сервера при загрузке. Данный коммутатор можно настроить в качестве агента ретрансляции DHCP. При настройке коммутатора в качестве агента ретрансляции коммутатор пересылает запросы DHCP на сетевой сервер DHCP. Если не настраивать коммутатор в качестве агента ретрансляции DHCP, сервер DHCP должен находиться в широковещательном домене клиентских компьютеров или клиентские компьютеры должны настраиваться вручную.

28.1.1 Режимы DHCP

Если в сети уже имеется сервер DHCP, данный коммутатор можно настроить в качестве агента ретрансляции DHCP. При получении коммутатором запроса от клиентского компьютера он обращается к серверу DHCP для получения нужной информации о протоколе IP, а затем передает полученные настройки обратно на компьютер.

28.1.2 Варианты настройки DHCP

Настройки DHCP на коммутатор осуществляются на экранах **Global** и **VLAN**. Выбор экрана для настройки зависит от тех служб DHCP, которые должны быть предоставлены клиентам DHCP в сети. При выборе руководствуйтесь следующими критериями:

- **Global** – коммутатор пересылает все запросы DHCP на один и тот же сервер DHCP.
- **VLAN** – коммутатор настраивается на уровне отдельной VLAN. Для клиентов из различных VLAN коммутатор может передавать запросы DHCP к различным серверам DHCP.

28.2 Состояние DHCP

Выберите в навигационной панели **IP Application > DHCP**. Появится экран **DHCP Status**.

Рисунок 129 Экран IP Application > DHCP Status

Поля экрана описаны в следующей таблице.

Таблица 89 Экран IP Application > DHCP Status

ПОЛЕ	ОПИСАНИЕ
Relay Status	В данном разделе отображаются настройки, относящиеся к режиму ретрансляции DHCP коммутатором.
Relay Mode	В этом поле отображается одно из следующих состояний: <ul style="list-style-type: none"> • None – если коммутатор не настроен в качестве агента ретрансляции DHCP. • Global – если коммутатор настроен только как агент ретрансляции DHCP. • VLAN, за которым следуют идентификаторы VLAN ID – если он настроен в качестве агента ретрансляции для конкретных VLAN.

28.3 Ретрансляция DHCP

Если клиенты DHCP и сервер DHCP находятся в различных широковещательных доменах, на коммутаторе необходимо настроить ретрансляцию DHCP. При первоначальном выделении IP-адреса коммутатор помогает передавать информацию о сети (такую как IP-адрес и маску подсети) от клиента DHCP к серверу DHCP. После получения клиентом DHCP IP-адреса и его подключения к сети обновление информации между клиентом DHCP и сервером DHCP производится без участия коммутатора.

Данный коммутатор можно настроить в качестве глобального агента ретрансляции DHCP. В этом случае коммутатор будет передавать все запросы DHCP от всех доменов на один и тот же сервер DHCP. Кроме того, на коммутаторе можно настроить ретрансляцию информации DHCP в зависимости от сети VLAN, к которой относится клиент.

28.3.1 Информация агента ретрансляции DHCP

Данный коммутатор позволяет добавлять информацию об источнике клиентского DHCP-запроса, который ретранслируется им на сервер DHCP, посредством добавления **информации агента ретрансляции**. Это помогает аутентифицировать источник запроса. После этого сервер DHCP может выделить IP-адрес с использованием этой информации. Дополнительную информацию можно найти в RFC 3046.

Функция **информации агента ретрансляции DHCP** добавляет поле информации агента к полю **Option 82**. Поле **Option 82** располагается в заголовке клиентских DHCP-запросов, ретранслируемых коммутатором на сервер DHCP.

Информация агента ретрансляции может включать в себя **имя системы**, если выбрать для коммутатора данный режим. Имя системы **System Name** можно изменить на экране **Basic Settings > General Setup**.

Информация агента ретрансляции DHCP, передаваемая коммутатором на сервер DHCP, описана ниже:

Таблица 90 Информация агента ретрансляции

ПОЛЕ	ОПИСАНИЕ
Slot ID	(1 байт) Данное значение всегда равно 0 для автономных коммутаторов.
Port ID	(1 байт) Номер порта, к которому подключен клиент DHCP.
VLAN ID	(2 байта) Идентификатор VLAN, к которой принадлежит порт.
Information	(до 64 байт) Опциональное поле только для чтения, которое устанавливается в соответствии с именем системы, настроенным на экране Basic Settings > General Setup .

28.3.2 Настройка глобальной ретрансляции DHCP

Настройка глобальной ретрансляции DHCP осуществляется на экране **DHCP Relay**. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application > DHCP** и нажмите на ссылке **Global**.

Рисунок 130 Экран IP Application > DHCP > Global

Поля экрана описаны в следующей таблице.

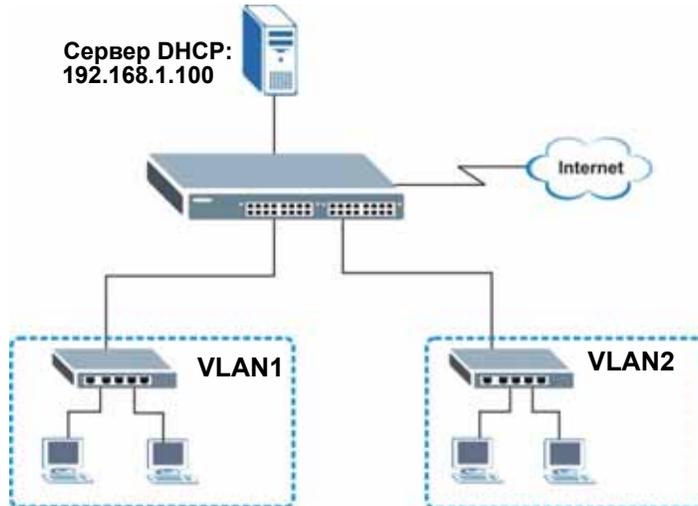
Таблица 91 Экран IP Application > DHCP > Global

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить ретрансляцию DHCP.
Remote DHCP Server 1 .. 3	Введите IP-адрес сервера DHCP в виде десятичных чисел, разделенных точками.
Relay Agent Information	Установите переключатель Option 82 , чтобы коммутатор добавлял информацию (номер слота, номер порта и идентификатор VLAN ID) к клиентским запросам DHCP, ретранслируемым им на сервер DHCP.
Information	В этом доступном только для чтения поля отображается имя системы, настроенное на экране General Setup . Установите данный переключатель, чтобы коммутатор добавлял имя системы к клиентским DHCP-запросам, ретранслируемым на сервер DHCP.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

28.3.3 Пример настройки глобальной ретрансляции DHCP

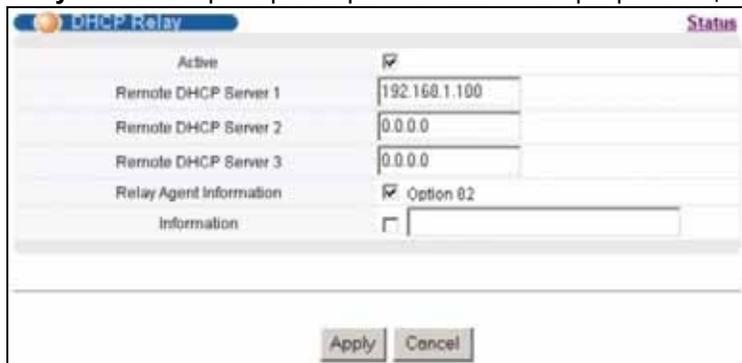
На приведенном ниже рисунке показан пример сети, в которой коммутатор используется для ретрансляции запросов DHCP в доменах **VLAN1** и **VLAN2**. В сети имеется только один сервер DHCP, который обслуживает клиентов DHCP в обоих доменах.

Рисунок 131 Пример сети с глобальной ретрансляцией DHCP



На экране **DHCP Relay** выполняются следующие настройки. Необходимо обязательно установить переключатель **Option 82**, чтобы коммутатор отправлял на сервер DHCP дополнительную информацию (в частности, идентификатор VLAN ID) вместе с запросами DHCP. В этом случае сервер DHCP сможет назначать нужные IP-адреса в зависимости от идентификатора VLAN ID.

Рисунок 132 Пример настройки глобальной ретрансляции DHCP



28.4 Настройка DHCP для конкретных VLAN

На данном экране можно настроить параметры DHCP для конкретных виртуальных локальных сетей VLAN, к которым относятся клиенты DHCP. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application > DHCP** и нажмите на ссылке **VLAN** на появившемся экране **DHCP Status**.



Для каждой сети VLAN, для которой требуется ввести настройки DHCP на коммутаторе, необходимо настроить собственный IP-адрес управления. О том, как это сделать, можно узнать в [разд. 7.6 на стр. 85](#).

Рисунок 133 Экран IP Application > DHCP > VLAN

Поля экрана описаны в следующей таблице.

Таблица 92 Экран IP Application > DHCP > VLAN

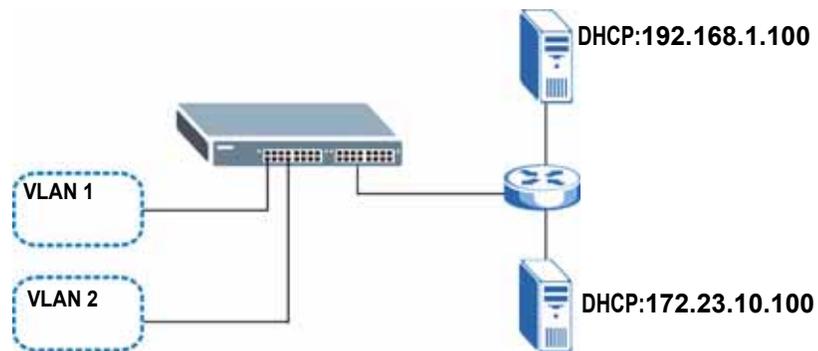
ПОЛЕ	ОПИСАНИЕ
VID	Введите идентификатор VLAN, к которой относятся данные настройки DHCP.
Remote DHCP Server 1 .. 3	Введите IP-адрес сервера DHCP в виде десятичных чисел, разделенных точками.
Relay Agent Information	Установите переключатель Option 82 , чтобы коммутатор добавлял информацию (номер слота, номер порта и идентификатор VLAN ID) к клиентским запросам DHCP, ретранслируемым им на сервер DHCP.
Information	В этом доступном только для чтения поля отображается имя системы, настроенное на экране General Setup . Установите данный переключатель, чтобы коммутатор добавлял имя системы к клиентским DHCP-запросам, ретранслируемым на сервер DHCP.
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clear	Нажмите на данную кнопку, чтобы очистить перечисленные выше поля.
VID	В данном поле отображается идентификатор VLAN, к которой относятся настройки DHCP.
Type	В данном поле отображается Relay в качестве режима DHCP.

Таблица 92 Экран IP Application > DHCP > VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
DHCP Status	При настройке в качестве агента ретрансляции DHCP в данном поле отображается IP-адрес первого удаленного сервера DHCP.
Delete	Выберите записи настройки, которые необходимо удалить, и нажмите на кнопку Delete для удаления.
Cancel	Нажмите Cancel , чтобы снять выделение с переключателей Delete .

28.4.1 Пример: Ретрансляция DHCP для двух VLAN

В следующем примере показана сеть группы зданий с двумя виртуальными локальными сетями VLAN (VID 1 и 2). Для обслуживания каждой из сетей VLAN установлено два сервера DHCP. В системе настроена ретрансляция запросов DHCP из комнат общежития (VLAN 1) на сервер DHCP с IP-адресом 192.168.1.100. Запросы из академических зданий (VLAN 2) направляются на другой сервер DHCP с IP-адресом 172.23.10.100.

Рисунок 134 Ретрансляция DHCP для двух VLAN

Для показанного примера настройки на экране **VLAN Setting** должны быть следующими.

Рисунок 135 Пример настройки ретрансляции DHCP для двух VLAN

The screenshot shows the 'VLAN Setting' configuration interface. The 'VID' field is set to 2. The 'Remote DHCP Server 1' field is set to 172.23.10.100, 'Remote DHCP Server 2' is 0.0.0.0, and 'Remote DHCP Server 3' is 0.0.0.0. The 'Relay Agent Information' section has 'Option 82' checked. Below the configuration fields are 'Add', 'Cancel', and 'Clear' buttons. At the bottom, there is a table with the following data:

VID	Type	DHCP Status	Delete
1	Relay	192.168.1.100	<input type="checkbox"/>

Below the table are 'Delete' and 'Cancel' buttons.

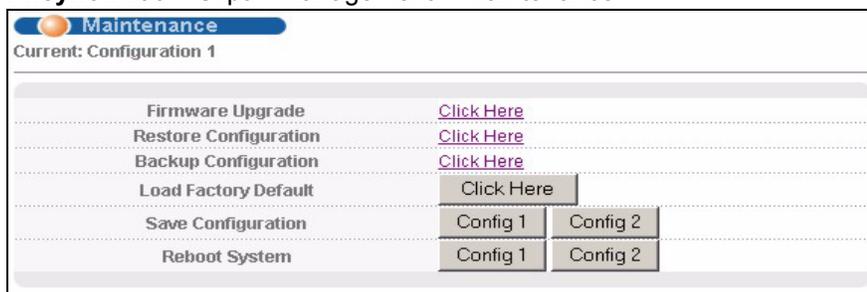
Обслуживание

В данной главе описаны настройки на экранах обслуживания, позволяющих работать с файлами встроенного программного обеспечения и конфигурации.

29.1 Экран обслуживания

На этом экране осуществляется управление встроенным программным обеспечением и файлами конфигурации. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > Maintenance**.

Рисунок 136 Экран Management > Maintenance



Поля экрана описаны в следующей таблице.

Таблица 93 Экран Management > Maintenance

ПОЛЕ	ОПИСАНИЕ
Current	В этом поле отображается, какая конфигурация используется коммутатором в данный момент (Configuration 1 или Configuration 2).
Firmware Upgrade	Нажмите Click Here для перехода к экрану обновления встроенного аппаратного обеспечения Firmware Upgrade .
Restore Configuration	Нажмите Click Here для перехода к экрану восстановления конфигурации Restore Configuration .
Backup Configuration	Нажмите Click Here для перехода к экрану резервного копирования конфигурации Backup Configuration .
Load Factory Default	Нажмите Click Here для сброса конфигурации к заводским настройкам по умолчанию.

Таблица 93 Экран Management > Maintenance (продолжение)

ПОЛЕ	ОПИСАНИЕ
Save Configuration	Нажмите Config 1 для сохранения текущей конфигурации в качестве Configuration 1 коммутатора. Нажмите Config 2 для сохранения текущей конфигурации в качестве Configuration 2 коммутатора.
Reboot System	Нажмите Config 1 для перезагрузки системы с использованием на коммутаторе конфигурации Configuration 1 . Нажмите Config 2 для перезагрузки системы с использованием на коммутаторе конфигурации Configuration 2 . Примечание: Не забывайте нажимать на кнопку Save на экранах настройки при изменении текущей конфигурации коммутатора.

29.2 Загрузка заводских настроек по умолчанию

Чтобы вернуться на коммутаторе к заводским настройкам по умолчанию, выполните следующее.

- 1 Чтобы сбросить всю введенную информацию о настройках коммутатора и вернуться к заводским настройкам по умолчанию, нажмите кнопку **Click Here** рядом с надписью **Load Factory Defaults** на экране **Maintenance**.
- 2 Чтобы вернуть все настройки коммутатора к заводским настройкам по умолчанию, нажмите **OK**

Рисунок 137 Загрузка заводских настроек: запуск

- 3 Изменения вступают в силу после нажатия на кнопку **Save** в Web-конфигураторе. Для повторного входа в Web-конфигуратор коммутатора, возможно, придется изменить IP-адрес компьютера, чтобы он находился в той же подсети, что и IP-адрес коммутатора по умолчанию (192.168.1.1).

29.3 Сохранение конфигурации

Нажмите **Config 1** для сохранения текущей конфигурации в качестве **Configuration 1** коммутатора.

Нажмите **Config 2** для сохранения текущей конфигурации в качестве **Configuration 2** коммутатора.

Кроме того, для сохранения изменений в текущей конфигурации можно воспользоваться кнопкой **Save** в правом верхнем углу на любом экране.



Нажатие на кнопки **Apply** и **Add NE** сохраняет изменения в постоянной памяти. Все несохраненные изменения будут утеряны после перезагрузки коммутатора.

29.4 Перезагрузка системы

Опция **Reboot System** позволяет перезагрузить коммутатор, не отключая питание физически. Кроме того, при перезагрузке можно выбрать конфигурацию один (**Config 1**) или конфигурацию два (**Config 2**). Чтобы перезагрузить коммутатор, выполните следующее.

- 1 Чтобы перезагрузить коммутатор с использованием первой конфигурации, нажмите на кнопку **Config 1** в поле **Reboot System** экрана **Maintenance**. Появится следующий экран.

Рисунок 138 Перезагрузка системы: подтверждение



- 2 Нажмите **OK** еще раз и дождитесь, пока коммутатор перезагрузится. Этот процесс занимает до двух минут. Он не влияет на настройки коммутатора.

Чтобы перезагрузить коммутатор с использованием второй конфигурации, нажмите **Config 2** и выполните действия 1 и 2.

29.5 Обновление встроенного программного обеспечения

Прежде чем приступить к загрузке встроенного программного обеспечения в устройство, убедитесь, что на компьютер загружено (и распаковано) встроенное программное обеспечение нужной модели и версии.



Убедитесь, что загружаемое встроенное программное обеспечение подходит для соответствующей модели, так как программное обеспечение для другой модели может повредить устройство.

Находясь на экране **Maintenance**, выберите **Firmware Upgrade**, чтобы открыть показанный ниже экран.

Рисунок 139 Экран Management > Maintenance > Firmware Upgrade

Введите путь и имя файла встроенного программного обеспечения, который необходимо загрузить в коммутатор, в текстовом поле **File Path**, или нажмите **Browse**, чтобы найти его вручную. Установите переключатель **Rebooting**, если необходимо перезагрузить коммутатор и применить новое встроенное программное обеспечение немедленно. (Обновления встроенного программного обеспечения применяются только после перезагрузки). Нажмите **Upgrade**, чтобы загрузить новое встроенное программное обеспечение.

После завершения процесса загрузки встроенного программного обеспечения откройте экран **System Info**, чтобы проверить текущий номер версии встроенного программного обеспечения.

29.6 Восстановление файла конфигурации

Экран **Restore Configuration** позволяет восстановить ранее сохраненные настройки с компьютера на коммутатор.

Рисунок 140 Экран Management > Maintenance > Restore Configuration

Введите имя и путь к файлу конфигурации, который необходимо восстановить, в текстовое поле **File Path**, или нажмите **Browse**, чтобы найти его вручную. После ввода пути к файлу нажмите **Restore**. Файл конфигурации в коммутаторе имеет имя «config», поэтому файл резервной копии конфигурации при восстановлении будет автоматически переименован.

29.7 Резервное копирование файла конфигурации

Функция резервного копирования конфигурации коммутатора позволяет создавать различные «снимки» конфигурации устройства, которые потом можно загрузить.

Резервное копирование конфигурации коммутатора на компьютер осуществляется с использованием экрана **Backup Configuration**.

Рисунок 141 Экран Management > Maintenance > Backup Configuration



Чтобы создать резервную копию текущей конфигурации коммутатора на компьютере, выполните на данном экране следующее.

- 1 Нажмите **Backup**.
- 2 Нажмите **Save**, чтобы открыть экран **Save As**.
- 3 Выберите расположение файла на компьютере в ниспадающем списке **Save in** и введите имя-описание для него в поле списка **File name**. Нажмите **Save**, чтобы сохранить конфигурацию на компьютере.

29.8 Командная строка FTP

В данном разделе описаны некоторые примеры загрузки или выгрузки с коммутатора файлов с помощью команд FTP. Прежде всего необходимо уяснить соглашения об именовании файлов.

29.8.1 Соглашения об именовании файлов

Файл конфигурации (также называемый файлом ROM) содержит заводские настройки по умолчанию для таких экранов, как коммутатор setup, IP Setup и т.д. После внесения изменений в настройки коммутатора их можно сохранить на компьютере под любым выбранным именем.

Операционная система ZyNOS (ZyXEL Network Operating System, часто называется «gas» -файлом) – это встроенное системное программное обеспечение, она имеет расширение файла «bin».

Таблица 94 Соглашения об именовании файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл конфигурации	config		Файл настроек коммутатора. При загрузке файла config данный файл конфигурации заменяется, в том числе заменяются настройки коммутатора, системная информация (в том числе пароль по умолчанию), журналы ошибок и отслеживания.
Встроенное программное обеспечение	gas	*.bin	Общее имя для встроенного программного обеспечения ZyNOS на коммутаторе.

29.8.1.1 Примеры команд FTP

```
ftp> put firmware.bin ras
```

Пример FTP-сессии, в которой происходит передача файла «firmware.bin» с компьютера на коммутатор.

```
ftp> get config config.cfg
```

Пример FTP-сессии, в которой происходит сохранение текущего файла конфигурации в файл с именем «config.cfg» на компьютере.

Если используемый (Т)FTP-клиент не позволяет указывать имя конечного файла, отличное от исходного, файлы придется переименовать, так как коммутатор распознает только имена «config» и «ras». Обязательно сохраните неизменные копии обоих файлов для дальнейшего использования.



Убедитесь, что загружаемое встроенное программное обеспечение подходит для соответствующей модели, так как программное обеспечение для другой модели может повредить устройство.

29.8.2 Работа с командной строкой FTP

- 1 Запустите на компьютере FTP-клиент.
- 2 Введите команду `open`, потом пробел и IP-адрес коммутатора.
- 3 Нажмите [ENTER], получив запрос имени пользователя.
- 4 После получения приглашения введите пароль (по умолчанию «1234»).
- 5 Введите `bin`, чтобы установить двоичный режим передачи.
- 6 Для загрузки файлов с компьютера на коммутатор используйте команду `put`, например: команда `put firmware.bin ras` переносит файл встроенного программного обеспечения с компьютера (`firmware.bin`) в коммутатор и переименовывает его в «`ras`». Точно так же команда `put config.cfg config` переносит файл конфигурации с компьютера (`config.cfg`) в коммутатор и переименовывает его в «`config`». С помощью команды `get config config.cfg` можно перенести файл конфигурации с коммутатора на компьютер и переименовать его в «`config.cfg`». Дополнительную информацию о соглашениях в отношении именования файлов можно найти в [табл. 94 на стр. 265](#).
- 7 Чтобы покинуть строку ftp-команд, введите `quit`.

29.8.3 FTP-клиенты с графическим пользовательским интерфейсом

Описания некоторых команд, которые встречаются в FTP-клиентах с графическим пользовательским интерфейсом, можно найти в следующей таблице.

Таблица 95 Общие команды для FTP-клиентов с графическим пользовательским интерфейсом

КОМАНДА	ОПИСАНИЕ
Host Address (Адрес хоста)	Введите адрес хост-сервера.
Login Type (Тип входа в систему)	Анонимный (Anonymous). Для тех случаев, когда идентификатор пользователя и пароль вводятся на сервере автоматически для анонимного доступа. Анонимные подключения работают только в том случае, если Интернет-провайдер или администратор службы включил эту опцию. Normal (Обычный). Для подключения к серверу требуются уникальные имя пользователя и пароль.
Transfer Type (Тип передачи)	Файлы передаются либо в формате ASCII (простой текстовый формат), либо в двоичном формате. Файлы настроек и встроенного программного обеспечения должны передаваться в двоичном формате.
Initial Remote Directory (Начальный удаленный каталог)	Укажите удаленный каталог по умолчанию (путь).
Initial Local Directory (Начальный локальный каталог)	Укажите локальный каталог по умолчанию (путь).

29.8.4 Ограничения FTP

Протокол FTP не будет работать, если:

- Служба FTP отключена на экране **Service Access Control**.
- IP-адрес (IP-адреса), введенные на экране **Remote Management**, не соответствуют IP-адресу клиента. Если адрес не совпадает, коммутатор немедленно разрывает FTP-сессию.

Контроль доступа

В данной главе описан контроль доступа к коммутатору.

30.1 Обзор контроля доступа

Для доступа с консольного порта или через FTP допускается по одной сессии, для доступа через Telnet и SSH допускается в общей сложности четыре сессии, для управления через Web поддерживается до пяти сессий (с пятью различными именами пользователей и паролями), количество сеансов контроля доступа через SNMP не ограничено.

Таблица 96 Обзор контроля доступа

Консольный порт	SSH	Telnet	FTP	Web	SNMP
Одна сессия	В общей сложности до четырех сессий		Одна сессия	До пяти учетных записей	Без ограничений

Сессии контроля доступа с консольного порта и через Telnet не могут быть осуществлены одновременно, если функция доступа нескольким пользователям (multi-login) отключена. Дополнительную информацию о запрещении доступа нескольким пользователям можно найти в Справочном руководстве по интерфейсу командной строки.

30.2 Главный экран контроля доступа

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > Access Control**.

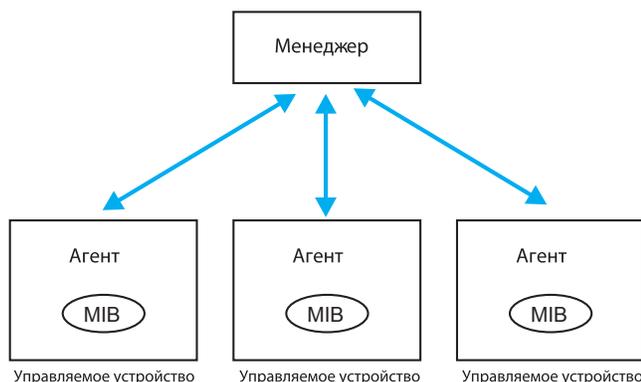
Рисунок 142 Экран Management > Access Control



30.3 Знакомство с протоколом SNMP

Простой протокол сетевого управления (SNMP) – это протокол прикладного уровня, который используется для управления и мониторинга устройств на основе TCP/IP. Протокол SNMP используется для обмена управляющей информацией между системой сетевого управления (NMS) и сетевым элементом (NE). Станция управления может управлять и осуществлять мониторинг коммутатора по сети с помощью протокола SNMP версии 1 (SNMPv1), SNMP версии 2с или SNMP версии 3. Пример управления с помощью протокола SNMP показан на следующем рисунке. Протокол SNMP будет работать только в том случае, если настроен протокол TCP/IP.

Рисунок 143 Модель управления по протоколу SNMP



Сеть под управлением протокола SNMP состоит из двух основных компонентов: агентов и менеджера.

Агент – это программный модуль управления, находящийся на управляемом коммутаторе (коммутатор). Агент переводит локальную информацию управления от управляемого коммутатора в форму, совместимую с протоколом SNMP. Менеджер – это консоль, посредством которой администраторы сети осуществляют функции сетевого управления. На ней запускаются приложения, осуществляющие контроль и мониторинг управляемых устройств.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют, какую информацию о коммутаторе необходимо получить. Примерами таких переменных являются количество полученных пакетов, состояние порта и т.д. База управляющей информации (MIB) представляет собой совокупность управляемых объектов. Протокол SNMP позволяет менеджеру и агентам общаться между собой для получения доступа к этим объектам.

Сам по себе SNMP – это простой протокол типа «запрос/ответ» на основе модели «менеджер/агент». Менеджер отправляет запрос, а агент отвечает на него посредством следующих операций протокола:

Таблица 97 Команды протокола SNMP

КОМАНДА	ОПИСАНИЕ
Get	Позволяет менеджеру получать объектные переменные от агента.
GetNext	Позволяет менеджеру получить следующую объектную переменную из таблицы или списка, хранящегося у агента. В протоколе SNMPv1, когда менеджер хочет получить от агента все элементы таблицы, он инициирует операцию Get и сразу за ней серию операций GetNext.

Таблица 97 Команды протокола SNMP

КОМАНДА	ОПИСАНИЕ
Set	Позволяет менеджеру устанавливать значения объектных переменных, хранящихся у агента.
Trap	Используется агентом для оповещения менеджера о каких-либо событиях.

30.3.1 SNMP v3 и безопасность

В SNMP v3 улучшены средства безопасности для управления через SNMP. Перед началом сессий управления от менеджеров SNMP может быть затребована аутентификация на агентах.

Дополнительно безопасность может быть повышена с использованием шифрования сообщений SNMP, отправляемых менеджерами. Шифрование защищает содержимое сообщения SNMP. В случае шифрования сообщений SNMP они могут быть прочитаны только целевыми получателями.

30.3.2 Поддерживаемые базы MIB

Базы управляющей информации позволяют администраторам собирать статистику и осуществлять мониторинг за состоянием и производительностью.

Данный коммутатор поддерживает следующие базы управляющей информации:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIB
- RFC 1643 Ethernet MIB
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c или более поздней версии, совместимый со стандартом RFC 2011 SNMPv2 MIB для IP, RFC 2012 SNMPv2 MIB для TCP, RFC 2013 SNMPv2 MIB для UDP

30.3.3 Команды Trap протокола SNMP

Данный коммутатор отправляет SNMP-менеджеру «ловушку» (команду Trap), когда происходит какое-нибудь событие. Команды Trap протокола SNMP для различных категорий описаны в следующих таблицах.

Идентификаторы объектов OID (Object ID), начинающиеся с «1.3.6.1.4.1.890.1.5», определены в частных MIB. Все прочие OID определены в стандартных MIB. Подробную информацию об идентификаторах объектов MIB OID, поддерживаемых коммутатором, можно найти в главе «Контроль доступа» Руководства пользователя.

В частных MIB идентификаторы OID для каждой модели начинаются со значений, приведенных в табл. 98 на стр. 272.

Таблица 98 Идентификаторы объектов по моделям

МОДЕЛЬ	ИДЕНТИФИКАТОР ОБЪЕКТА (НАЧАЛО)
ES-3124	1.3.6.1.4.1.890.1.5.8.12
ES-3124PWR	1.3.6.1.4.1.890.1.5.8.14
ES-3124-4F	1.3.6.1.4.1.890.1.5.8.26
ES-3124F	1.3.6.1.4.1.890.1.5.8.31

Таблица 99 Системные команды Trap протокола SNMP (System)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	Эта команда Trap отправляется при включении коммутатора.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	Эта команда Trap отправляется при перезагрузке коммутатора.
fanspeed	FanSpeedEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при понижении или повышении скорости вентилятора так, что она выходит из нормального рабочего диапазона.
	FanSpeedEventClear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trap отправляется при возвращении скорости вентилятора в нормальный рабочий диапазон.
temperature	TemperatureEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при понижении или повышении температуры так, что она выходит из нормального рабочего диапазона.
	TemperatureEventClear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trap отправляется при возвращении температуры в нормальный рабочий диапазон.

Таблица 99 Системные команды Trap протокола SNMP (System) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
voltage	VoltageEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при понижении или повышении напряжения так, что оно выходит из нормального рабочего диапазона.
	VoltageEventClear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trap отправляется при возвращении напряжения в нормальный рабочий диапазон.
reset	UncontrolledResetEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при автоматическом сбросе коммутатора.
	ControlledResetEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при сбросе коммутатора администратором через интерфейс управления.
	RebootEvent	1.3.6.1.4.1.890.1.5.0.1	Эта команда Trap отправляется при перезагрузке коммутатора администратором через интерфейс управления.
timesync	RTCNotUpdatedEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при неполучении коммутатором времени и даты от сервера времени.
	RTCNotUpdatedEventClear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trap отправляется при получении коммутатором времени и даты от сервера времени.

Таблица 99 Системные команды Trap протокола SNMP (System) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
intrusionlock	IntrusionLockEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при блокировке порта для защиты от вторжения.
loopguard	LoopguardEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trap отправляется при блокировке порта функцией защиты от образования петель.

Таблица 100 Интерфейсные команды Trap протокола SNMP (Interface)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	Эта команда Trap отправляется при установлении Ethernet-соединения.
	LinkDownEventClear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trap отправляется при установлении Ethernet-соединения.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	Эта команда Trap отправляется при разрыве Ethernet-соединения.
	LinkDownEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при разрыве Ethernet-соединения.

Таблица 100 Интерфейсные команды Trar протокола SNMP (Interface) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
autonegotiation	AutonegotiationFailedEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trar отправляется в случае, когда интерфейсу Ethernet не удается автоматически согласовать параметры соединения с другим интерфейсом Ethernet.
	AutonegotiationFailedEventClear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trar отправляется в случае, когда интерфейсу Ethernet удается автоматически согласовать параметры соединения с другим интерфейсом Ethernet.

Таблица 101 Команды Trar протокола SNMP для аутентификации, авторизации и учета (AAA)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Эта команда Trar отправляется при невозможности аутентификации из-за неправильного имени пользователя и/или пароля.
	AuthenticationFailureEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trar отправляется при невозможности аутентификации из-за неправильного имени пользователя и/или пароля.
	RADIUSNotReachableEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trar отправляется при отсутствии ответа от сервера RADIUS.
	RADIUSNotReachableEventClear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trar отправляется при недоступности сервера RADIUS.

Таблица 101 Команды Trar протокола SNMP для аутентификации, авторизации и учета (AAA)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
accounting	RADIUSNotReachableEvent On	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trar отправляется при отсутствии ответа от сервера учета RADIUS.
	RADIUSNotReachableEvent Clear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trar отправляется при недоступности сервера учета RADIUS.

Таблица 102 Команды Trar протокола SNMP для IP

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	Эта команда Trar отправляется при неудаче выполнения одиночной команды ping.
	pingTestFailed	1.3.6.1.2.1.80.0.2	Эта команда Trar отправляется при неудаче выполнения теста соединения (включающего в себя несколько команд ping).
	pingTestCompleted	1.3.6.1.2.1.80.0.3	Эта команда Trar отправляется при завершении одиночной команды ping.
traceroute	traceRoutePathChange	1.3.6.1.2.1.81.0.1	Эта команда Trar отправляется при изменении пути к пункту назначения.
	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	Эта команда Trar отправляется при неудаче выполнения теста traceroute.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	Эта команда Trar отправляется при завершении теста traceroute.

Таблица 103 Команды Trar протокола SNMP для коммутатора (Switch)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	Эта команда Trar отправляется при изменении корневого коммутатора STP.
	MRSTPNewRoot	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.36.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.36.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.36.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.36.2.1	Эта команда Trar отправляется при изменении корневого коммутатора MRSTP.
	MSTPNewRoot	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.107.70.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.107.70.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.107.70.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.107.70.1	Эта команда Trar отправляется при изменении корневого коммутатора MSTP.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	Эта команда Trar отправляется при изменении топологии STP.
	MRSTPTopologyChange	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.36.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.36.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.36.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.36.2.2	Эта команда Trar отправляется при изменении топологии MRSTP.
	MSTPTopologyChange	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.107.70.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.107.70.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.107.70.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.107.70.2	Эта команда Trar отправляется при изменении топологии MSTP.

Таблица 103 Команды Trap протокола SNMP для коммутатора (Switch) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
mactable	MacTableFullEventOn	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.1 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.1 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.1 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.1	Эта команда Trap отправляется при использовании более 99% таблицы MAC-адресов.
	MacTableFullEventClear	ES-3124: 1.3.6.1.4.1.890.1.5.8.12.27.2.2 ES-3124 PWR: 1.3.6.1.4.1.890.1.5.8.14.27.2.2 ES-3124-4F: 1.3.6.1.4.1.890.1.5.8.26.32.2.2 ES-3124F: 1.3.6.1.4.1.890.1.5.8.31.32.2.2	Эта команда Trap отправляется при использовании менее 95% таблицы MAC-адресов.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	Эта команда Trap отправляется при выходе переменной за пределы верхнего порогового значения RMON.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	Эта команда Trap отправляется при выходе переменной за пределы нижнего порогового значения RMON.

30.3.4 Настройка SNMP

Доступ к экрану **SNMP** осуществляется с экрана **Access Control**. Чтобы вернуться к экрану **Access Control**, выберите пункт **Access Control**.

Рисунок 144 Экран Management > Access Control > SNMP

The screenshot shows the SNMP configuration page with the following sections:

- General Setting:**
 - Version: v2c (dropdown)
 - Get Community: public (text input)
 - Set Community: public (text input)
 - Trap Community: public (text input)
- Trap Destination:**

Version	IP	Port	Username
v2c	0.0.0.0	162	
- User Information:**

Index	Username	Security Level	Authentication	Privacy
1	admin	noauth	MD5	DES

Buttons: Apply, Cancel

Поля экрана описаны в следующей таблице.

Таблица 104 Экран Management > Access Control > SNMP

ПОЛЕ	ОПИСАНИЕ
General Setting	В данном разделе определяются версия SNMP и параметр community (пароль).
Version	Выберите версию SNMP для коммутатора. Версия SNMP, установленная на коммутаторе, должна совпадать с версией на менеджере SNMP. Выберите вариант SNMP версии 2с (v2c), SNMP версии 3 (v3) или оба этих варианта (v3v2c). Примечание: SNMP версии 2с обратно совместим с SNMP версии 1.
Get Community	Введите значение Get Community – это пароль для входящих запросов Get и GetNext от станции управления. Строка Get Community используется менеджерами SNMP только при выборе SNMP версии 2с и ниже.
Set Community	Введите значение Set Community – это пароль для входящих запросов Set от станции управления. Строка Set Community используется менеджерами SNMP только при выборе SNMP версии 2с и ниже.
Trap Community	Введите значение Trap Community – это пароль, отправляемый SNMP-менеджеру с каждой командой Trap. Строка Trap Community используется менеджерами SNMP только при выборе SNMP версии 2с и ниже.
Trap Destination	В данном разделе настраивается, куда должны отправляться команда Trap SNMP коммутатором.
Version	Укажите версию SNMP для отправки сообщений Trap.

Таблица 104 Экран Management > Access Control > SNMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP	Введите IP-адреса менеджеров (до 4-х), которым будут отправляться команды Trap.
Port	Введите номер порта, который прослушивается менеджером в ожидании сообщений Trap SNMP.
Username	Введите имя пользователя, отправляемое на менеджер SNMP в случае команды Trap через SNMP v3. Примечание: Данное имя пользователя должно соответствовать существующей учетной записи на коммутаторе (настраивается на экране Management > Access Control > Logins).
User Information	В данном разделе настраиваются пользователи для аутентификации на менеджерах при использовании SNMP v3. Примечание: Для создания учетных записей на менеджере SNMP v3 используйте имена пользователей и пароли, введенные в данном разделе.
Index	Порядковый номер (только для чтения) учетной записи на коммутаторе.
Username	В этом поле отображается имя пользователя для учетной записи на коммутаторе.
Security Level	Выберите, необходимо ли использовать аутентификацию и/или шифрование в сеансах SNMP с данным пользователем. Варианты: <ul style="list-style-type: none"> • noauth – имя пользователя используется в качестве пароля при отправке на менеджер SNMP. Это эквивалентно параметрам Get, Set и Trap Community в SNMP v2c. Наименее защищенный режим. • auth – для сообщений SNMP, отправляемых данным пользователем, используется механизм аутентификации. • priv – для сообщений SNMP, отправляемых данным пользователем, используются механизмы аутентификации и шифрования. Самый защищенный режим. Примечание: На менеджере SNMP должен быть настроен аналогичный или более высокий уровень безопасности, чем на коммутаторе.
Authentication	Выберите алгоритм аутентификации. При аутентификации данных SNMP применяются алгоритмы хэширования MD5 (Message Digest 5) и SHA (Secure Hash Algorithm). Аутентификация SHA считается более стойкой по сравнению с MD5, но более медленной.
Privacy	Укажите алгоритм шифрования для обмена данными SNMP с этим пользователем. Можно выбрать один из следующих вариантов: <ul style="list-style-type: none"> • DES – стандарт Data Encryption Standard представляет собой широко распространенный (однако не очень стойкий) алгоритм шифрования данных. В этом алгоритме к каждому 64-битному блоку данных применяется 56-битный ключ. • AES – стандарт Advanced Encryption Standard представляет собой еще один метод шифрования с закрытым ключом. В AES к каждому 128-битному блоку данных применяется 128-битный ключ.

Таблица 104 Экран Management > Access Control > SNMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

30.3.5 Настройка группы «ловушек» SNMP

Чтобы отобразить показанный ниже экран, нажмите на экране **SNMP** на ссылку **Trap Group**. На экране **Trap Group** можно выбрать типы «ловушек» SNMP, которые должны отправляться на каждый из менеджеров SNMP.

Рисунок 145 Экран Management > Access Control > SNMP > Trap Group

Type	Options
System <input type="checkbox"/> *	<input type="checkbox"/> coldstart <input type="checkbox"/> warmstart <input checked="" type="checkbox"/> fanspeed
	<input type="checkbox"/> temperature <input type="checkbox"/> voltage <input checked="" type="checkbox"/> reset
	<input type="checkbox"/> timesync <input type="checkbox"/> intrusionlock <input type="checkbox"/> loopguard
Interface <input type="checkbox"/> *	<input type="checkbox"/> linkup <input type="checkbox"/> linkdown <input type="checkbox"/> autonegotiation
AAA <input type="checkbox"/> *	<input type="checkbox"/> authentication <input type="checkbox"/> accounting
IP <input type="checkbox"/> *	<input type="checkbox"/> ping <input type="checkbox"/> traceroute
Switch <input type="checkbox"/> *	<input type="checkbox"/> stp <input type="checkbox"/> mactable <input type="checkbox"/> rmon

Поля экрана описаны в следующей таблице.

Таблица 105 Экран Management > Access Control > SNMP > Trap Group

ПОЛЕ	ОПИСАНИЕ
Trap Destination IP	Выберите один из настроенных IP-адресов назначения для передачи команд Trap. Они представляют собой IP-адреса менеджеров SNMP. IP-адреса назначения должны быть предварительно настроены на экране SNMP Setting . Далее на этом экране настраиваются команды Trap, направляемые коммутатором на данный менеджер SNMP.
Type	Выберите категории сообщений Trap SNMP, которые будут отправляться коммутатором на данный менеджер SNMP.
Options	Выберите отдельные команды Trap SNMP, которые будут направляться коммутатором на станцию SNMP. Описания отдельных команд Trap приводятся в разд. 30.3.3 на стр. 271 . Подробную информацию об идентификаторах объектов MIB OID, поддерживаемых коммутатором, можно найти в главе «Контроль доступа» Руководства пользователя. Команды Trap группируются по категориям. При выборе категории автоматически выбираются все команды Trap, относящиеся к данной категории. При снятии выделения с переключателей отдельных команд Trap эти команды не будут отправляться коммутатором на станцию SNMP. Если снять выделение с переключателя категории, автоматически снимается выделение со всех переключателей отдельных команд, относящихся к данной категории (коммутатор отправляет команды Trap лишь для выбранных категорий).

Таблица 105 Экран Management > Access Control > SNMP > Trap Group (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

30.3.6 Настройка учетных записей пользователей

Доступ к коммутатору через Web-конфигуратор одновременно могут получить до пяти пользователей (один администратор и четыре обычных пользователя).

- Администратор – это пользователь, который может как просматривать, так и вносить изменения в настройки коммутатора. Имя пользователя для администратора не может быть изменено – это всегда **admin**. Пароль по умолчанию – **1234**.



Настоятельно рекомендуется изменить пароль администратора по умолчанию (**1234**).

- Обычный пользователь (не администратор, с именем, отличным от **admin**) может только просматривать, но не изменять настройки коммутатора.

Чтобы открыть приведенный ниже экран, нажмите **Management > Access Control > Logins**.

Рисунок 146 Экран Management > Access Control > Logins

Logins [Access Control](#)

Administrator

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Edit Logins

Login	User Name	Password	Retype to confirm
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

Поля экрана описаны в следующей таблице.

Таблица 106 Экран Management > Access Control > Logins

ПОЛЕ	ОПИСАНИЕ
Administrator	Учетная запись администратора по умолчанию, с именем пользователя «admin». Имя пользователя администратора по умолчанию изменить нельзя. Только администратор имеет права чтения/записи.
Old Password	Введите существующий системный пароль (пароль по умолчанию при поставке – 1234).
New Password	Введите новый системный пароль.
Retype to confirm	Введите новый системный пароль еще раз для подтверждения.
Edit Logins	Имеется возможность настроить до четырех пользовательских записей с паролями. У этих пользователей будут права только на чтение. Более высокие привилегии могут назначаться пользователям через интерфейс командной строки. Дополнительную информацию о назначении уровней привилегий можно найти в Справочном руководстве по интерфейсу командной строки.
User Name	Введите имя пользователя (до 32 символов ASCII).
Password	Введите новый системный пароль.
Retype to confirm	Введите новый системный пароль еще раз для подтверждения.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

30.4 Обзор протокола SSH

В отличие от протоколов Telnet или FTP, которые передают данные в обычном текстовом формате, протокол SSH (Secure Shell) является защищенным протоколом, который совмещает возможности аутентификации и шифрования для обеспечения безопасной передачи данных между двумя хостами с использованием небезопасной сети.

Рисунок 147 Пример связи по протоколу SSH



30.5 Как работает протокол SSH

Процесс установки защищенного соединения между двумя удаленными хостами описан в следующей таблице.

Рисунок 148 Как работает протокол SSH

**1 Идентификация хоста**

SSH-клиент отправляет запрос на соединение SSH-серверу. Сервер идентифицирует себя с помощью ключа хоста. Клиент шифрует случайно сгенерированный ключ сессии с помощью ключа хоста и ключа сервера, затем отправляет результат обратно на сервер.

Клиент автоматически сохраняет все новые открытые ключи сервера. При последующих подключениях открытый ключ сервера сверяется с сохраненной версией на клиентском компьютере.

2 Метод шифрования

После проверки идентификационной информации клиент и сервер должны согласовать используемый метод шифрования.

3 Аутентификация и передача данных

После проверки идентификационных данных и активации шифрования образуется защищенный туннель между клиентом и сервером. Для подключения к серверу клиент отправляет ему аутентификационную информацию (имя пользователя и пароль).

30.6 Реализация протокола SSH на коммутаторе

Данный коммутатор поддерживает протокол SSH версии 2 с использованием аутентификации по методу RSA и трех методов шифрования (DES, 3DES и Blowfish). Для удаленного управления и передачи файлов на коммутаторе реализован SSH-сервер (порт 22). Одновременно допускается только одно SSH-соединение.

30.6.1 Требования к использованию протокола SSH

Для подключения к коммутатору по протоколу SSH необходимо установить программу-клиент SSH на клиентском компьютере (с установленной операционной системой Windows или Linux).

30.7 Знакомство с протоколом HTTPS

Протокол HTTPS (протокол передачи гипертекста через протокол защищенных сокетов, или HTTP через SSL) – это Web-протокол, обеспечивающий шифрование и дешифрование Web-страниц. Протокол защищенных сокетов Secure Socket Layer (SSL) представляет собой протокол уровня приложений, реализующий безопасную передачу данных посредством обеспечения конфиденциальности (посторонние не смогут прочесть передаваемые данные), аутентификации (одна сторона может идентифицировать другую) и целостности данных (изменение данных будет заметно).

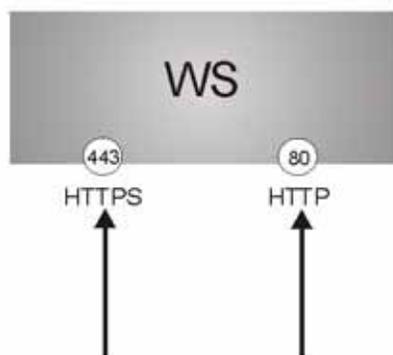
Этот протокол работает на основе сертификатов, открытых и секретных ключей.

Протокол HTTPS на коммутаторе используется для получения защищенного доступа к коммутатору через Web-конфигуратор. Протокол SSL предусматривает, что SSL-сервер (коммутатор) должен всегда предоставлять свою аутентификационную информацию SSL-клиенту (компьютеру, который запрашивает HTTPS-соединение с коммутатором), тогда как SSL-клиент должен проходить аутентификацию только по требованию SSL-сервера. Аутентификация клиентских сертификатов необязательна, и если она выбрана, то SSL-клиент должен отправить коммутатору сертификат. За сертификатом для браузера следует обращаться к поставщику сертификатов, являющемуся доверенным поставщиком сертификатов для коммутатора.

См. следующий рисунок.

- 1 Запросы на HTTPS-соединение от Web-браузера с поддержкой SSL поступают (по умолчанию) на порт 443 Web-сервера (WS) коммутатора.
- 2 Запросы на HTTP-соединение от Web-браузера поступают (по умолчанию) на порт 80 Web-сервера (WS) коммутатора.

Рисунок 149 Реализация протокола HTTPS





При отключении **HTTP** на экране **Service Access Control** коммутатор блокирует все попытки соединения по HTTP.

30.8 Пример подключения по протоколу HTTPS

Если порт HTTPS по умолчанию для коммутатора не менялся, введите в адресной строке браузера «https://IP-адрес коммутатора», где «IP-адрес коммутатора» – это IP-адрес или доменное имя коммутатора, к которому необходимо получить доступ.

30.8.1 Предупреждения от Internet Explorer

При попытке получить доступ к коммутатору через HTTPS-сервер появится диалоговое окно Windows с вопросом, доверяете ли вы сертификату сервера. Нажмите кнопку **View Certificate**, чтобы проверить, принадлежит ли сертификат коммутатору.

В Internet Explorer появляется следующее сообщение **Security Alert**. Нажмите **Yes**, чтобы проследовать на экран ввода имени пользователя и пароля Web-конфигуратора; Если нажать **No**, то доступ к Web-конфигуратору будет заблокирован.

Рисунок 150 Диалоговое окно Security Alert (Internet Explorer)



30.8.2 Предупреждения от Netscape Navigator

При попытке получить доступ к коммутатору через HTTPS-сервер появится сообщение **Website Certified by an Unknown Authority** с вопросом, доверяете ли вы сертификату сервера. Чтобы проверить, действительно ли сертификат принадлежит коммутатору, нажмите кнопку **Examine Certificate**.

В случае выбора варианта **Accept this certificate temporarily for this session** нажмите **OK**, чтобы продолжить работу в Netscape.

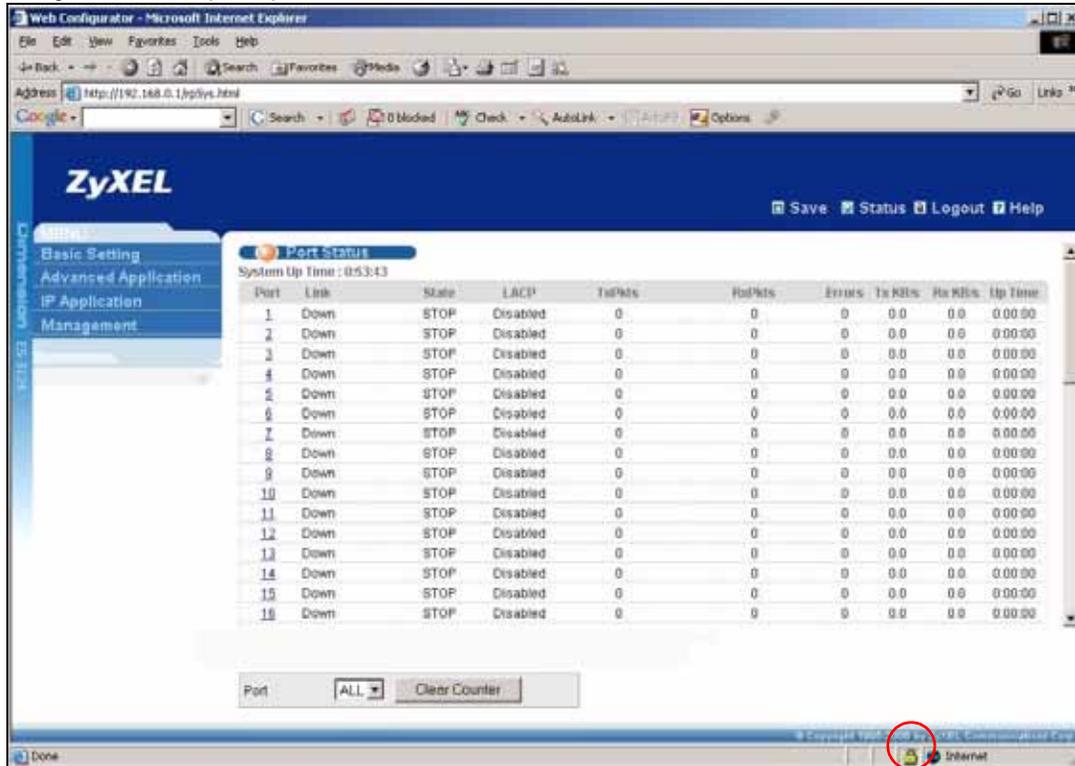
Чтобы импортировать сертификат коммутатора в SSL-клиент для постоянной работы, выберите **Accept this certificate permanently**.

Рисунок 151 Сертификат безопасности 1 (Netscape)**Рисунок 152** Сертификат безопасности 2 (Netscape)

30.8.3 Основной экран

После того, как был принят сертификат и введены имя пользователя и пароль, появится основной экран коммутатора. В нижней части экрана браузера появится значок замка, что свидетельствует об установлении защищенного соединения.

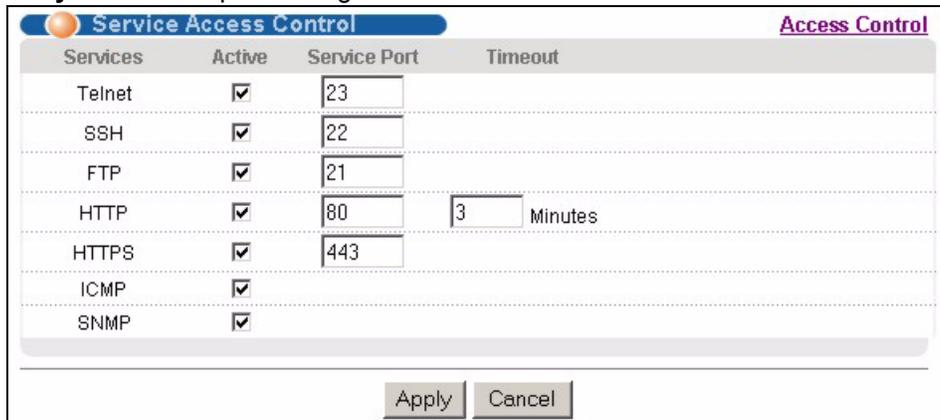
Рисунок 153 Пример: значок замка для защищенного соединения



30.9 Контроль доступа к портам служб

Контроль доступа к службам позволяет определить, каким службам разрешен доступ к коммутатору. Также имеется возможность изменить номер порта службы по умолчанию и настроить «доверенные компьютеры» для каждой службы на экране **Remote Management** (будет рассмотрен ниже). Для возврата к основному экрану **Access Control** нажмите **Access Control**.

Рисунок 154 Экран Management > Access Control > Service Access Control



Поля экрана описаны в следующей таблице.

Таблица 107 Экран Management > Access Control > Service Access Control

ПОЛЕ	ОПИСАНИЕ
Services	В этом столбце перечислены службы, с помощью которых можно получить доступ к коммутатору.
Active	Установите этот переключатель, чтобы разрешить соответствующей службе получать доступ к коммутатору.
Service Port	Номер порта службы по умолчанию для Telnet, SSH, FTP, HTTP или HTTPS; можно изменить посредством ввода нового номера порта в поле Server Port . В случае изменения номера порта по умолчанию не забудьте сообщить новый номер пользователям, которым может понадобиться эта служба.
Timeout	Укажите время простоя сессии управления (через Web-конфигуратор), по истечении которого сессия будет прекращена по тайм-ауту. После тайм-аута необходимо будет заново ввести имя пользователя и пароль. Слишком большое значение Timeout создает угрозу безопасности.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

30.10 Удаленное управление

Находясь на экране **Access Control**, перейдите на экран **Remote Management**, показанный ниже.

Имеется возможность определить группу из одного или нескольких «доверенных компьютеров», с которых администратор может использовать службы управления коммутатором. Для возврата к экрану **Access Control** нажмите **Access Control**.

Рисунок 155 Экран Management > Access Control > Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>						
2	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						

Apply Cancel

Поля экрана описаны в следующей таблице.

Таблица 108 Экран Management > Access Control > Remote Management

ПОЛЕ	ОПИСАНИЕ
Entry	Порядковый номер клиентского набора. Клиентский набор – это группа из одного или нескольких компьютеров, с которых администратор может использовать службы управления коммутатором.
Active	Установите этот переключатель, чтобы активировать данный клиентский набор. Снимите выделение с переключателя, если необходимо временно отключить набор, не удаляя его.
Start Address End Address	Введите диапазон IP-адресов доверенных компьютеров, с которых можно управлять коммутатором. Данный коммутатор проверяет соответствие IP-адреса компьютера, запрашивающего службу или протокол, введенному здесь диапазону. Если адрес не совпадает, коммутатор немедленно разрывает сессию.
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Выберите службы, которые могут быть использованы для управления коммутатором с указанных доверенных компьютеров.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

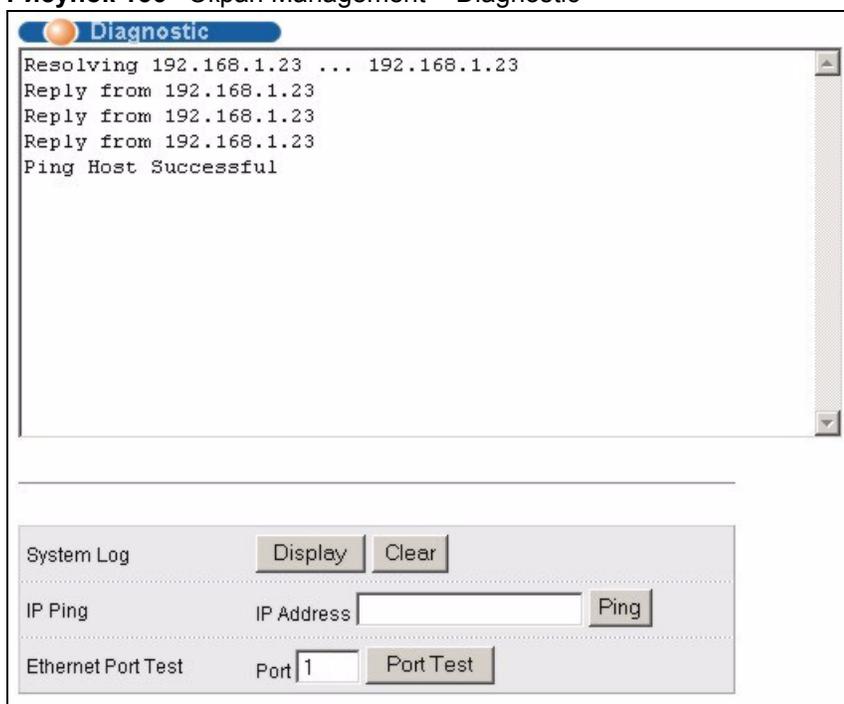
Диагностика

В данной главе описан экран диагностики **Diagnostic**.

31.1 Экран Diagnostic

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > Diagnostic**. На этом экране можно проверять системные журналы, пинговать IP-адреса и тестировать порты.

Рисунок 156 Экран Management > Diagnostic



Поля экрана описаны в следующей таблице.

Таблица 109 Экран Management > Diagnostic

ПОЛЕ	ОПИСАНИЕ
System Log	Нажмите Display , чтобы отобразить журнал событий в многострочном текстовом окне. Нажмите Clear , чтобы очистить текстовое окно и сбросить запись системного журнала.
IP Ping	Введите IP-адрес устройства, которое необходимо пропинговать для проверки соединения. Нажмите Ping , чтобы коммутатор пропинговал IP-адрес (введенный в поле слева).
Ethernet Port Test	Введите номер порта и нажмите Port Test для выполнения теста внутренней обратной петли.

Системный журнал Syslog

В данной главе описаны экраны системного журнала Syslog.

32.1 Обзор Syslog

С помощью протокола syslog устройства могут пересылать по IP-сети извещения о событиях серверам syslog, собирающим информацию о событиях. Устройства с поддержкой syslog позволяют генерировать сообщения syslog и отправлять их на сервер syslog.

Протокол Syslog определен в стандарте RFC 3164. RFC определяет формат пакета, содержание и относящуюся к системному журналу информацию в сообщениях syslog. Каждое сообщение syslog содержит определение категории (facility) и уровня серьезности (level). Категория syslog идентифицирует файл на сервере syslog. Более подробную информацию можно найти в документации на сервер syslog. Уровни серьезности протокола syslog описаны в следующей таблице.

Таблица 110 Уровни серьезности Syslog

КОД	УРОВЕНЬ СЕРЬЕЗНОСТИ
0	Авария: система неработоспособна.
1	Тревога: требуются немедленные действия.
2	Критическое состояние: система находится в критическом состоянии.
3	Ошибка: обнаружена ошибка в системе.
4	Предупреждение: системой сгенерировано предупреждение.
5	Уведомление: нормальное, но важное состояние в системе.
6	Информация: информационное сообщение в журнале syslog.
7	Отладка: сообщение предназначено для отладки.

32.2 Настройка Syslog

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > Syslog**. Функция syslog позволяет передавать записи системных журналов на внешний сервер syslog. На этом экране можно настроить параметры ведения системного журнала устройства.

Рисунок 157 Экран Management > Syslog

Logging type	Active	Facility
System	<input checked="" type="checkbox"/>	local use 0
Interface	<input checked="" type="checkbox"/>	local use 0
Switch	<input checked="" type="checkbox"/>	local use 0
AAA	<input checked="" type="checkbox"/>	local use 0
IP	<input checked="" type="checkbox"/>	local use 0

Поля экрана описаны в следующей таблице.

Таблица 111 Экран Management > Syslog

ПОЛЕ	ОПИСАНИЕ
Syslog	Выберите Active , чтобы включить syslog (ведение системного журнала) и настроить параметры syslog.
Logging Type	В данном столбце отображаются имена категорий журналов, которые могут генерироваться устройством.
Active	Установите данный переключатель, чтобы активировать на устройстве генерирование журнала соответствующей категории.
Facility	В этом поле можно выбрать категорию журнала, чтобы записывать журналы в различные файлы на сервере syslog. Более подробную информацию можно найти в документации на сервер syslog.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

32.3 Настройка сервера Syslog

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > Syslog > Syslog Server Setup**. На открывшемся экране можно настроить список внешних серверов syslog.

Рисунок 158 Экран Management > Syslog > Server Setup

Поля экрана описаны в следующей таблице.

Таблица 112 Экран Management > Syslog > Server Setup

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на устройстве отправку журналов на сервер syslog. Снимите выделение с переключателя, если необходимо внести запись о сервере syslog, но не отправлять на него журналы с устройства (запись можно изменить позднее).
Server Address	Введите IP-адрес сервера syslog.
Log Level	Выберите уровень серьезности для сообщений, которые будут отправляться устройством на данный сервер syslog. Меньшие номера соответствуют более важным сообщениям системного журнала.
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clear	Нажмите Clear , чтобы вернуться к заводским настройкам.
Index	Порядковый номер записи сервера syslog. Нажатие на данный номер позволяет внести изменения в запись.
Active	В данном поле отображается Yes , если устройство отправляет журналы на сервер syslog. Значение No означает, что журналы на сервер syslog устройством не отправляются.
IP Address	В этом поле отображается IP-адрес сервера syslog.
Log Level	В этом поле отображается уровень серьезности для сообщений, которые отправляются устройством на данный сервер syslog.
Delete	Для удаления записи установите переключатель в столбце Delete этой записи и нажмите на Delete .
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Управление кластерами

В данной главе описано управление кластерами.

33.1 Обзор управления кластерами

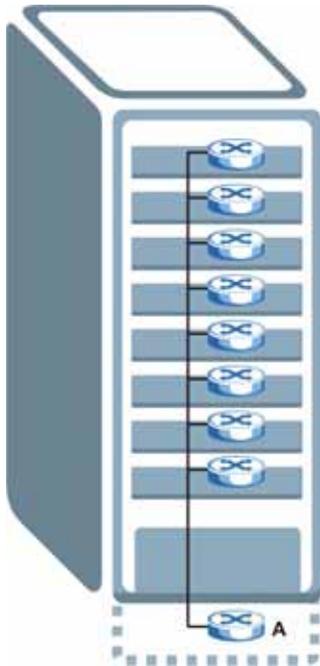
Управление кластерами позволяет управлять несколькими коммутаторами через один коммутатор, называемый менеджером кластера. Чтобы коммутаторы могли взаимодействовать друг с другом, они должны быть подключены напрямую и принадлежать к одной группе VLAN.

Таблица 113 Спецификации управления кластерами ZyXEL

Максимальное количество членов кластера	24
Модели членов кластера	Должны быть совместимы с реализацией управления кластерами ZyXEL.
Менеджер кластера	Это коммутатор, с помощью которого осуществляется управление другими коммутаторами.
Члены кластера	Коммутаторы, управление которыми осуществляется через коммутатор-менеджер кластера.

В данном примере коммутатор А, стоящий в подвале, является менеджером кластера, а остальные коммутаторы на верхних этажах здания – членами кластера.

Рисунок 159 Пример реализации кластера



33.2 Состояние управления кластером

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > Cluster Management**.



У кластера может быть только один менеджер.

Рисунок 160 Экран Management > Cluster Management

Clustering Management Status		Configuration		
Status	Manager			
Manager	00:13:49:00:00:02			
The Number Of Member = 1				
Index	MacAddr	Name	Model	Status
1	00:a0:c5:01:23:46		GS-2024	Online

Поля экрана описаны в следующей таблице.

Таблица 114 Экран Management > Cluster Management

ПОЛЕ	ОПИСАНИЕ
Status	В этом поле отражается роль данного коммутатора внутри кластера. Manager – менеджер Member – член (отображается, если доступ на этот экран осуществляется непосредственно через члена кластера, а не его менеджера) None – коммутатор не является ни менеджером, ни членом кластера
Manager	В этом поле отображается аппаратный MAC-адрес коммутатора-менеджера кластера.
The Number of Member	В этом поле отображается количество коммутаторов в данном кластере. В следующих полях описаны коммутаторы-члены кластера.
Index	Коммутаторами-членами кластера можно управлять через коммутатор-менеджер. Каждый номер в столбце Index – это гиперссылка на Web-конфигуратор коммутатора-члена кластера (см. рис. 161 на стр. 299).
MacAddr	В этом поле отображается аппаратный MAC-адрес коммутатора-члена кластера.
Name	Системное имя (System Name) члена кластера.
Model	В этом поле отображается название модели.
Status	В этом поле отображается одно из следующих состояний: Online (член кластера доступен) Error (ошибка; например, пароль доступа к коммутатору-члену кластера изменился или коммутатор стал менеджером и покинул список членов, и т.д). Offline (коммутатор отключен – состояние Offline возникает примерно через полторы минуты после того, как канал между членом кластера и менеджером разрывается)

33.2.1 Управление коммутаторами-членами кластера

Откройте экран **Clustering Management Status** на коммутаторе-менеджере кластера, затем нажмите на гиперссылку **Index** в списке членов, чтобы открыть домашнюю страницу Web-конфигуратора этого члена кластера. Домашняя страница Web-конфигуратора члена кластера отличается от домашней страницы коммутатора, доступ к которому осуществляется напрямую.

Рисунок 161 Управление кластером: экран Web-конфигуратора члена кластера



33.2.1.1 Загрузка встроенного программного обеспечения на коммутатор-член кластера

Загрузить встроенное программное обеспечение на коммутатор-член кластера через менеджер кластера можно посредством FTP, как показано на следующем примере.

Рисунок 162 Пример: загрузка встроенного программного обеспечения на коммутатор-член кластера

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 коммутатор FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner   group       3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner   group       393216 Jul 01 12:00 config
--w--w--w-   1 owner   group         0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner   group         0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 3701t0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

Некоторые параметры FTP описаны в следующей таблице.

Таблица 115 Пример загрузки встроенного программного обеспечения на член кластера посредством FTP

ПАРАМЕТР FTP	ОПИСАНИЕ
User	Введите «admin».
Password	Пароль Web-конфигуратора по умолчанию – «1234».
ls	Введите эту команду, чтобы вывести на экран имена файлов встроенного программного обеспечения и конфигурации коммутатора-члена кластера.
3601t0.bin	Имя файла встроенного программного обеспечения, который загружается на коммутатор-член кластера.
fw-00-a0-c5-01-23-46	Имя файла встроенного программного обеспечения члена кластера в том виде, в котором его воспринимает менеджер кластера.
config-00-a0-c5-01-23-46	Имя файла конфигурации члена кластера в том виде, в котором его воспринимает менеджер кластера.

33.3 Настройка управления кластерами

Данный экран используется для настройки управления кластерами. Чтобы отобразить показанный ниже экран, выберите **Configuration** на экране **Cluster Management**.

Рисунок 163 Экран Management > Clustering Management > Configuration

Поля экрана описаны в следующей таблице.

Таблица 116 Экран Management > Clustering Management > Configuration

ПОЛЕ	ОПИСАНИЕ
Clustering Manager	
Active	Установите переключатель Active , чтобы этот коммутатор стал менеджером кластера. У кластера может быть только один менеджер. Остальные (подключенные напрямую) коммутаторы, назначенные менеджерами кластера, не будут отображаться в списке Clustering Candidates . Если коммутатор ранее был членом кластера, а затем был назначен менеджером кластера, то его состояние Status на экране Cluster Management Status может отображаться как Error («Ошибка»), а в соответствующей строке в итоговом списке членов кластера появится значок предупреждения ().
Name	Введите имя для идентификации менеджера кластера (Clustering Manager) – до 32 отображаемых символов (пробелы допускаются).

Таблица 116 Экран Management > Clustering Management > Configuration

ПОЛЕ	ОПИСАНИЕ
VID	Идентификатор VLAN, и он доступен только в том случае, если коммутатором используются виртуальные локальные сети типа 802.1Q . Коммутаторы, принадлежащие к одному кластеру, должны быть подключены напрямую и принадлежать к одной группе VLAN. Коммутаторы, которые не принадлежат к одной группе VLAN, не будут отображаться в списке Clustering Candidates . Если на коммутаторе-менеджере кластера (Clustering Manager) используются виртуальные локальные сети на основе портов (Port-based), поле будет не активно.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Clustering Candidate	Следующие поля относятся к коммутаторам, являющимся потенциальными членами кластера.
List	Здесь отображается список подходящих кандидатов в члены кластера, обнаруженных автоматически. Коммутаторы должны быть соединены напрямую. Напрямую подключенные коммутаторы, назначенные менеджерами кластера, в списке Clustering Candidate отображаться не будут. Коммутаторы, которые не принадлежат к одной группе управления VLAN, в списке Clustering Candidates также отображаться не будут.
Password	Пароль каждого члена кластера – это пароль его Web-конфигуратора. Выберите член кластера в списке Clustering Candidate и введите пароль его Web-конфигуратора. Если после этого администратор того коммутатора изменит пароль Web-конфигуратора, то управлять коммутатором с менеджера кластера станет невозможно. В этом случае его состояние Status на экране Cluster Management Status будет отображаться как Error («Ошибка»), а в соответствующей строке в итоговом списке членов кластера появится значок предупреждения (⚠). Если у нескольких устройств одинаковый пароль, то их можно выбрать, удерживая нажатой клавишу [SHIFT]. Затем введите их общий пароль Web-конфигуратора.
Add	Нажмите Add , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.
Refresh	Нажмите кнопку Refresh , чтобы провести поиск потенциальных кандидатов в члены кластера еще раз.
В следующей итоговой таблице отображается информация о настроенных членах кластера.	
Index	Порядковый номер коммутатора-члена кластера.
MacAddr	В этом поле отображается MAC-адрес коммутатора-члена кластера.
Name	Системное имя (System Name) члена кластера.
Model	Название модели коммутатора-члена кластера.
Remove	Установите этот переключатель и нажмите кнопку Remove , чтобы удалить коммутатор-член из кластера.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

Таблица MAC-адресов

В данной главе описан экран настройки таблицы MAC-адресов **MAC Table**.

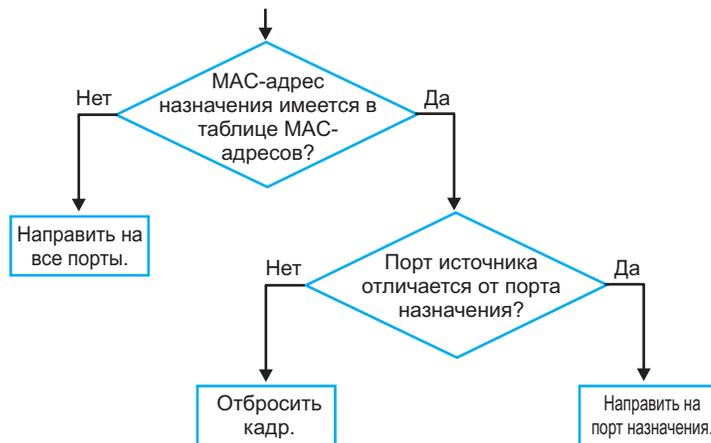
34.1 Обзор таблицы MAC-адресов

На экране настройки таблицы MAC-адресов **MAC Table** (которую еще называют базой данных фильтрации) можно увидеть, каким образом кадры пересылаются или фильтруются на портах коммутатора. На этом экране отображается, на какой порт (порты) передается MAC-адрес какого устройства, принадлежащего к какой из групп VLAN (если они определены), и является ли MAC-адрес динамическим (полученным коммутатором) или статическим (введенным вручную на экране настроек **Static MAC Forwarding**).

Чтобы определить, куда направлять кадры, коммутатор пользуется таблицей MAC-адресов. См. следующий рисунок.

- 1 Данный коммутатор изучает полученный кадр и запоминает порт, на который пришел этот MAC-адрес источника.
 - 2 Затем коммутатор проверяет, соответствует ли MAC-адрес назначения этого кадра MAC-адресу источника, уже имеющемуся в таблице MAC-адресов.
- Если коммутатору уже известен порт для этого MAC-адреса, то он направляет кадр на этот порт.
 - Если коммутатору еще не известен порт для этого MAC-адреса, то кадр направляется на все порты сразу. Если таким образом направляется слишком много кадров, то происходит перегрузка сети.
 - Если коммутатору уже известен порт для MAC-адреса, и порт назначения совпадает с портом источника, то этот кадр отбрасывается.

Рисунок 164 Схема работы таблицы MAC-адресов



34.2 Просмотр таблицы MAC-адресов

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > MAC Table**.

Рисунок 165 Экран Management > MAC Table

Index	MAC Address	VID	Port	Type
1	00:85:a0:01:01:00	1	8	dynamic
2	00:85:a0:01:01:04	1	8	dynamic
3	00:a0:c5:00:00:01	1	2	dynamic
4	00:a0:c5:fe:ea:71	1	CPU	static
5	00:a0:c5:fe:ea:71	2	CPU	static

Поля экрана описаны в следующей таблице.

Таблица 117 Экран Management > MAC Table

ПОЛЕ	ОПИСАНИЕ
Sort by	Нажмите на одну из кнопок, чтобы отобразить и отсортировать данные по одному из параметров. После этого информация отображается в итоговой таблице ниже.
MAC	Нажмите эту кнопку, чтобы отсортировать данные по MAC-адресу.
VID	Нажмите эту кнопку, чтобы отсортировать данные по группе VLAN.
Port	Нажмите эту кнопку, чтобы отсортировать данные по номеру порта.
Index	Порядковый номер входящего кадра.
MAC Address	MAC-адрес устройства, с которого прибыл входящий кадр.
VID	Группа VLAN, к которой принадлежит данный кадр.
Port	Номер порта, с которого был получен указанный выше MAC-адрес.
Type	В этом поле отображается тип MAC-адреса – dynamic (динамический, то есть полученный коммутатором) или static (статический, то есть внесенный вручную на экране Static MAC Forwarding).

Таблица ARP

В данной главе описана таблица протокола разрешения адресов (ARP).

35.1 Обзор таблицы ARP

Протокол разрешения адресов (ARP) – это протокол, предназначенный для определения соответствия между IP-адресом и физическим адресом машины, также известным как адрес управления доступом к среде, или MAC-адрес, в локальной сети.

Длина IP-адреса (версии 4) составляет 32 бита. В локальной сети Ethernet длина MAC-адреса составляет 48 бит. Таблица протокола ARP определяет соответствие между каждым MAC-адресом и соответствующим ему IP-адресом.

35.1.1 Как работает протокол ARP

Когда входящий пакет, предназначенный для хост-устройства в локальной сети, прибывает на коммутатор, программа протокола ARP на коммутаторе ищет его в таблице ARP и, если адрес обнаружен, отправляет пакет на устройство.

Если для IP-адреса не найдено записи, протокол ARP направляет широковещательный запрос всем устройствам в локальной сети. Данный коммутатор заполняет поля его собственных MAC-адреса и IP-адреса в адресе отправителя, а затем вносит известный IP-адрес получателя в соответствующем поле. Кроме того, коммутатор заполняет единицами поле MAC-адреса пункта назначения (FF.FF.FF.FF.FF.FF – адрес для широковещательных сообщений в сети Ethernet). Отвечающее устройство (устройство с искомым IP-адресом или маршрутизатор, которому известен путь к нему) заменяет широковещательный адрес на свой MAC-адрес, меняет местами пары отправитель-получатель и отправляет одноадресный ответ непосредственно машине, приславшей запрос. Протокол ARP обновляет таблицу ARP для дальнейших обращений и затем отправляет пакет на ответивший MAC-адрес.

35.2 Просмотр таблицы ARP

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > ARP Table**. Таблица ARP используется для просмотра соответствия между IP-адресами и MAC-адресами.

Рисунок 166 Экран Management > ARP Table

Index	IP Address	MAC Address	Type
1	172.21.0.2	00:05:5d:04:30:f1	dynamic
2	172.21.3.16	00:05:1c:15:08:71	dynamic
3	172.21.3.19	00:0b:cd:8c:6d:ed	dynamic
4	172.21.3.40	00:0c:76:07:41:0d	dynamic
5	172.21.3.66	00:50:8d:47:73:4f	dynamic
6	172.21.3.90	00:05:5d:f4:49:20	dynamic
7	172.21.3.91	00:50:ba:ad:56:7c	dynamic
8	172.21.3.95	00:10:b5:ae:56:97	dynamic
9	172.21.3.120	00:10:b5:ae:62:32	dynamic
10	172.21.3.138	00:a0:c5:b2:62:26	dynamic
11	172.21.4.99	00:0c:76:09:cf:88	dynamic
12	172.21.10.11	08:00:20:ad:f6:88	dynamic
13	172.21.100.153	00:90:27:be:a2:8c	dynamic
14	172.21.207.247	00:0c:76:09:17:1a	dynamic
15	192.168.1.1	00:a0:c5:3f:91:56	dynamic
16	192.168.1.5	00:85:a0:01:01:04	dynamic
17	192.168.1.10	00:a0:c5:5e:df:f9	static
18	192.168.1.100	00:85:a0:01:01:00	dynamic

Поля экрана описаны в следующей таблице.

Таблица 118 Экран Management > ARP Table

ПОЛЕ	ОПИСАНИЕ
Index	Порядковый номер записи в таблице ARP.
IP Address	IP-адрес, полученный от устройства, подключенного к порту коммутатора, с соответствующим ему MAC-адресом.
MAC Address	MAC-адрес устройства с соответствующим ему IP-адресом.
Type	В этом поле отображается тип MAC-адреса – dynamic (динамический, то есть полученный коммутатором) или static (статический, то есть внесенный вручную на экране Static MAC Forwarding).

Настройка клонирования

В данной главе описывается возможность копирования настроек одного порта на другие порты.

36.1 Настройка клонирования

С помощью клонирования можно скопировать основные и расширенные настройки порта-источника на один или несколько портов назначения. Чтобы отобразить показанный ниже экран, нажмите **Management > Configure Clone**.

Рисунок 167 Экран Management > Configure Clone

The screenshot shows the 'Configure Clone' configuration page. At the top, there are two input fields labeled 'Source Port' and 'Destination Port'. Below these is a section titled 'Port Features' which is divided into two sub-sections: 'Basic Setting' and 'Advanced Application'. Each sub-section contains a list of features with checkboxes. The 'Basic Setting' section includes: Active, Name, Speed / Duplex, BPDU Control, Flow Control, and Intrusion Lock. The 'Advanced Application' section includes: VLAN1q, VLAN1q Member, Bandwidth Control, VLAN Stacking, Port Security, Broadcast Storm Control, Mirroring, Port Authentication, Queuing Method, IGMP Filtering, Spanning Tree Protocol, Multiple Rapid Spanning Tree Protocol, Protocol-based VLAN, Port-based VLAN, MAC Authentication, Two-rate three color marker, Ethernet OAM, Loop Guard, ARP Inspection, and DHCP Snooping. At the bottom of the page, there are two buttons: 'Apply' and 'Cancel'.

Поля экрана описаны в следующей таблице.

Таблица 119 Экран Management > Configure Clone

ПОЛЕ	ОПИСАНИЕ
Source/ Destination Port	<p>Введите номер порта-источника в поле Source. Параметры этого порта будут копироваться.</p> <p>Введите порты или порты назначения в поле Destination. На эти порты будут скопированы параметры порта-источника. Можно ввести несколько номеров портов через запятую, либо диапазон портов через дефис.</p> <p>Пример:</p> <ul style="list-style-type: none"> • 2, 4, 6 – в качестве портов назначения используются порты 2, 4 и 6. • 2-6 – в качестве портов назначения используются порты со 2 по 6.
Basic Setting	Выберите настройки порта (установленные на экранах основных настроек Basic Setting), которые должны быть скопированы на порты назначения.
Advanced Application	Выберите настройки порта (установленные на экранах расширенных приложений Advanced Application), которые должны быть скопированы на порты назначения.
Apply	Нажмите Apply , чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке Save в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите Cancel , чтобы начать настройку на этом экране заново.

ЧАСТЬ IV

Устранение неполадок и характеристики

Устранение неполадок (313)

Характеристики продукта (317)

Устранение неполадок

В данной главе описаны некоторые способы разрешения проблем, с которыми можно столкнуться при эксплуатации устройства. Возможные проблемы разделены по следующим категориям:

- Проблемы с питанием, аппаратные подключения и индикаторы
- Проблемы с доступом и входом на коммутатор

37.1 Проблемы с питанием, аппаратные подключения и индикаторы



Не включается коммутатор. Ни один из индикаторов не горит.

- 1 Убедитесь, что коммутатор включен (модели с питанием от постоянного тока).
- 2 Убедитесь, что с коммутатором используются адаптер питания или шнур питания из комплекта поставки.
- 3 Убедитесь, что адаптер питания или шнур подключены к коммутатору и к соответствующему источнику питания. Убедитесь, что источник питания включен и работает.
- 4 Выключите и снова включите коммутатор (модели с питанием от постоянного тока).
- 5 Отсоедините и вновь присоедините адаптер питания или шнур к коммутатору (модели с питанием от переменного тока).
- 6 Если проблема сохраняется, обратитесь к поставщику.



Горит индикатор **ALARM/ALM**.

- 1 Выключите и вновь включите коммутатор. (модели с питанием от постоянного тока)
- 2 Отсоедините и вновь подсоедините адаптер питания к коммутатору. (модели с питанием от переменного тока)
- 3 Если проблема сохраняется, обратитесь к поставщику.



Показания одного из индикаторов отличаются от обычного.

- 1 Проверьте, какими именно должны быть показания индикатора в нормальном режиме. См. [разд. 3.3 на стр. 51](#).
- 2 Проверьте аппаратные подключения. См. [гл. 2 на стр. 41](#).
- 3 Осмотрите кабели на предмет повреждений. Обратитесь к поставщику для замены всех поврежденных кабелей.
- 4 Выключите и снова включите коммутатор (модели с питанием от постоянного тока).
- 5 Отсоедините и вновь присоедините адаптер питания к коммутатору (модели с питанием от переменного тока).
- 6 Если проблема сохраняется, обратитесь к поставщику.

37.2 Проблемы с доступом и входом на коммутатор



Забыт IP-адрес коммутатора.

- 1 IP-адрес для внеполосного управления по умолчанию – **192.168.0.1**. IP-адрес для внутрисетевых соединений по умолчанию – **192.168.1.1**.
- 2 Подключитесь к коммутатору через консольный порт.
- 3 Подключитесь к коммутатору через порт управления. Используйте при этом IP-адрес для внеполосного управления.
- 4 Если это не помогает, можно сбросить коммутатор к заводским настройкам по умолчанию. См. [разд. 4.6 на стр. 64](#).



Забыто имя пользователя или пароль.

- 1 Имя пользователя по умолчанию – **admin**, а соответствующий ему пароль по умолчанию – **1234**. Данные значения чувствительны к регистру, поэтому убедитесь, что [Caps Lock] не включен.
- 2 Если это не помогает, можно сбросить коммутатор к заводским настройкам по умолчанию. См. [разд. 4.6 на стр. 64](#).



Невозможно получить доступ к экрану Login Web-конфигуратора.

- 1 Убедитесь, что используется правильный IP-адрес.
 - IP-адрес для внеполосного управления по умолчанию – 192.168.0.1.
 - IP-адрес для внутрисетового управления по умолчанию – 192.168.1.1.
 - Если IP-адрес был изменен (разд. 7.6 на стр. 85), используйте новый IP-адрес.
 - Если IP-адрес был изменен, но невозможно узнать, на какой именно, обратитесь к рекомендациям раздела [Забыв IP-адрес коммутатора](#).
- 2 Проверьте аппаратные подключения и убедитесь, что показания индикаторов соответствуют нормальным. См. [разд. 3.3 на стр. 51](#).
- 3 Убедитесь, что в браузере не включена блокировка всплывающих окон и включены JavaScripts и Java. См. [прил. В на стр. 349](#).
- 4 Убедитесь, что компьютер находится в той же подсети, что и коммутатор. (Если точно известно, что подключение компьютера к коммутатору осуществляется через маршрутизатор, пропустите данный шаг).
- 5 Попробуйте получить доступ к коммутатору с использованием другой службы, например, через Telnet. В случае успешного доступа к коммутатору проверьте настройки удаленного управления и настройки защищенного клиента, чтобы выяснить, почему коммутатор не отвечает на подключения через HTTP.
- 6 Выполните сброс коммутатора к заводским настройкам по умолчанию и попытайтесь получить доступ к коммутатору с использованием IP-адреса по умолчанию. См. [разд. 4.6 на стр. 64](#).
- 7 Если проблема сохраняется, обратитесь к поставщику.



Экран Login появляется, но выполнить вход на коммутатор не удается.

- 1 Убедитесь, что имя пользователя и пароль вводятся правильно. Имя пользователя по умолчанию – **admin**, а соответствующий ему пароль по умолчанию – **1234**. Данные значения чувствительны к регистру, поэтому убедитесь, что [Caps Lock] не включен.
- 2 При наличии подключения к коммутатору через Telnet или консольный порт получить доступ к нему через Web-конфигуратор невозможно. Выполните отключение от коммутатора в другой сессии, или попросите подключившегося выполнить выход из системы.
- 3 Выключите и снова включите коммутатор (модели с питанием от постоянного тока).
- 4 Отсоедините и вновь присоедините адаптер питания или шнур к коммутатору (модели с питанием от переменного тока).
- 5 Если это не помогает, можно сбросить коммутатор к заводским настройкам по умолчанию. См. [разд. 4.6 на стр. 64](#).



Невозможно получить доступ к коммутатору через Telnet.

См. рекомендации по устранению неполадок в разделе [Невозможно получить доступ к экрану Login Web-конфигуратора](#). Не обращайтесь на рекомендации, касающиеся браузера. Кроме того, перед сбросом коммутатора к заводским настройкам по умолчанию обратите внимание на следующие вопросы.

- 1 Возможно, превышено допустимое количество одновременных Telnet-сессий. Завершите остальные Telnet-сессии или попробуйте подключиться еще раз.
- 2 Попробуйте получить доступ к коммутатору с использованием другой службы, например, через HTTP. В случае успешного доступа к коммутатору проверьте настройки удаленного управления и настройки защищенного клиента, чтобы выяснить, почему коммутатор не отвечает на подключения через Telnet.



Невозможно выгрузить / загрузить файл конфигурации через FTP. / Невозможно загрузить новое встроенное программное обеспечение через FTP.

См. рекомендации по устранению неполадок в разделе [Невозможно получить доступ к экрану Login Web-конфигуратора](#). Не обращайтесь на рекомендации, касающиеся браузера. Кроме того, перед сбросом коммутатора к заводским настройкам по умолчанию обратите внимание на следующие вопросы.

- 1 Возможно, превышено допустимое количество одновременных FTP-сессий. Завершите остальные FTP-сессии или попробуйте подключиться еще раз.
- 2 Попробуйте получить доступ к коммутатору с использованием другой службы, например, через HTTP. В случае успешного доступа к коммутатору проверьте настройки удаленного управления и настройки защищенного клиента, чтобы выяснить, почему коммутатор не отвечает на подключения через FTP.

Характеристики продукта

В данной главе подробно описаны характеристики аппаратного обеспечения и встроенного программного обеспечения коммутатора.

38.1 Общие характеристики коммутатора

Характеристики аппаратного обеспечения и встроенного программного обеспечения коммутатора описаны в приведенных ниже таблицах.

Таблица 120 Характеристики оборудования и параметры окружающей среды

СПЕЦИФИКАЦИЯ	ОПИСАНИЕ
Интерфейсы Ethernet	24 интерфейса 10/100 Base-TX Автосогласование Автоматический выбор режима MDI/MDIX Совместимость со стандартом IEEE 802.3/3u Управление потоком методом обратного давления для полудуплексного режима Управление потоком для дуплексного режима согласно IEEE 802.3x Поддержка питания устройств по витой паре согласно стандарту IEEE 802.3af (только в ES-3124PWR) Разъемы для кабелей RJ-45 на портах Ethernet (только в ES-3124, ES-3124-4F и ES-3124PWR)
SFP-интерфейсы Fast Ethernet	24 слота SFP стандарта 100Base (только в ES-3124F) Совместимость со стандартом IEEE 802.3/3u Управление потоком методом обратного давления для полудуплексного режима Управление потоком для дуплексного режима согласно IEEE 802.3x
Интерфейсы Gigabit Ethernet	2 совмещенных интерфейса Gigabit Ethernet / mini-GBIC. 2 порта Gigabit Ethernet (только в ES-3124 и ES-3124PWR) 2 порта mini-GBIC (только в ES-31234-4F и ES-3124F)
Индикаторы	На коммутатор: BPS, PWR, SYS, ALM На порт Ethernet: LNK/ACT, PoE (только в ES-3124PWR) На порт Ethernet: LNK/ACT, FDX (только в ES-3124 и ES-3124-4F) На порт SFP стандарта Fast Ethernet: LNK, ACT (только в ES-3124F) На порт Gigabit Ethernet: LNK/ACT, FDX На слот mini-GBIC: LNK, ACT На порт управления: 10, 100
Габариты	438 мм (Ш) x 270 мм (Г) x 44,5 мм (В) (только ES-3124, ES-3124-4F и ES-3124F) 438 мм (Ш) x 420 мм (Г) x 44,45 мм (В) (только ES-3124PWR) Возможность установки в стандартную 19-дюймовую стойку

Таблица 120 Характеристики оборудования и параметры окружающей среды

СПЕЦИФИКАЦИЯ	ОПИСАНИЕ
Вес устройства	4 кг (ES-3124F) 4,2 кг (ES-3124 и ES-3124-4F) 6,8 кг (ES-3124PWR)
Температура:	Рабочая: 0°С ~ 45°С Хранения: -10°С ~ 70°С
Влажность	10 ~ 90% (без конденсации)
Источник питания	Защита от перегрузки Версия с питанием от переменного тока ES-3124: 100 ~ 240 В, 60 Вт, 1,5 А макс. ES-3124-4F: 100 ~ 240 В, 60 Вт, 1,5 А макс. ES-3124F: 100 ~ 240 В, 58 Вт, 1,5 А макс. ES-3124PWR: 100 ~ 240 В, 600 Вт, 10 А макс. Версия с питанием от постоянного тока: Допусков на входное напряжение постоянного тока не предусмотрено. Провода сечением 18 AWG или больше. ES-3124: -48 В ~ -60 В, 48 Вт макс., 1,5 А макс. ES-3124-4F: -48 В ~ -60 В, 48 Вт макс., 1,5 А макс. ES-3124F: -48 В ~ -60 В, 48 Вт, 1,5 А макс.
Безопасность	ANS/UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
Электромагнитная совместимость (EMC)	FCC Часть 15 (Класс А) CE EMC (Класс А)

Таблица 121 Характеристики функций

ХАРАКТЕРИСТИКИ		ОПИСАНИЕ
Уровень 2	Мостовая конфигурация	Таблица MAC-адресов на 16 тыс. записей Фильтрация статических MAC-адресов (блокирование портов) Контроль широковещательных штормов Ограничение максимального количества MAC-адресов на порту
	Коммутация	Коммутирующая матрица: 13,6 Гбит/с, без блокирования Максимальный размер кадра: 1522 байта Пересылка кадров: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Предотвращение пересылки поврежденных пакетов
	STP	IEEE 802.1d – протокол покрывающего дерева IEEE 802.1w – быстрый протокол покрывающего дерева IEEE 802.1s – протокол нескольких экземпляров покрывающего дерева До 6 конфигураций покрывающего дерева STP
	Управление качеством обслуживания (QoS)	IEEE 802.1p Восемь очередей приоритетов Поддержка механизма DiffServ RFC 2475, отображение маркеров DSCP на приоритеты IEEE 802.1p
	VLAN	Виртуальные локальные сети на основе портов Виртуальные локальные сети на основе тегов (IEEE 802.1Q) Количество сетей VLAN: 4 тыс. (1000 статических сетей VLAN) Поддержка GVRP Поддержка VLAN на основе протоколов Сети VLAN на основе IP-подсетей
	Агрегация портов	Поддержка стандарта IEEE 802.3ad; статическое и динамическое (по протоколу LACP) группирование портов До шести групп и агрегация до восьми портов в каждой группе
	Зеркальное копирование портов	Поддержка зеркального копирования на всех портах
	Управление пропускной способностью	Поддержка ограничения скорости с шагом 64 кбит/с TRTSM
Уровень 3	Функции IP	Поддержка IPV4 64 домена IP-маршрутизации Таблица IP-адресов на 4 тыс. записей Пересылка IP-пакетов на скорости среды передачи
	Протоколы маршрутизации	Статические маршруты
	IP-службы	Ретрансляция DHCP; Ретрансляция DHCP на основе VLAN Дифференцированное обслуживание DiffServ

Таблица 121 Характеристики функций (продолжение)

ХАРАКТЕРИСТИКИ		ОПИСАНИЕ
Безопасность		<p>Аутентификация порта по стандарту IEEE 802.1x</p> <p>Пересылка на основе статических MAC-адресов</p> <p>Несколько серверов RADIUS</p> <p>Несколько серверов TACACS+</p> <p>Защита от подмены IP-адресов</p> <p>Статическая привязка IP-/MAC-адреса</p> <p>Отслеживание DHCP</p> <p>Инспекция ARP-пакетов</p> <p>Аутентификация по MAC-адресам</p>
Управление	Контроль системы	<p>Контроль сигналов тревоги/состояния</p> <p>Светодиодные индикаторы сигналов тревоги и состояния системы</p> <p>Мониторинг производительности</p> <p>Скорость линии</p> <p>Четыре группы удаленного мониторинга RMON (история, статистика, сигналы тревоги и события)</p> <p>Мониторинг пропускной способности</p> <p>Передача SMP-пакетов</p> <p>Зеркальное копирование и агрегация портов</p> <p>Протокол покрывающего дерева</p> <p>Защита от образования петель</p> <p>Отслеживание многоадресного трафика IGMP</p> <p>Обновление и загрузка встроенного программного обеспечения по FTP/TFTP</p> <p>Авторизация при входе в систему и различные уровни безопасности (только чтение и чтение/записи)</p> <p>Самодиагностика</p> <p>FLASH-память</p> <p>Поддержка летнего времени</p> <p>802.3ah OAM</p>
	Сетевое управление	<p>Работа с интерфейсом командной строки через консольный порт и Telnet</p> <p>Управление через Web</p> <p>Кластеризация: управление группой коммутаторов количеством до 24 через один IP-адрес</p> <p>SNMP</p> <p>Четыре группы удаленного мониторинга RMON (история, статистика, сигналы тревоги и события)</p>
	MIB	<p>RFC1213 MIB II</p> <p>RFC1493 Bridge MIB</p> <p>RFC1643 Ethernet MIB</p> <p>RFC1757 Четыре группы RMON</p> <p>RFC2011 IP MIB</p> <p>RFC2012 TCP MIB</p> <p>RFC2013 UDP MIB</p> <p>RFC2674 Расширение Bridge MIB (для IEEE 802.1Q)</p>

Поддерживаемые коммутатором стандарты приводятся в следующем списке (который не является исчерпывающим).

Таблица 122 Поддерживаемые стандарты

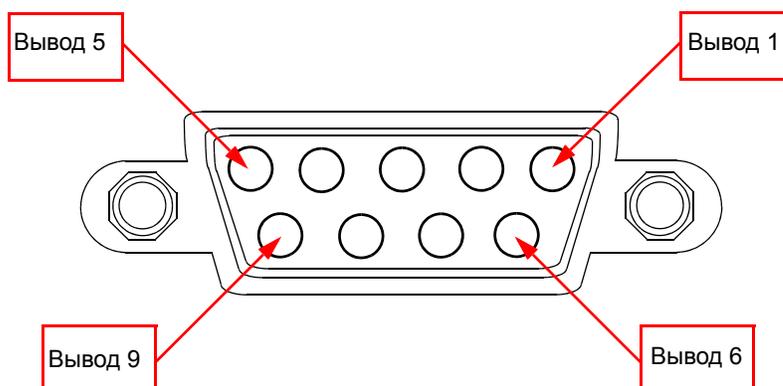
СТАНДАРТ	ОПИСАНИЕ
RFC 826	Протокол разрешения адресов (ARP)
RFC 867	Протокол времени суток
RFC 868	Протокол службы времени
RFC 894	Инкапсуляция Ethernet II
RFC 1112	IGMP v1
RFC 1155	SMI
RFC 1157	SNMPv1: Простой протокол сетевого управления версии 1
RFC 1213	SNMP MIB II
RFC 1305	Протокол сетевого времени (NTP версии 3)
RFC 1441	SNMPv2: простой протокол сетевого управления версии 2
RFC 1493	Bridge MIB
RFC 1643	Ethernet MIB
RFC 1757	Четыре группы RMON
RFC 1901	SNMPv2c: простой протокол сетевого управления версии 2c
RFC 2011	SNMPv2 MIB для IP
RFC 2012	SNMPv2 MIB для TCP
RFC 2013	SNMPv2 MIB для UDP
RFC 2131	DHCP (протокол динамической конфигурации хоста)
RFC 2132	DHCP (протокол динамической конфигурации хоста)
RFC 2138	Служба RADIUS (Remote Authentication Dial In User Service)
RFC 2139	Учет с использованием RADIUS
RFC 2236	Межсетевой протокол управления группами (IGMP), версия 2
RFC 2475	DiffServ, отображение маркеров DSCP на приоритеты IEEE 802.1p
RFC 2674	P-BRIDGE-MIB, Q-BRIDGE-MIB
RFC 2698	Маркеры TRTCM
RFC 2865	Специальные атрибуты производителя для аутентификации RADIUS
RFC 2866	Специальные атрибуты производителя для учета RADIUS
RFC 2869	Специальные атрибуты производителя для учета RADIUS
RFC 3046	Информация агента ретрансляции DHCP (протокола динамической конфигурации хоста)
RFC 3164	Системный журнал Syslog
RFC 3376	Межсетевой протокол управления группами (IGMP), версия 3
RFC 3414	Модель безопасности на базе пользователей (USM) для версии 3 простого протокола сетевого управления (SNMP v3)
RFC 3580	Протокол туннелирования специальных атрибутов производителя для аутентификации RADIUS
IEEE 802.1D	Мосты MAC
IEEE 802.1d	Приоритеты на уровне управления доступом к среде (MAC)

Таблица 122 Поддерживаемые стандарты (продолжение)

СТАНДАРТ	ОПИСАНИЕ
IEEE 802.1p	Приоритеты на уровне управления доступом к среде (MAC)
IEEE 802.1s	Протокол нескольких экземпляров покрывающего дерева
IEEE 802.1Q	VLAN на основе тегов
IEEE 802.1w	Быстрый протокол покрывающего дерева
IEEE 802.1x	Аутентификация портов
IEEE 802.3/3u	Fast Ethernet
IEEE 802.3ab	Gigabit Ethernet
IEEE 802.3ad	Агрегация каналов
IEEE 802.3af	Питание устройств по витой паре
IEEE 802.3x	Управление потоком
IEEE 802.3z	1000BASE-X Для оптоволоконных соединений 1000BASE-SX/LX.

38.2 Назначение выводов кабеля

При соединении через последовательный порт компьютер, как правило, выступает в роли DTE (оконечного оборудования данных, ООД), а модем – в роли DCE (аппаратуры передачи данных, АПД). Данный коммутатор выступает в роли DCE при подключении компьютера к консольному порту. При подключении модема к порту резервного коммутируемого соединения коммутатор выступает в роли DTE.³

Рисунок 168 Назначение выводов консольного порта/порта резервного коммутируемого соединения

3. Используются выводы 2,3 и 5.

Таблица 123 Назначение выводов консольного порта/порта резервного коммутируемого соединения

КОНСОЛЬНЫЙ ПОРТ RS-232 (типа «мама») DB-9F	ПОРТ РЕЗЕРВНОГО КОММУТИРУЕМОГО СОЕДИНЕНИЯ RS-232 (типа «папа») DB-9M (не на всех моделях)
Вывод 1 = НЕТ Вывод 2 = DCE-TXD Вывод 3 = DCE-RXD Вывод 4 = DCE-DSR Вывод 5 = ЗЕМЛЯ Вывод 6 = DCE-DTR Вывод 7 = DCE-CTS Вывод 8 = DCE-RTS Вывод 9 = НЕТ	Вывод 1 = НЕТ Вывод 2 = DTE-RXD Вывод 3 = DTE-TXD Вывод 4 = DTE-DTR Вывод 5 = ЗЕМЛЯ Вывод 6 = DTE-DSR Вывод 7 = DTE-RTS Вывод 8 = DTE-CTS Вывод 9 = НЕТ
Аналогичные назначения выводов имеет порт CON/AUX. С помощью переключателя CON/AUX изменяются настройки только во встроенном аппаратном обеспечении, и не изменяются назначения выводов порта CON/AUX.	С коммутаторами, оснащенными портом CON/AUX, также поставляется 9-пиновый адаптер для консольного кабеля, который имеет указанные назначения выводов на стороне разъем типа «папа».

Таблица 124 Назначение выводов кабеля Ethernet

НАЗНАЧЕНИЕ ВЫВОДОВ КАБЕЛЯ ETHERNET ДЛЯ ПОРТОВ WAN / LAN							
Стандартный				Кроссоверный			
(Коммутатор)		(Адаптер)		(Коммутатор)		(Коммутатор)	
1	IRD +		1	OTD +	1	IRD +	
2	IRD -		2	OTD -	2	IRD -	
3	OTD +		3	IRD +	3	OTD +	
6	OTD -		6	IRD -	6	OTD -	

ЧАСТЬ V

Приложения и индекс



В приложениях приводится общая информация. Некоторые сведения могут быть неприменимы к данному коммутатору.

[Настройка IP-адреса компьютера \(327\)](#)

[Всплывающие окна, JavaScript и разрешения Java \(349\)](#)

[IP-адреса и подсети \(357\)](#)

[Часто используемые службы \(369\)](#)

[Импорт сертификатов \(373\)](#)

[Правовая информация \(379\)](#)

[Поддержка пользователей \(385\)](#)

[Индекс \(387\)](#)

Настройка IP-адреса компьютера

На компьютере должна быть установлена карта адаптера Ethernet на 10 или 100 Мбит/с и протокол TCP/IP.

Все необходимые программные компоненты для установки и использования протокола TCP/IP на компьютере включены в состав операционных систем Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 и более поздних версий, а также всех версий UNIX/LINUX. Для Windows 3.1 потребуется приобрести пакет TCP/IP стороннего поставщика.

TCP/IP обычно предустанавливается на компьютерах под управлением операционных систем Windows NT/2000/XP, Macintosh OS 7 и более поздних версий.

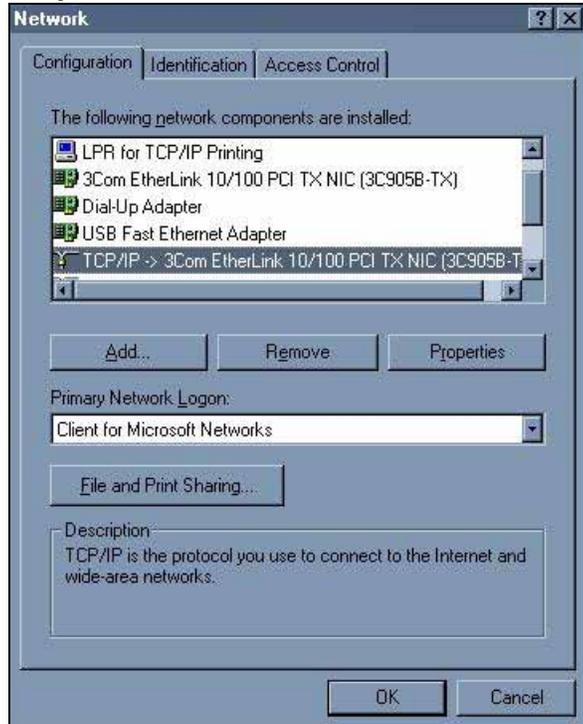
После установки необходимых компонентов TCP/IP потребуется настроить TCP/IP таким образом, чтобы компьютер мог «общаться» с сетью.

В случае настройки IP вручную вместо автоматического назначения все компьютеры должны иметь IP-адреса в той же подсети, что и порт локальной сети коммутатора.

Windows 95/98/Me

Нажмите **Start**, **Settings**, **Control Panel** и дважды щелкните на значке **Network**, чтобы открыть окно **Network**.

Рисунок 169 Windows 95/98/Me: окно Network: Configuration



Установка компонент

Список установленных компонент приводится в окне **Network** на вкладке **Configuration**. В этом списке должны присутствовать сетевой адаптер, протокол TCP/IP и клиент для сетей Microsoft.

Если необходимо добавить адаптер:

- 1 В окне **Network** нажмите на **Add**.
- 2 Выберите **Adapter** и затем нажмите на **Add**.
- 3 Выберите производителя и модель используемого сетевого адаптера и затем нажмите **OK**.

Если необходимо добавить протокол TCP/IP:

- 1 В окне **Network** нажмите на **Add**.
- 2 Выберите **Protocol** и затем нажмите на **Add**.
- 3 Из списка производителей выберите **Microsoft**.
- 4 Выберите из списка сетевых протоколов **TCP/IP** и затем нажмите **OK**.

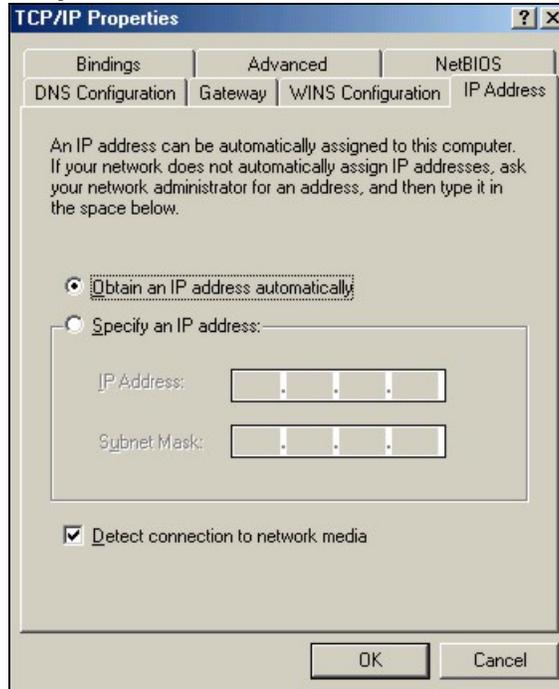
Если необходимо установить клиента для сетей Microsoft:

- 1 Нажмите **Add**.
- 2 Выберите **Client** и затем нажмите на **Add**.
- 3 Из списка производителей выберите **Microsoft**.
- 4 Выберите из списка сетевых клиентов **Client for Microsoft Networks** и затем нажмите **OK**.
- 5 Перезапустите компьютер, чтобы изменения вступили в силу.

Настройка

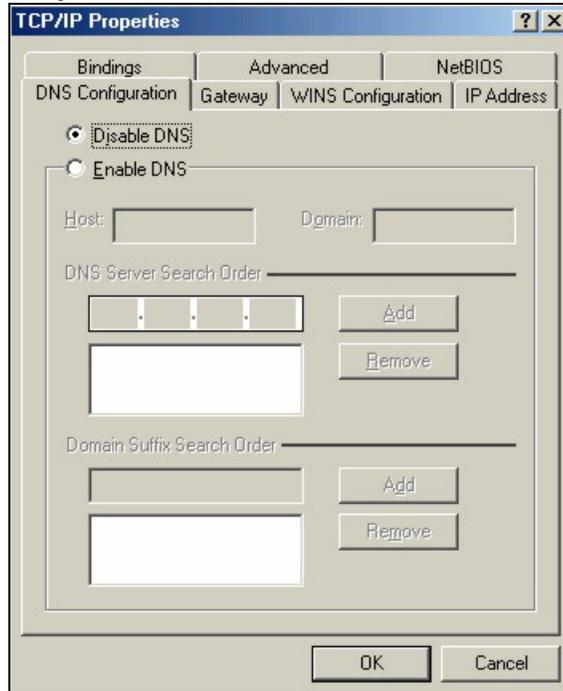
- 1 На вкладке **Configuration** в окне **Network** выберите запись TCP/IP для нужного сетевого адаптера и нажмите на **Properties**
- 2 Нажмите на вкладку **IP Address**.
 - В случае динамического назначения IP-адресов выберите **Obtain an IP address automatically**.
 - В случае статического IP-адреса выберите **Specify an IP address** и введите информацию в поля **IP Address** и **Subnet Mask**.

Рисунок 170 Windows 95/98/Me: окно TCP/IP Properties: IP Address



- 3 Нажмите на вкладку **DNS Configuration**.
 - Если настройки DNS не известны, выберите **Disable DNS**.
 - В случае известных настроек DNS выберите **Enable DNS** и введите информацию в приведенные ниже поля (заполнение всех полей требуется не всегда).

Рисунок 171 Windows 95/98/Me: окно TCP/IP Properties: DNS Configuration



- 4 Нажмите на вкладку **Gateway**.
 - Если IP-адрес шлюза не известен, удалите ранее настроенные шлюзы.
 - В случае известного IP-адреса шлюза введите его в поле **New gateway** и нажмите **Add**.
- 5 Нажмите **OK**, чтобы сохранить изменения и закрыть окно **TCP/IP Properties**.
- 6 Нажмите **OK**, чтобы закрыть окно **Network**. Вставьте компакт-диск с дистрибутивом Windows, если поступит соответствующий запрос.
- 7 Включите коммутатор и перезапустите компьютер после соответствующего запроса системы.

Проверка настроек

- 1 Нажмите **Start** и выберите **Run**.
- 2 В окне **Run** введите «winipcfg» и нажмите **OK**, чтобы открыть окно **IP Configuration**.
- 3 Выберите нужный сетевой адаптер. При этом будут отображены IP-адрес, маска подсети и шлюз по умолчанию вашего компьютера.

Windows 2000/NT/XP

На приведенных ниже рисунках показан графический интерфейс Windows XP с темой по умолчанию.

- 1 Нажмите **start** (**Start** в Windows 2000/NT), **Settings, Control Panel**.

Рисунок 172 Windows XP: меню Start



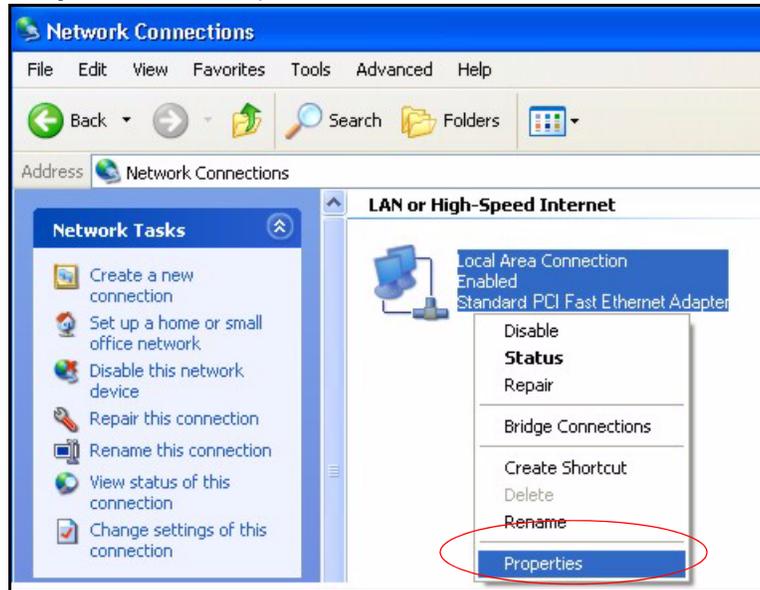
2 В окне **Control Panel** дважды щелкните на **Network Connections (Network and Dial-up Connections** в Windows 2000/NT).

Рисунок 173 Windows XP: окно Control Panel



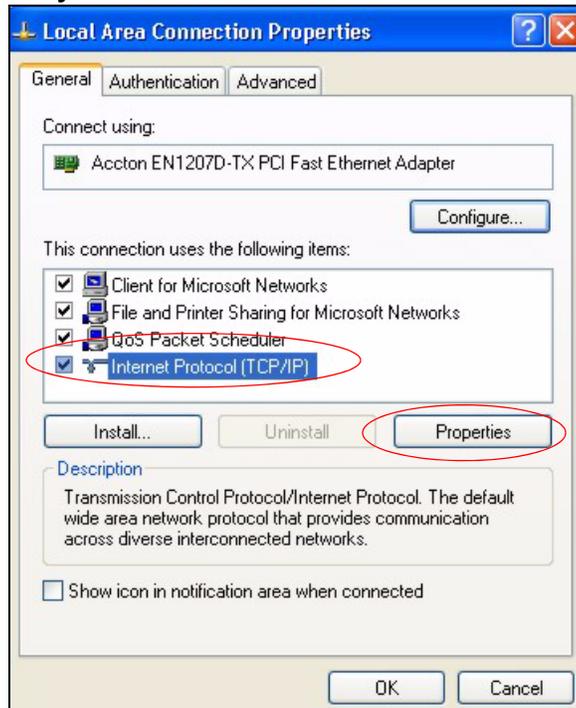
3 Щелкните правой кнопкой мыши на **Local Area Connection** и нажмите **Properties**.

Рисунок 174 Выбор Windows XP: Control Panel: Network Connections: Properties



4 Выберите **Internet Protocol (TCP/IP)** (на вкладке **General** в Win XP) и нажмите **Properties**.

Рисунок 175 Windows XP: окно Local Area Connection Properties

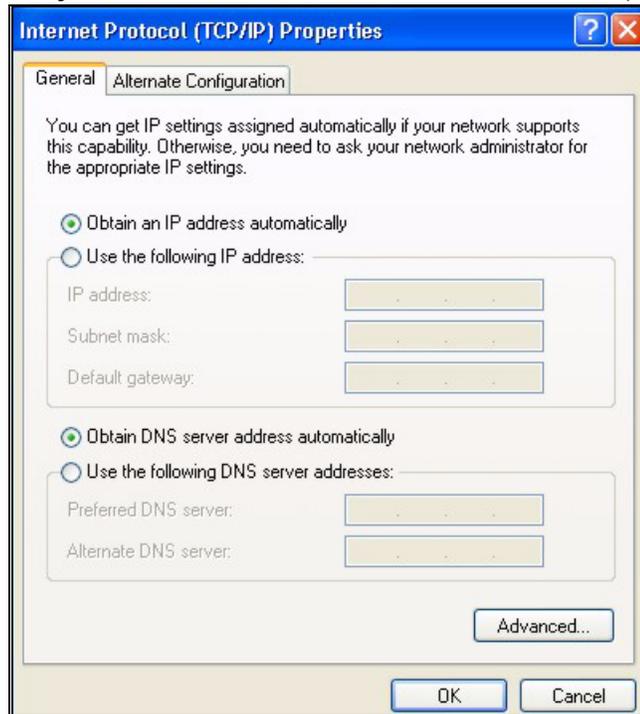


5 Откроется окно **Internet Protocol TCP/IP Properties** (на вкладке **General** в Windows XP).

- В случае динамического назначения IP-адресов нажмите **Obtain an IP address automatically**.
- В случае статического IP-адреса нажмите **Use the following IP Address** и введите значения в поля **IP address**, **Subnet mask** и **Default gateway**.

- Нажмите на **Advanced**.

Рисунок 176 Windows XP: окно Internet Protocol (TCP/IP) Properties

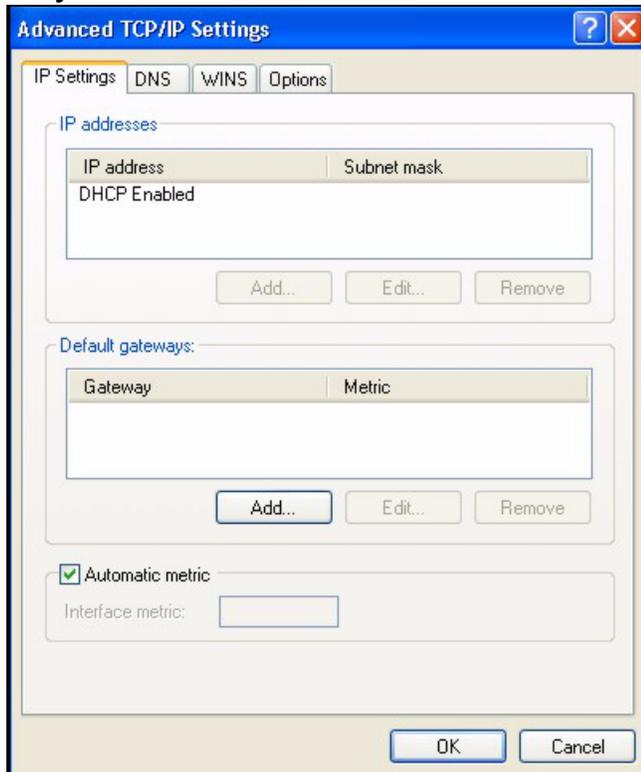


- 6** Если IP-адрес шлюза не известен, удалите все ранее настроенные шлюзы на вкладке **IP Settings** и нажмите **OK**.

При необходимости настроить дополнительные IP-адреса выполните одно или несколько из нижеперечисленных действий:

- На вкладке **IP Settings** в разделе IP-адресов нажмите на **Add**.
- В разделе **TCP/IP Address** введите IP-адрес в поле **IP address** и маску подсети в поле **Subnet mask**, после чего нажмите на **Add**.
- Повторите два приведенных выше шага для всех IP-адресов, которые необходимо добавить.
- Настройте дополнительные шлюзы по умолчанию на вкладке **IP Settings**, нажав на **Add** в разделе **Default gateways**.
- В разделе **TCP/IP Gateway Address** введите IP-адрес шлюза по умолчанию в поле **Gateway**. Чтобы вручную настроить метрику по умолчанию (количество шагов передачи), снимите выделение с переключателя **Automatic metric** и введите значение метрики в поле **Metric**.
- Нажмите **Add**.
- Повторите три приведенных выше шага для всех шлюзов по умолчанию, которые необходимо добавить.
- По окончании нажмите на **OK**.

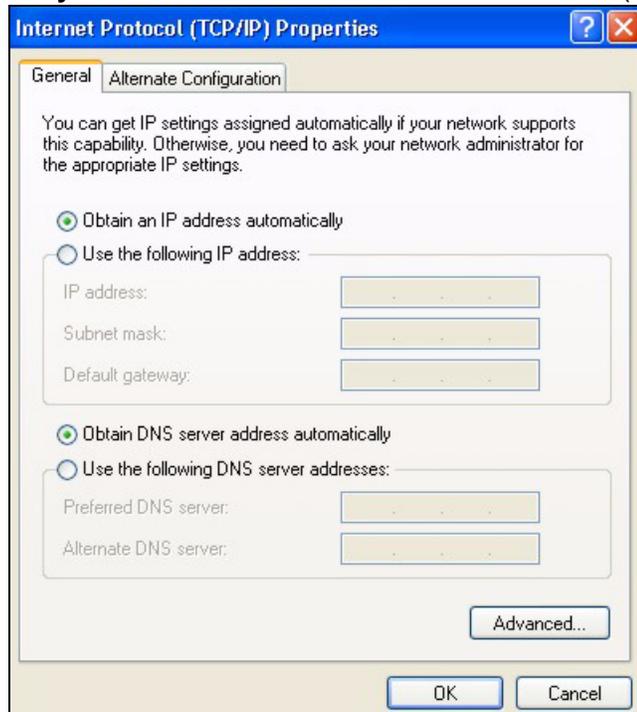
Рисунок 177 Windows XP: окно Advanced TCP/IP Properties



7 В окне **Internet Protocol TCP/IP Properties** (на вкладке **General** в Windows XP):

- Нажмите на **Obtain DNS server address automatically**, если IP-адрес или IP-адреса серверов DNS не известны.
- Если IP-адреса серверов DNS известны, нажмите на **Use the following DNS server addresses** и введите их в поля **Preferred DNS server** и **Alternate DNS server**.

Если ранее адреса DNS-серверов уже настраивались, нажмите на **Advanced** и затем перейдите на вкладку **DNS**, чтобы упорядочить их.

Рисунок 178 Windows XP: окно Internet Protocol (TCP/IP) Properties

- 8** Нажмите **OK**, чтобы закрыть окно **Internet Protocol (TCP/IP) Properties**.
- 9** Нажмите **Close (OK)** в Windows 2000/NT), чтобы закрыть окно **Local Area Connection Properties**.
- 10** Закройте окно **Network Connections (Network and Dial-up Connections)** в Windows 2000/NT).
- 11** Включите коммутатор и перезапустите компьютер (в случае получения соответствующего запроса системы).

Проверка настроек

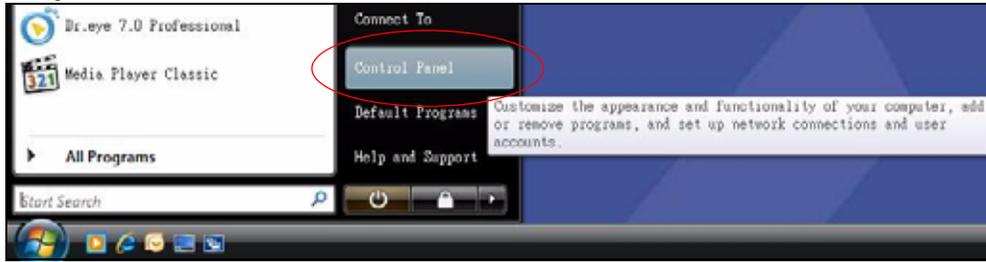
- 1** Нажмите на **Start, All Programs, Accessories** и затем **Command Prompt**.
- 2** В окне **Command Prompt** введите «ipconfig» и нажмите [ENTER]. Кроме того, можно открыть окно **Network Connections**, щелкнуть правой кнопкой мыши на сетевом соединении, нажать на **Status** и затем перейти на вкладку **Support**.

Windows Vista

В данном разделе приводятся изображения экранов для версии Windows Vista Enterprise Version 6.0.

- 1** Нажмите на значок **Start, Control Panel**.

Рисунок 179 Windows Vista: меню Start



2 В окне **Control Panel** дважды щелкните на **Network and Internet**.

Рисунок 180 Windows Vista: окно Control Panel



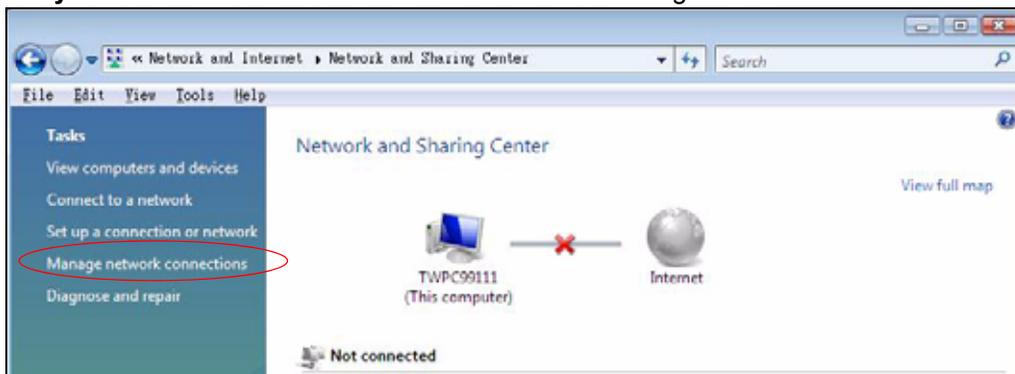
3 Нажмите на **Network and Sharing Center**.

Рисунок 181 Windows Vista: окно Network And Internet



4 Нажмите на **Manage network connections**.

Рисунок 182 Windows Vista: окно Network and Sharing Center

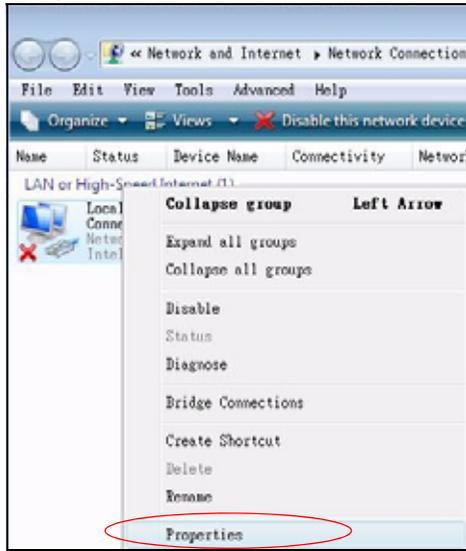


5 Щелкните правой кнопкой мыши на **Local Area Connection** и нажмите **Properties**.



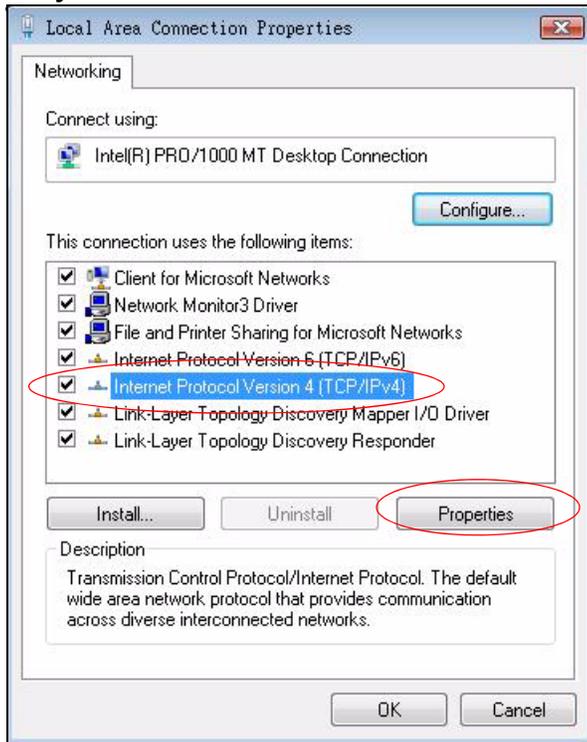
В ходе данной процедуры нажимайте на **Continue** всякий раз, когда Windows запрашивает разрешение на продолжение.

Рисунок 183 Windows Vista: окно Network and Sharing Center



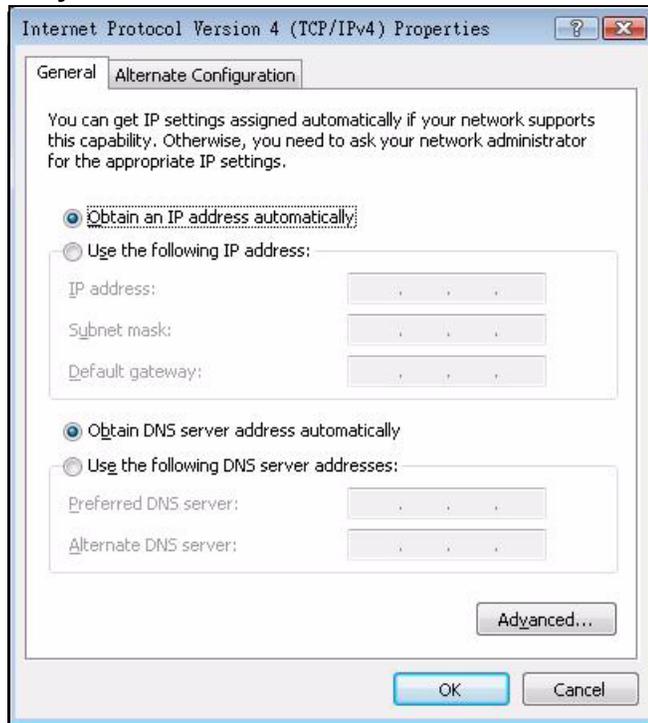
6 Выберите **Internet Protocol Version 4 (TCP/IPv4)** и нажмите на **Properties**.

Рисунок 184 Windows Vista: окно Local Area Connection Properties



- 7 Откроется окно **Internet Protocol Version 4 (TCP/IPv4) Properties** (вкладка **General**).
 - В случае динамического назначения IP-адресов нажмите **Obtain an IP address automatically**.
 - В случае статического IP-адреса нажмите **Use the following IP address** и введите значения в поля **IP address**, **Subnet mask** и **Default gateway**.
 - Нажмите на **Advanced**.

Рисунок 185 Windows Vista: окно Internet Protocol Version 4 (TCP/IPv4) Properties



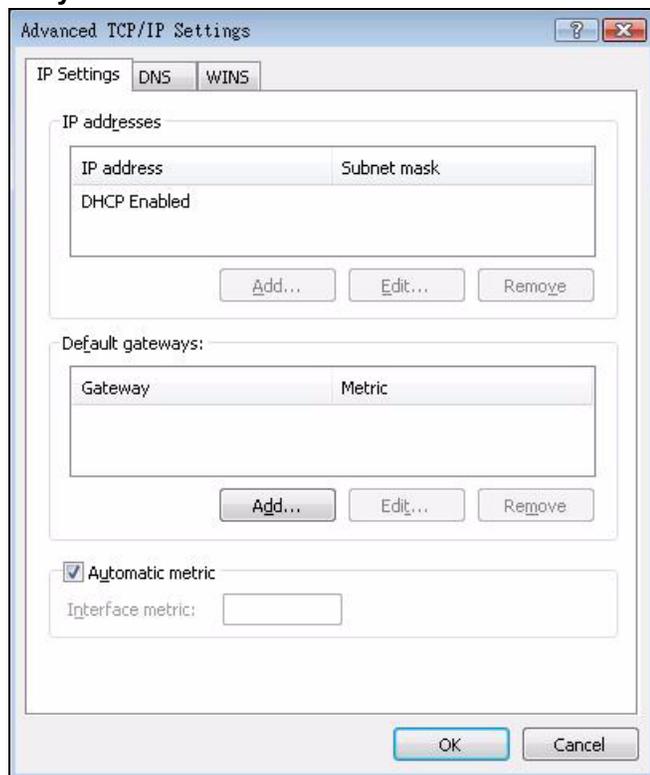
- 8 Если IP-адрес шлюза не известен, удалите все ранее настроенные шлюзы на вкладке **IP Settings** и нажмите **OK**.

При необходимости настроить дополнительные IP-адреса выполните одно или несколько из нижеперечисленных действий:

- На вкладке **IP Settings** в разделе IP-адресов нажмите на **Add**.
- В разделе **TCP/IP Address** введите IP-адрес в поле **IP address** и маску подсети в поле **Subnet mask**, после чего нажмите на **Add**.
- Повторите два приведенных выше шага для всех IP-адресов, которые необходимо добавить.
- Настройте дополнительные шлюзы по умолчанию на вкладке **IP Settings**, нажав на **Add** в разделе **Default gateways**.
- В разделе **TCP/IP Gateway Address** введите IP-адрес шлюза по умолчанию в поле **Gateway**. Чтобы вручную настроить метрику по умолчанию (количество шагов передачи), снимите выделение с переключателя **Automatic metric** и введите значение метрики в поле **Metric**.
- Нажмите **Add**.

- Повторите три приведенных выше шага для всех шлюзов по умолчанию, которые необходимо добавить.
- По окончании нажмите на **ОК**.

Рисунок 186 Windows Vista: окно Advanced TCP/IP Properties

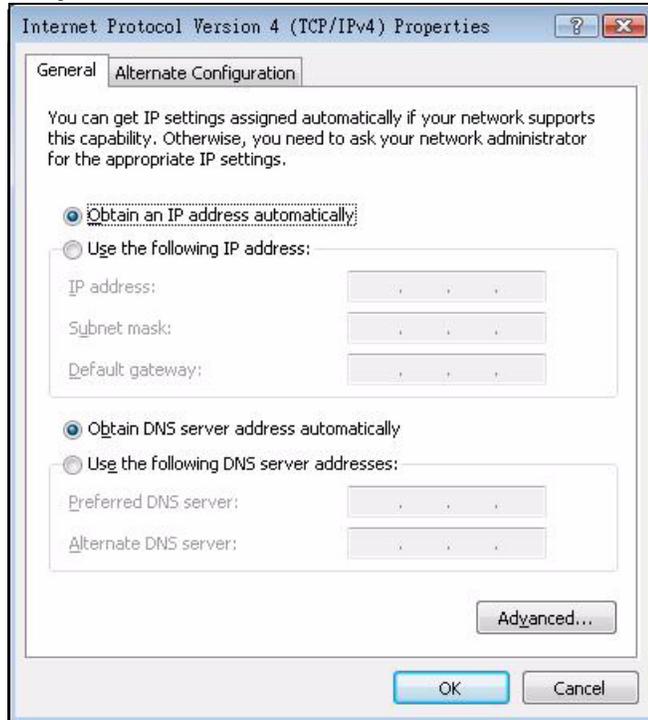


9 В окне **Internet Protocol Version 4 (TCP/IPv4) Properties** (на вкладке **General**):

- Нажмите на **Obtain DNS server address automatically**, если IP-адрес или IP-адреса серверов DNS не известны.
- Если IP-адреса серверов DNS известны, нажмите на **Use the following DNS server addresses** и введите их в поля **Preferred DNS server** и **Alternate DNS server**.

Если ранее адреса DNS-серверов уже настраивались, нажмите на **Advanced** и затем перейдите на вкладку **DNS**, чтобы упорядочить их.

Рисунок 187 Windows Vista: окно Internet Protocol Version 4 (TCP/IPv4) Properties



10 Нажмите **OK**, чтобы закрыть окно **Internet Protocol Version 4 (TCP/IPv4) Properties**.

11 Нажмите **Close**, чтобы закрыть окно **Local Area Connection Properties**.

12 Закройте окно **Network Connections**.

13 Включите коммутатор и перезапустите компьютер (в случае получения соответствующего запроса системы).

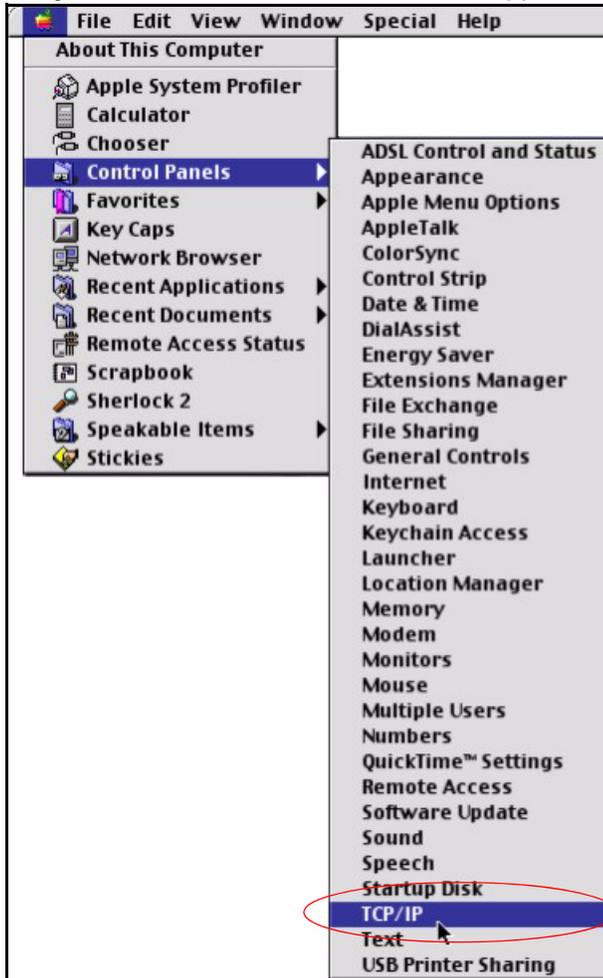
Проверка настроек

- 1** Нажмите на **Start**, **All Programs**, **Accessories** и затем **Command Prompt**.
- 2** В окне **Command Prompt** введите «ipconfig» и нажмите [ENTER]. Кроме того, можно открыть окно **Network Connections**, щелкнуть правой кнопкой мыши на сетевом соединении, нажать на **Status** и затем перейти на вкладку **Support**.

Macintosh OS 8/9

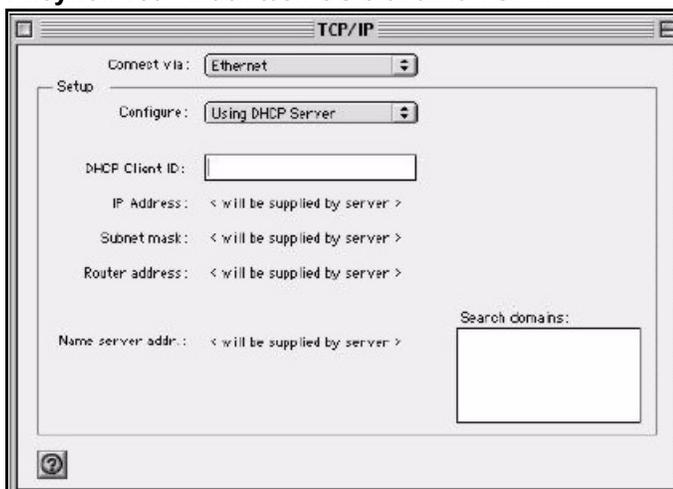
- 1** Нажмите на меню **Apple**, **Control Panel** и дважды щелкните на **TCP/IP**, чтобы открыть окно **TCP/IP Control Panel**.

Рисунок 188 Macintosh OS 8/9: меню Apple



2 Выберите из списка **Connect via** пункт **Ethernet built-in**.

Рисунок 189 Macintosh OS 8/9: окно TCP/IP



3 В случае динамического назначения параметров выберите из списка **Configure:** пункт **Using DHCP Server**.

4 В случае статических настроек выполните следующие действия:

- В поле **Configure** выберите **Manually**.
 - Введите IP-адрес в поле **IP Address**.
 - Введите маску подсети в поле **Subnet mask**.
 - Введите IP-адрес коммутатора в поле **Router address**.
- 5 Закройте окно **TCP/IP Control Panel**.
 - 6 При появлении запроса нажмите на **Save**, чтобы сохранить изменения конфигурации.
 - 7 Включите коммутатор и перезапустите компьютер (в случае получения соответствующего запроса системы).

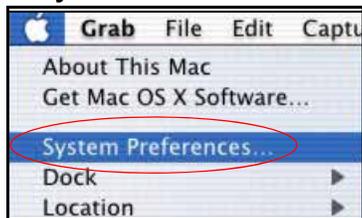
Проверка настроек

Настройки TCP/IP можно проверить в окне **TCP/IP Control Panel**.

Macintosh OS X

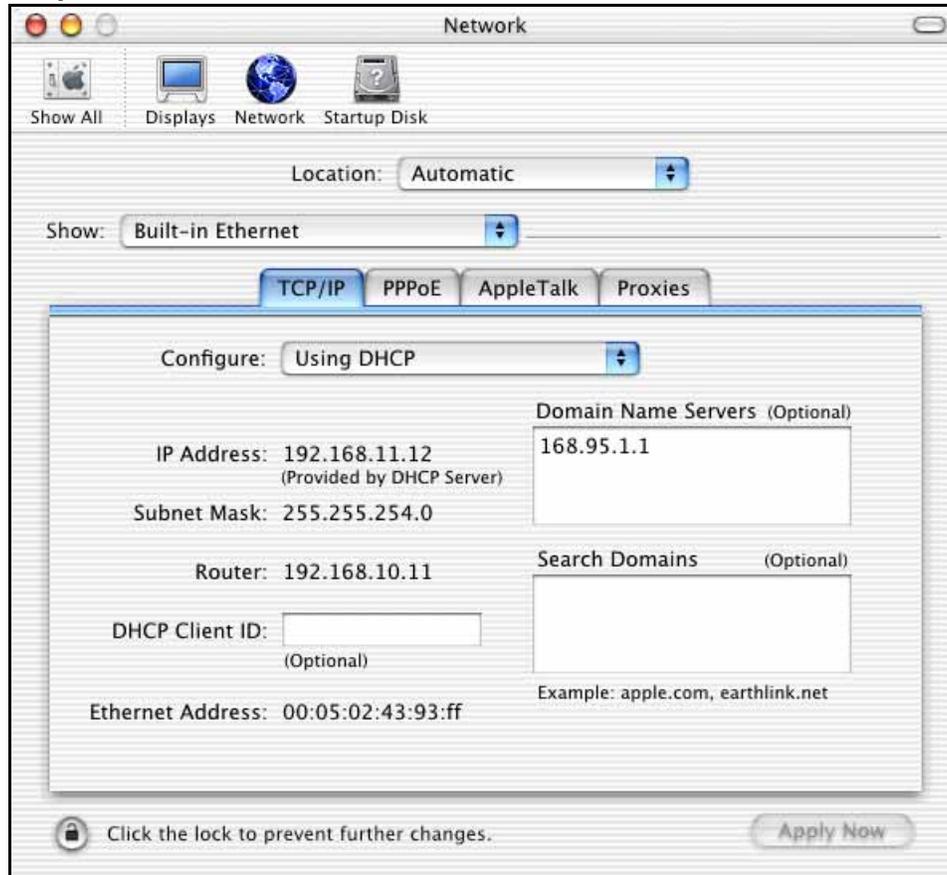
- 1 Нажмите на меню **Apple** и выберите **System Preferences**, чтобы открыть окно **System Preferences**.

Рисунок 190 Macintosh OS X: меню Apple



- 2 Нажмите на **Network** в строке значков.
 - Выберите из списка **Location** значение **Automatic**.
 - Выберите из списка **Show** значение **Built-in Ethernet**.
 - Нажмите на вкладку **TCP/IP**.
- 3 В случае динамического назначения параметров выберите из списка **Configure** пункт **Using DHCP**.

Рисунок 191 Macintosh OS X: окно Network



- 4 В случае статических настроек выполните следующие действия:
 - В поле **Configure** выберите **Manually**.
 - Введите IP-адрес в поле **IP Address**.
 - Введите маску подсети в поле **Subnet mask**.
 - Введите IP-адрес коммутатора в поле **Router address**.
- 5 Нажмите **Apply Now** и закройте окно.
- 6 Включите коммутатор и перезапустите компьютер (в случае получения соответствующего запроса системы).

Проверка настроек

Настройки TCP/IP можно проверить в окне **Network**.

Linux

В данном разделе описана настройка параметров TCP/IP для компьютера под управлением Red Hat Linux 9.0. Порядок действий, внешний вид экранов и расположение файлов зависит от дистрибутива и версии Linux.



Необходимо выполнить вход в систему с правами администратора root.

Использование среды K Desktop Environment (KDE)

Чтобы настроить IP-адрес компьютера с использованием среды KDE, выполните следующие действия.

- 1 Нажмите на кнопку Red Hat (расположена в левом нижнем углу), выберите **System Setting** и нажмите на **Network**.

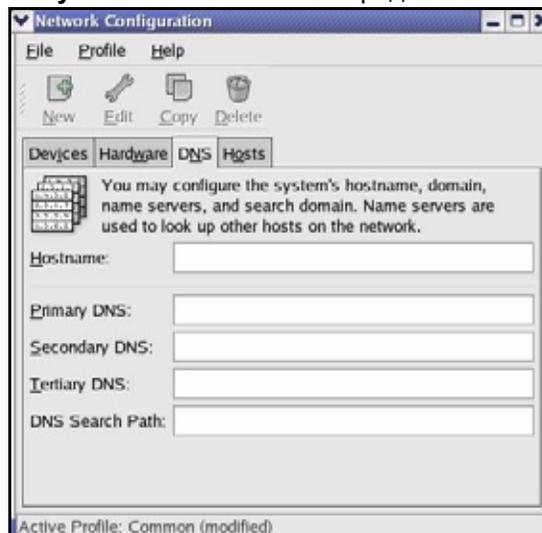
Рисунок 192 Red Hat 9.0: среда KDE: окно Network Configuration: Devices



- 2 Дважды щелкните на профиле сетевой карты, которую необходимо настроить. Появится экран **Ethernet Device General**, показанный на следующем рисунке.

Рисунок 193 Red Hat 9.0: среда KDE: окно Ethernet Device: General

- Если IP-адрес назначается динамически, нажмите на **Automatically obtain IP address settings with** и выберите из выпадающего списка **dhcp**.
 - В случае статического IP-адреса нажмите на **Statically set IP Addresses** и заполните поля **Address**, **Subnet mask** и **Default Gateway Address**.
- 3** Нажмите на **OK**, чтобы сохранить изменения и закрыть экран **Ethernet Device General**.
 - 4** Если известны IP-адреса серверов DNS, нажмите на вкладку **DNS** на экране **Network Configuration**. Введите информацию о серверах DNS в соответствующие поля.

Рисунок 194 Red Hat 9.0: среда KDE: окно Network Configuration: DNS

- 5** Нажмите на вкладку **Devices**.
- 6** Нажмите на кнопку **Activate**, чтобы изменения вступили в силу. Появится следующий экран. Нажмите на **Yes**, чтобы сохранить изменения на всех экранах.

Рисунок 195 Red Hat 9.0: среда KDE: окно Network Configuration: Activate



- 7 После завершения процесса перезапуска сетевой карты убедитесь, что ее статус в поле **Status** на экране **Network Configuration** отображается как **Active**.

Использование файлов конфигурации

Чтобы настроить IP-адрес компьютера посредством редактирования файлов конфигурации сети, выполните следующие действия.

- 1 Если в компьютере установлена только одна сетевая карта, найдите конфигурационный файл `ifconfig-eth0` (где `eth0` – имя карты Ethernet). Откройте конфигурационный файл в любом текстовом редакторе.
 - В случае динамического назначения IP-адреса введите в поле `BOOTPROTO=` значение **dhcp**. Пример показан на следующем рисунке.

Рисунок 196 Red Hat 9.0: настройка динамического получения IP-адреса в файле `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- В случае статического IP-адреса введите в поле `BOOTPROTO=` значение **static**. Введите `IPADDR=` и затем IP-адрес (в формате десятичных чисел, разделенных точками), после чего введите `NETMASK=` и затем маску подсети. В следующем примере показано назначение статического IP-адреса 192.168.1.10 с маской подсети 255.255.255.0.

Рисунок 197 Red Hat 9.0: настройка статического IP-адреса в файле `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 Если известны IP-адреса серверов DNS, введите информацию о серверах DNS в файл `resolv.conf`, находящийся в каталоге `/etc`. Ниже показан пример с вводом IP-адресов двух серверов DNS.

Рисунок 198 Red Hat 9.0: настройки DNS в файле `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 После редактирования и сохранения конфигурационных файлов необходимо перезапустить сетевую карту. Введите `./network restart` в каталоге `/etc/rc.d/init.d`. Пример показан на следующем рисунке.

Рисунок 199 Red Hat 9.0: перезапуск сетевой карты

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Проверка настроек

Чтобы проверить настройки TCP/IP, введите на экране терминала `ifconfig`.

Рисунок 200 Red Hat 9.0: проверка настроек TCP/IP

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```


Всплывающие окна, JavaScript и разрешения Java

Для использования Web-конфигуратора нужно разрешить:

- Всплывающие окна браузера на устройстве.
- JavaScript (по умолчанию включен).
- Разрешения Java (по умолчанию включены).



Ниже описаны экраны браузера Internet Explorer 6. Экраны других версий Internet Explorer могут отличаться.

Блокировщики всплывающих окон Internet Explorer

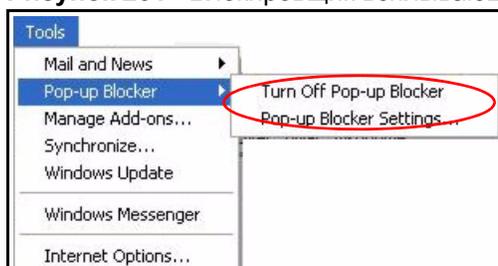
Для подключения к устройству нужно отключить блокировку всплывающих окон.

Необходимо либо отключить блокировку всплывающих окон (она включена по умолчанию в ОС Windows XP с установленным пакетом обновлений Service Pack 2), либо включить блокировку и создать исключение для IP-адреса устройства.

Отключение блокировки всплывающих окон

- 1 В Internet Explorer выберите пункт **Tools, Pop-up Blocker** и затем **Turn Off Pop-up Blocker**.

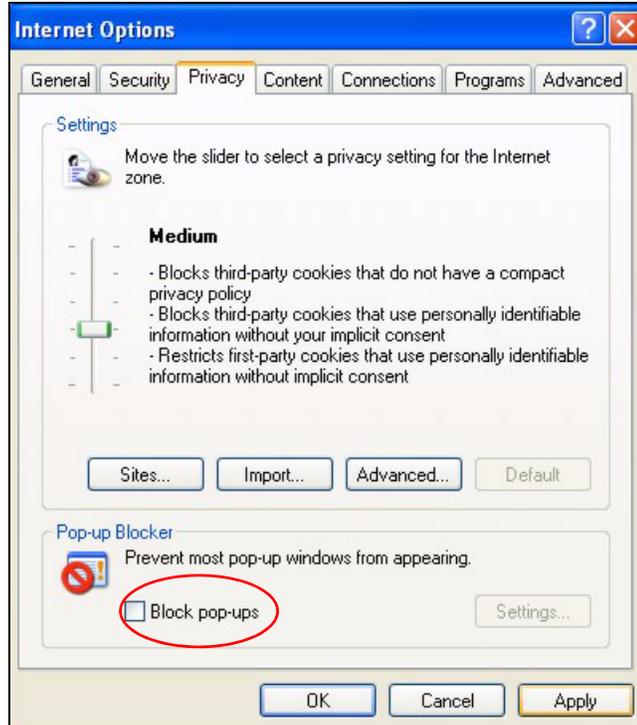
Рисунок 201 Блокировщик всплывающих окон



Проверить, включена ли блокировка всплывающих окон, можно также в разделе **Pop-up Blocker** на вкладке **Privacy**.

- 1 В браузере Internet Explorer выберите пункты **Tools, Internet Options, Privacy**.
- 2 Снимите выделение с переключателя **Block pop-ups** в разделе **Pop-up Blocker** на этом экране. В результате будет отключены все блокировщики окон, которые были включены.

Рисунок 202 Меню Internet Options: Privacy



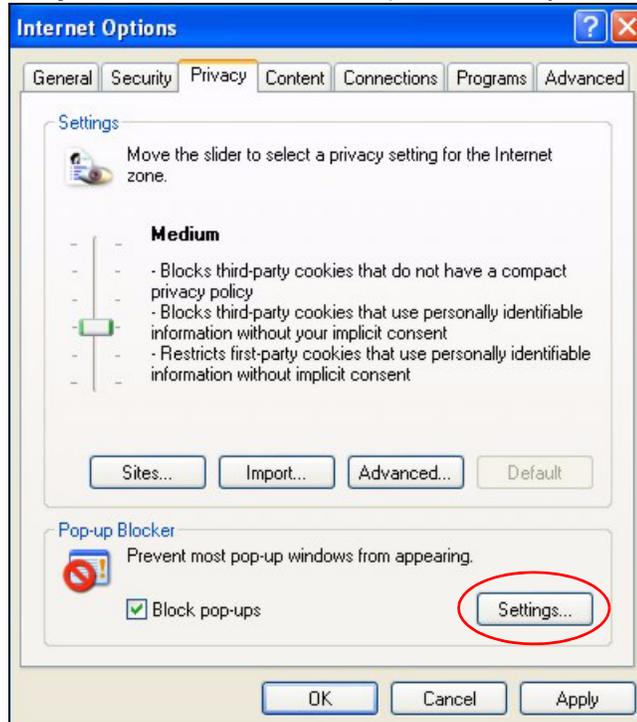
- 3 Нажмите **Apply**, чтобы сохранить эти настройки.

Включение блокировки всплывающих окон и создание исключений

Как вариант, если необходимо разрешить всплывающие окна только от устройства, выполните следующие действия.

- 1 В браузере Internet Explorer выберите пункты меню **Tools, Internet Options, Privacy**.
- 2 Выберите **Settings...**, чтобы открыть экран **Pop-up Blocker Settings**.

Рисунок 203 Меню Internet Options: Privacy



- 3 Введите IP-адрес устройства (Web-страницы, которую не требуется блокировать) с префиксом «http://». Например, http://192.168.167.1.
- 4 Нажмите **Add**, чтобы этот IP-адрес попал в список разрешенных сайтов **Allowed sites**.

Рисунок 204 Экран Pop-up Blocker Settings



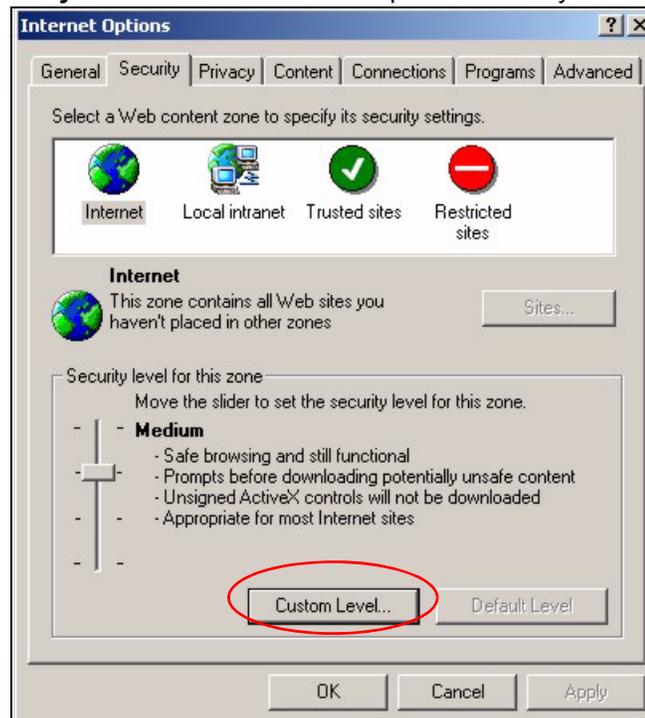
- 5 Нажмите **Close**, чтобы вернуться к экрану **Privacy**.
- 6 Нажмите **Apply**, чтобы сохранить эти настройки.

JavaScript

Если страницы Web-конфигуратора отображаются в Internet Explorer неправильно, проверьте, включен ли JavaScript.

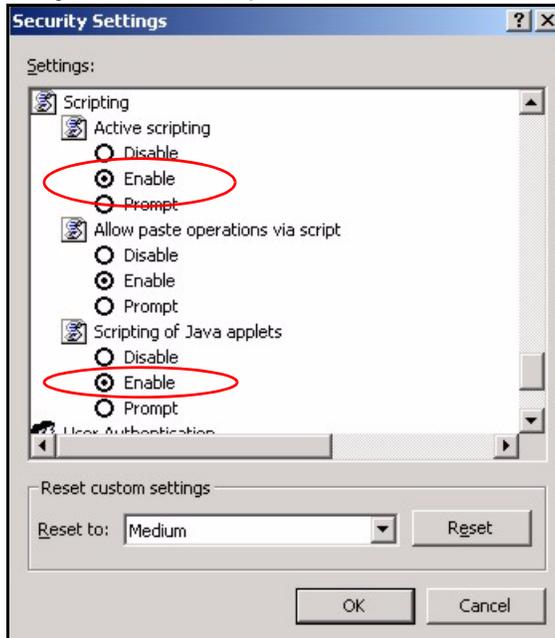
- 1 В браузере Internet Explorer выберите пункты меню **Tools, Internet Options, Privacy**.

Рисунок 205 Меню Internet Options: Security



- 2 Нажмите кнопку **Custom Level...**
- 3 Прокрутите экран до пункта **Scripting**.
- 4 Убедитесь, что в разделе **Active scripting** выбран параметр **Enable** (по умолчанию).
- 5 Убедитесь, что в разделе **Scripting of Java applets** выбран параметр **Enable** (по умолчанию).
- 6 Нажмите **OK**, чтобы закрыть это окно.

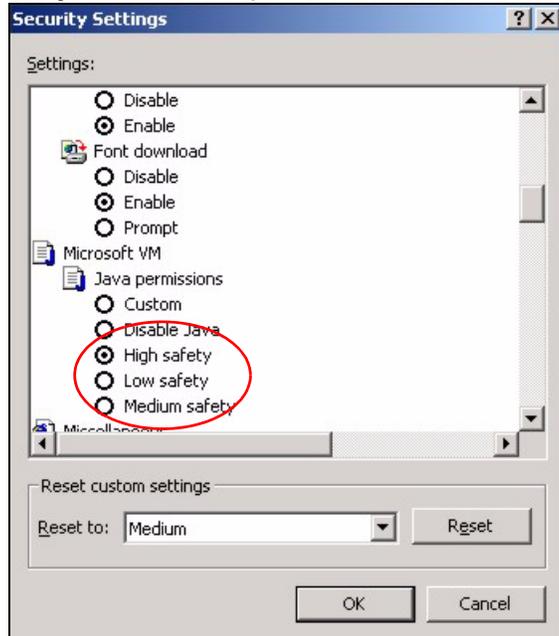
Рисунок 206 Настройки безопасности – JavaScript



Разрешения Java

- 1 В браузере Internet Explorer выберите пункты меню **Tools, Internet Options**, затем **Security**.
- 2 Нажмите кнопку **Custom Level...**
- 3 Прокрутите экран до пункта **Microsoft VM**.
- 4 Убедитесь, что в разделе **Java permissions** выбран нужный уровень безопасности.
- 5 Нажмите **ОК**, чтобы закрыть это окно.

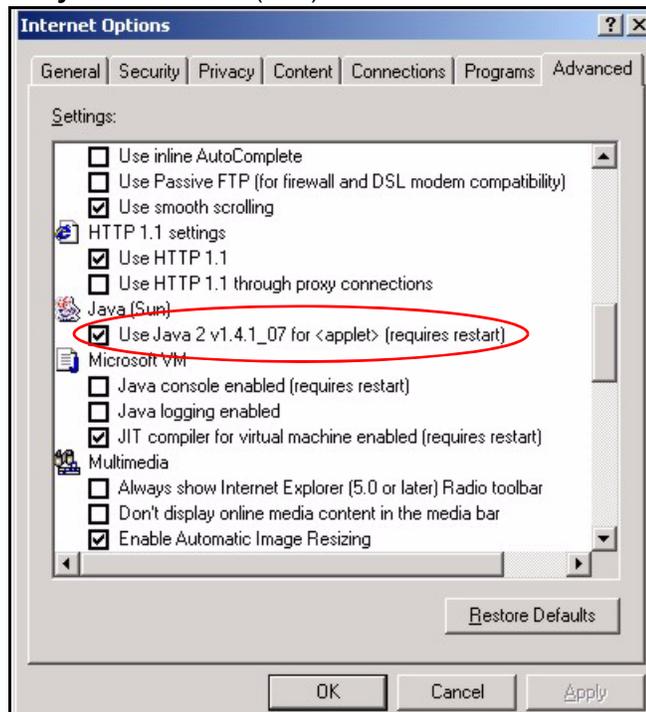
Рисунок 207 Настройки безопасности – Java



JAVA (Sun)

- 1 В браузере Internet Explorer выберите пункты меню **Tools, Internet Options**, затем **Advanced**.
- 2 Убедитесь, в разделе **Java (Sun)** установлен переключатель **Use Java 2 for <applet>**.
- 3 Нажмите **ОК**, чтобы закрыть это окно.

Рисунок 208 Java (Sun)

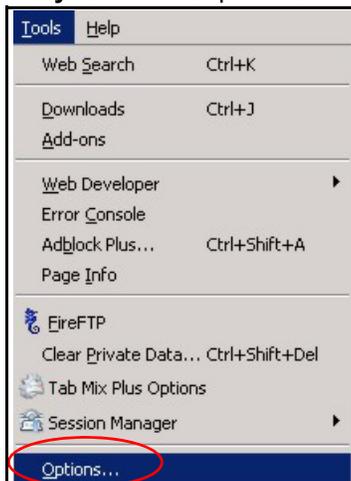


Mozilla Firefox

Ниже описаны экраны браузера Mozilla Firefox 2.0. Экраны других версий могут отличаться.

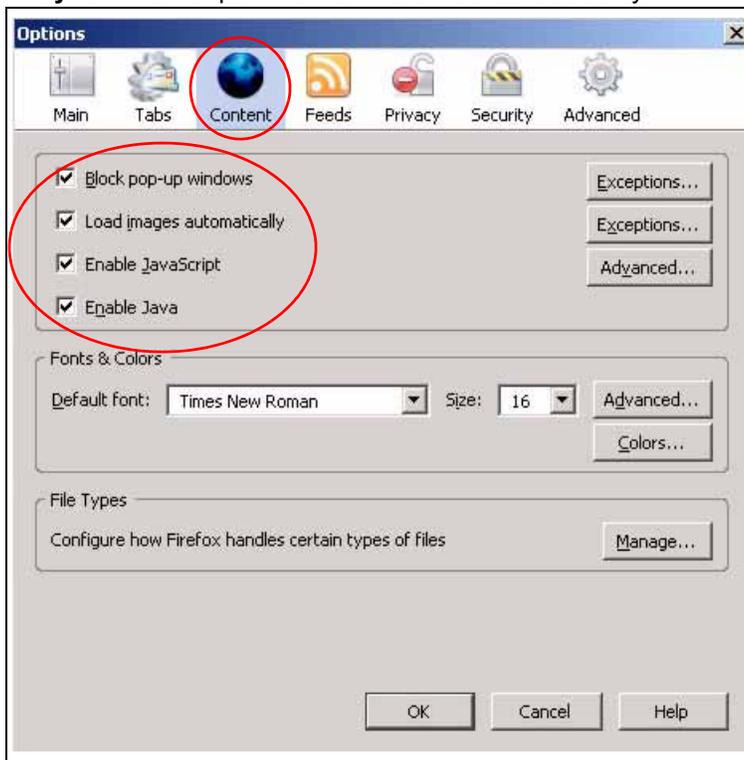
Включение Java, Javascript и всплывающих окон осуществляется на одном экране. Нажмите **Tools** и на появившемся экране выберите **Options**.

Рисунок 209 Экран Mozilla Firefox: Tools > Options



Нажмите **Content**, чтобы открыть показанный ниже экран. Установите переключатели, как показано на следующем экране.

Рисунок 210 Экран Mozilla Firefox Content Security



IP-адреса и подсети

В данном приложении описываются IP-адреса и маски подсетей.

IP-адреса используются для идентификации устройств в сети. Для взаимодействия по сети IP-адрес должен быть назначен каждому сетевому устройству (в том числе компьютерам, серверам, маршрутизаторам, принтерам и т.д.). Такие устройства в сети называют хостами.

С помощью маски подсети определяется максимально возможное число хостов в конкретной сети. Маски подсети позволяют разделить одну сеть на несколько подсетей.

Знакомство с IP-адресами

Одна часть IP-адреса представляет собой номер сети, другая – идентификатор хоста. Точно так же, как у разных домов на одной улице в адресе присутствует одно и то же название улицы, у хостов в сети в адресе имеется общий номер сети. И точно так же, как у различных домов имеется собственный номер дома, у каждого хоста в сети имеется собственный уникальный идентификационный номер – идентификатор хоста. Номер сети используется маршрутизаторами для передачи пакетов в нужные сети, тогда как идентификатор хоста определяет конкретное устройство в этой сети, которому должны быть доставлены пакеты.

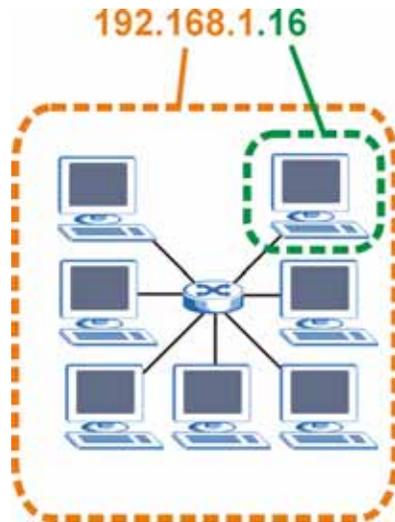
Структура

IP-адрес состоит из четырех частей, записанных в виде десятичных чисел с точками (например, 192.168.1.1). Каждую из этих четырех частей называют октетом. Октет представляет собой восемь двоичных цифр (например, 11000000, или 192 в десятичном виде).

Таким образом, каждый октет может принимать в двоичном виде значения от 00000000 до 11111111, или от 0 до 255 в десятичном виде.

На следующем рисунке показан пример IP-адреса, в котором первые три октета (192.168.1) представляют собой номер сети, а четвертый октет (16) – идентификатор хоста.

Рисунок 211 Номер сети и идентификатор хоста



Количество двоичных цифр в IP-адресе, которые приходятся на номер сети, и количество цифр в адресе, приходящееся на идентификатор хоста, может быть различным в зависимости от маски подсети.

Маски подсети

Маска подсети используется для определения того, какие биты являются частью номера сети, а какие – частью идентификатора хоста (для этого применяется логическая операция конъюнкции – «И»).

Маска подсети включает в себя 32 бита. Если бит в маске подсети равен «1», то соответствующий бит IP-адреса является частью номера сети. Если бит в маске подсети равен «0», то соответствующий бит IP-адреса является частью идентификатора хоста.

На следующем рисунке показана маска подсети, выделяющая номер сети (полужирным шрифтом) и идентификатор хоста в IP-адресе (который в десятичном виде записывается как 192.168.1.2).

Таблица 125 Пример выделения номера сети и идентификатора хоста в IP-адресе

	1-ЫЙ ОКТЕТ: (192)	2-ОЙ ОКТЕТ: (168)	3-ИЙ ОКТЕТ: (1)	4-ЫЙ ОКТЕТ: (2)
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Маска подсети (двоичная)	11111111	11111111	11111111	00000000
Номер сети	11000000	10101000	00000001	
Идентификатор хоста				00000010

Маски подсети всегда состоят из серии последовательных единиц начиная с самого левого бита маски, за которой следует серия последовательных нулей, составляющих в общей сложности 32 бита.

Маску подсети можно определить как количество бит в адресе, представляющих номер сети (количество бит со значением «1»). Например, «8-битной маской» называют маску, в которой 8 бит – единичные, а остальные 24 бита – нулевые.

Маски подсети записываются в формате десятичных чисел с точками, как и IP-адреса. В следующих примерах показаны двоичная и десятичная запись 8-битной, 16-битной, 24-битной и 29-битной масок подсети.

Таблица 126 Маски подсети

	ДВОИЧНАЯ				ДЕСЯТИЧНАЯ
	1-ЫЙ ОКТЕТ:	2-ОЙ ОКТЕТ:	3-ИЙ ОКТЕТ:	4-ЫЙ ОКТЕТ:	
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Количество разрядов в номере сети определяет максимальное количество хостов, которые могут находиться в такой сети. Чем больше бит в номере сети, тем меньше бит остается на идентификатор хоста в адресе.

IP-адрес с идентификатором хоста из всех нулей представляет собой IP-адрес сети (192.168.1.0 с 24-битной маской подсети, например). IP-адрес с идентификатором хоста из всех единиц представляет собой широковещательный адрес данной сети (192.168.1.255 с 24-битной маской подсети, например).

Так как такие два IP-адреса не могут использоваться в качестве идентификаторов отдельных хостов, максимально возможное количество хостов в сети вычисляется следующим образом:

Таблица 127 Максимально возможное число хостов

МАСКА ПОДСЕТИ		РАЗМЕР ИДЕНТИФИКАТОРА ХОСТА		МАКСИМАЛЬНОЕ КОЛИЧЕСТВО ХОСТОВ
8 бит	255.0.0.0	24 бит	$2^{24} - 2$	16777214
16 бит	255.255.0.0	16 бит	$2^{16} - 2$	65534
24 бит	255.255.255.0	8 бит	$2^8 - 2$	254
29 бит	255.255.255.248	3 бит	$2^3 - 2$	6

Формат записи

Поскольку маска всегда является последовательностью единиц слева, дополняемой серией нулей до 32 бит, можно просто указывать количество единиц, а не записывать значение каждого октета. Обычно это записывается как «/» после адреса и количество единичных бит в маске.

Например, адрес 192.1.1.0 /25 представляет собой адрес 192.1.1.0 с маской 255.255.255.128.

Некоторые возможные маски подсети в обоих форматах показаны в следующей таблице.

Таблица 128 Альтернативный формат записи маски подсети

МАСКА ПОДСЕТИ	АЛЬТЕРНАТИВНЫЙ ФОРМАТ ЗАПИСИ	ПОСЛЕДНИЙ ОКТЕТ (В ДВОИЧНОМ ВИДЕ)	ПОСЛЕДНИЙ ОКТЕТ (В ДЕСЯТИЧНОМ ВИДЕ)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

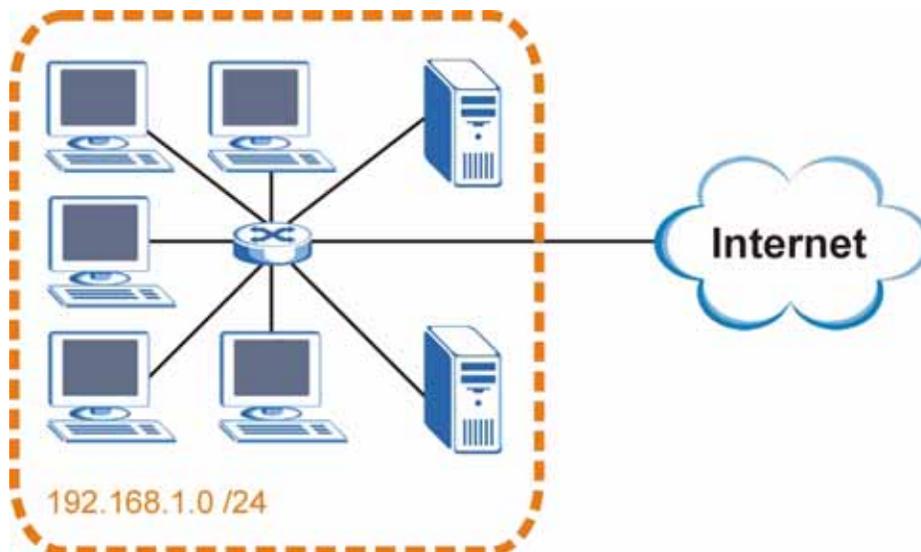
Формирование подсетей

С помощью подсетей одну сеть можно разделить на несколько. В приведенном ниже примере администратор сети создает две подсети, чтобы изолировать группу серверов от остальных устройств в целях безопасности.

В этом примере сеть компании имеет адрес 192.168.1.0. Первые три октета адреса (192.168.1) представляют собой номер сети, а оставшийся октет – идентификатор хоста, что позволяет использовать в сети максимум $2^8 - 2 = 254$ хостов.

Сеть компании до ее деления на подсети показана на следующем рисунке.

Рисунок 212 Пример формирования подсетей: до деления на подсети

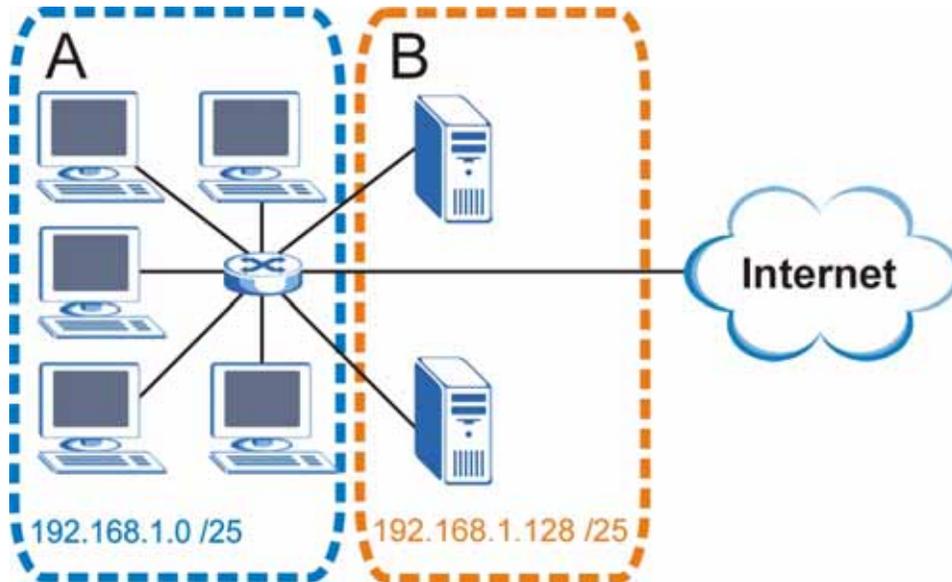


Чтобы разделить сеть 192.168.1.0 на две отдельные подсети, можно «позаимствовать» один бит из идентификатора хоста. В этом случае маска подсети станет 25-битной (255.255.255.128 или /25).

«Одолженный» бит идентификатора хоста может быть либо нулем, либо единицей, что дает нам две подсети; 192.168.1.0 /25 и 192.168.1.128 /25.

Сеть компании после ее деления на подсети показана на следующем рисунке. Теперь она включает в себя две подсети, **A** и **B**.

Рисунок 213 Пример формирования подсетей: после деления на подсети



В 25-битной подсети на идентификатор хоста выделяется 7 бит, поэтому в каждой подсети может быть максимум $2^7 - 2 = 126$ хостов (идентификатор хоста из всех нулей – это сама подсеть, а из всех единиц – широковещательный адрес для подсети).

Адрес 192.168.1.0 с маской 255.255.255.128 является адресом подсети **A**, а 192.168.1.127 с маской 255.255.255.128 является ее широковещательным адресом. Таким образом, наименьший IP-адрес, который может быть закреплен за действительным хостом в подсети **A** – это 192.168.1.1, а наибольший – 192.168.1.126.

Аналогичным образом, диапазон идентификаторов хоста для подсети **B** составляет от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В предыдущем примере было показано использование 25-битной маски подсети для разделения 24-битного адреса на две подсети. Аналогичным образом, для разделения 24-битного адреса на четыре подсети потребуется «одолжить» два бита идентификатора хоста, чтобы получить четыре возможных комбинации (00, 01, 10 и 11). Маска подсети состоит из 26 бит (11111111.11111111.11111111.11000000), то есть 255.255.255.192.

Каждая подсеть содержит 6 битов идентификатора хоста, что в сумме дает $2^6 - 2 = 62$ хоста для каждой подсети (идентификатор хоста из всех нулей – это сама подсеть, а из всех единиц – широковещательный адрес для подсети).

Таблица 129 Подсеть 1

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес (десятичный)	192.168.1.	0
IP-адрес (двоичный)	11000000.10101000.00000001.	00000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети 192.168.1.0	Наименьший идентификатор хоста: 192.168.1.1	
Широковещательный адрес: 192.168.1.63	Наибольший идентификатор хоста: 192.168.1.62	

Таблица 130 Подсеть 2

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	64
IP-адрес (двоичный)	11000000.10101000.00000001.	01000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети 192.168.1.64	Наименьший идентификатор хоста: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Наибольший идентификатор хоста: 192.168.1.126	

Таблица 131 Подсеть 3

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	128
IP-адрес (двоичный)	11000000.10101000.00000001.	10000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети 192.168.1.128	Наименьший идентификатор хоста: 192.168.1.129	
Широковещательный адрес: 192.168.1.191	Наибольший идентификатор хоста: 192.168.1.190	

Таблица 132 Подсеть 4

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	192
IP-адрес (двоичный)	11000000.10101000.00000001.	11000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000

Таблица 132 Подсеть 4 (продолжение)

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
Адрес подсети 192.168.1.192	Наименьший идентификатор хоста: 192.168.1.193	
Широковещательный адрес: 192.168.1.255	Наибольший идентификатор хоста: 192.168.1.254	

Пример: Восемь подсетей

Аналогичным образом для создания восьми подсетей используется 27-битная маска (000, 001, 010, 011, 100, 101, 110 и 111).

Значения последнего октета IP-адреса для каждой подсети показаны в следующей таблице.

Таблица 133 Восемь подсетей

ПОДСЕТЬ	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКОВЕЩАТЕЛЬНЫЙ АДРЕС
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Планирование подсетей

Сводная информация по планированию подсетей для сети с 24-битным номером сети приводится в следующей таблице.

Таблица 134 Планирование подсетей для сети с 24-битным номером

КОЛИЧЕСТВО «ОДОЛЖЕННЫХ» БИТОВ ИДЕНТИФИКАТОРА ХОСТА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ПОДСЕТИ
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Сводная информация по планированию подсетей для сети с 16-битным номером сети приводится в следующей таблице.

Таблица 135 Планирование подсетей для сети с 16-битным номером

КОЛИЧЕСТВО «ОДОЛЖЕННЫХ» БИТОВ ИДЕНТИФИКАТОРА ХОСТА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ПОДСЕТИ
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Настройка IP-адресов

Где именно можно получить номер сети – зависит от конкретной ситуации. Если провайдером услуг Интернета или администратором сети был выделен блок зарегистрированных IP-адресов, при выборе IP-адресов и маски подсети необходимо выполнять полученные от них инструкции.

Если провайдер не указал явным образом номер IP-сети, скорее всего у вас однопользовательская учетная запись, и IP-адрес назначается провайдером динамически при установлении соединения. В этом случае в качестве номера сети рекомендуется использовать значения от 192.168.0.0 до 192.168.255.0. Уполномоченной организацией по распределению нумерации в сети Интернет (IANA) этот блок адресов специально зарезервирован для частного использования; адреса вне этого диапазона следует использовать, лишь получив явные на то указания. Кроме того, необходимо включить на коммутаторекоммутатор механизм трансляции сетевых адресов (NAT).

Определившись с номером сети, выберите легкий для запоминания адрес для своего коммутатора коммутатор (например, 192.168.1.1), и позаботьтесь о том, чтобы этот адрес не использовался никаким другим устройством в сети.

Маска подсети определяет, какую часть в IP-адресе занимает номер сети. коммутатор вычислит маску подсети автоматически на основе введенного IP-адреса. Изменять автоматически вычисленную коммутатором коммутатор маску подсети можно, лишь получив соответствующие инструкции.

Частные IP-адреса

У каждой машины в сети Интернет должен быть уникальный адрес. Если ваши сети изолированы от Интернета (например, связывают два филиала), для хостов без проблем можно использовать любые IP-адреса. Однако, Уполномоченной организацией по распределению нумерации в сети Интернет (IANA) специально для частных сетей зарезервированы следующие три блока IP-адресов:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

IP-адреса можно получить через IANA, у своего провайдера услуг Интернет, или назначить из диапазона адресов для частных сетей. Если ваша организация является небольшой и осуществляет доступ к Интернету через провайдера услуг Интернет, именно провайдер выделит Интернет-адреса для ваших локальных сетей. С другой стороны, если вы являетесь отделом более крупной организации, соответствующие IP-адреса можно получить у администратора корпоративной сети.

В любом случае, не следует назначать IP-адреса произвольным образом; обязательно придерживайтесь приведенных выше рекомендаций. Дополнительную информацию о назначении адресов можно найти в стандартах RFC 1597, Выделение адресов для частных IP-сетей, и RFC 1466, Рекомендации по управлению адресным пространством IP-сетей.

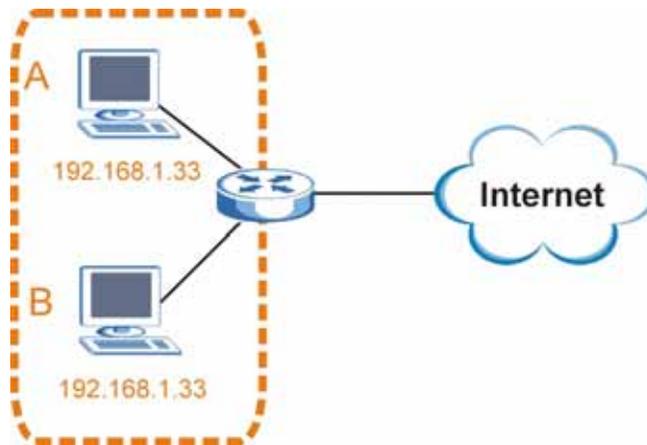
Конфликты IP-адресов

Каждое устройство в сети должно иметь уникальный IP-адрес. Устройства с дублирующимися IP-адресами в одной сети не смогут получить доступа к Интернету и другим ресурсам. Такие устройства также могут оказаться недоступными по сети.

Пример с конфликтом IP-адресов компьютеров

Несколько устройств не должны использовать один и тот же IP-адрес. В показанном ниже примере на компьютере **A** настроен статический (фиксированный) IP-адрес, совпадающий с IP-адресом, назначенным компьютеру **B** (клиенту DHCP) сервером DHCP. Ни один из компьютеров не сможет получить доступа к Интернету. Данную проблему можно разрешить, если назначить компьютеру **A** другой статический IP-адрес или настроить на компьютере **A** режим автоматического получения IP-адреса.

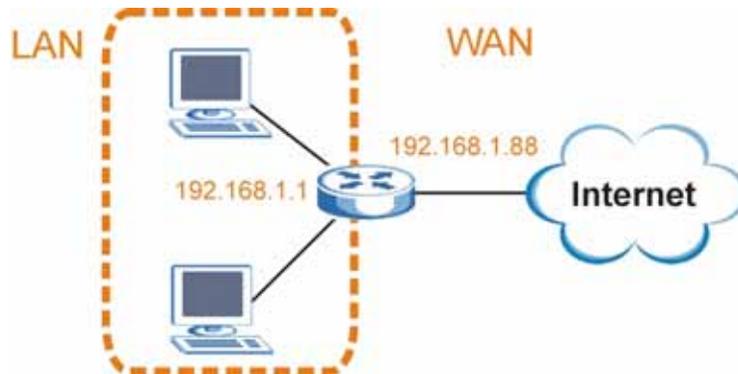
Рисунок 214 Пример с конфликтом IP-адресов компьютеров



Пример с конфликтом IP-адресов маршрутизатора

Так как маршрутизатор подключается к различным сетям, его интерфейсы также должны использовать различные номера сети. Например, если маршрутизатор установлен между локальной сетью и Интернетом (распределенной сетью), то адреса для локальной и распределенной сетей на маршрутизаторе должны относиться к различным подсетям. В показанном ниже примере адреса LAN- и WAN-интерфейсов находятся в одной подсети. Компьютеры в локальной сети не смогут получить доступа к Интернету, так как маршрутизатор не сможет выполнять маршрутизацию между сетями.

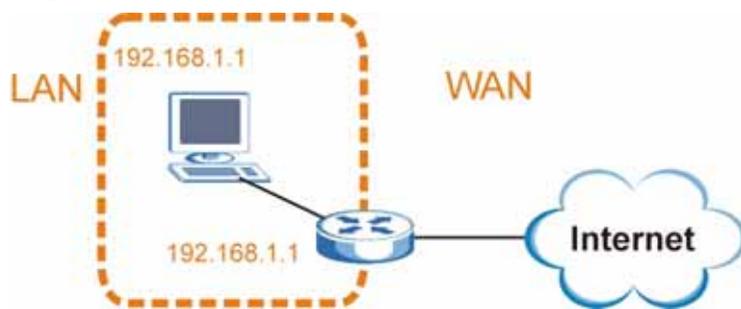
Рисунок 215 Пример с конфликтом IP-адресов маршрутизатора



Пример с конфликтом IP-адресов компьютера и маршрутизатора

Несколько устройств не должны использовать один и тот же IP-адрес. В показанном ниже примере для компьютера и LAN-порта маршрутизатора используется один и тот же IP-адрес 192.168.1.1. Компьютер не сможет получить доступа к Интернету. Данную проблему можно разрешить, если назначить другой IP-адрес компьютеру или LAN-порту маршрутизатора.

Рисунок 216 Пример с конфликтом IP-адресов компьютера и маршрутизатора



Часто используемые службы

В приведенной ниже таблице перечислен ряд наиболее часто используемых служб, с указанием соответствующих протоколов и номеров портов. Полный перечень номеров портов, кодов/типов ICMP и служб можно найти на сайте IANA (уполномоченной организации по распределению нумерации в сети Интернет).

- **Наименование:** Краткое описательное имя службы. Можно использовать это имя или создать другое, при желании.
- **Протокол:** Тип IP-протокола, используемого службой. Если в этом столбце указано **TCP/UDP**, данной службой используются одинаковые номера портов как для TCP, так и для UDP. Если в этом столбце указано **ОПРЕДЕЛЯЕТСЯ ПОЛЬЗОВАТЕЛЕМ**, в столбце **Порт(ы)** указывается номер протокола IP, а не номер порта.
- **Порты(ы):** Значение в данном столбце зависит от значения в столбце **Протокол**. Более подробную информацию о номерах портов можно найти в RFC 1700.
 - Если в столбце **Протокол** указано **TCP, UDP** или **TCP/UDP**, в данном столбце указывается номер порта IP.
 - Если в столбце **Протокол** стоит **ОПРЕДЕЛЯЕТСЯ ПОЛЬЗОВАТЕЛЕМ**, в данном столбце указывается номер протокола IP.
- **Описание:** Краткое описание приложений, которые используют службу, или ситуаций, в которых используется служба.

Таблица 136 Часто используемые службы

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	Определяется пользователем	51	Данная служба используется протоколом туннелирования IPSEC AH (заголовок аутентификации).
AIM/New-ICQ	TCP	5190	Служба Интернет-сообщений AOL. Также используется как порт прослушивания ICQ.
AUTH	TCP	113	Протокол аутентификации, используемый некоторыми серверами.
BGP	TCP	179	Протокол пограничной маршрутизации.
BOOTP_CLIENT	UDP	68	Клиент DHCP.
BOOTP_SERVER	UDP	67	Сервер DHCP.
CU-SEEME	TCP UDP	7648 24032	Популярное решение для видеоконференций от White Pines Software.

Таблица 136 Часто используемые службы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
DNS	TCP/UDP	53	Сервер доменных имен, служба, определяющая соответствие между именами в Интернете (такими как www.zyxel.com) и IP-адресами.
ESP (IPSEC_TUNNEL)	Определяется пользователем	50	Данная служба используется протоколом туннелирования IPSEC ESP (Encapsulation Security Protocol).
FINGER	TCP	79	Finger – команда в UNIX или в Интернете, используемая для поиска зарегистрированных в системе пользователей.
FTP	TCP TCP	20 21	Программа передачи файлов, программа, обеспечивающая быструю передачу файлов, в том числе файлов большого размера, которые не всегда возможно передать по электронной почте.
H.323	TCP	1720	Данный протокол используется программой NetMeeting.
HTTP	TCP	80	Протокол передачи гипертекста – протокол клиент/сервер для сети World Wide Web.
HTTPS	TCP	443	HTTPS – защищенные сессии http, часто используемые в электронной коммерции.
ICMP	Определяется пользователем	1	Межсетевой протокол контрольных сообщений часто используется для диагностики или маршрутизации.
ICQ	UDP	4000	Популярная программа для Интернет-чата.
IGMP (MULTICAST)	Определяется пользователем	2	Межсетевой протокол управления группами используется при отправке пакетов определенной группе хостов.
IKE	UDP	500	Алгоритм обмена ключами в Интернете используется для распространения ключей и управления ключами.
IRC	TCP/UDP	6667	Еще одна популярная программа Интернет-чата.
MSN Messenger	TCP	1863	Данный протокол используется службой сообщений Microsoft Networks.
NEW-ICQ	TCP	5190	Программа Интернет-чата.
NEWS	TCP	144	Протокол новостных групп.
NFS	UDP	2049	Сетевая файловая система NFS – распределенная файловая служба клиент/сервер, обеспечивающая прозрачный доступ к совместному использованию файлов в сети.
NNTP	TCP	119	Сетевой протокол передачи новостей представляет собой механизм доставки для службы новостей USENET.

Таблица 136 Часто используемые службы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
PING	Определяется пользователем	1	Packet INternet Groper – протокол, рассылающий эхо-запросы ICMP для проверки доступности удаленного хоста.
POP3	TCP	110	Почтовый протокол Post Office Protocol версии 3 позволяет клиентским компьютерам получать электронную почту с сервера POP3 с использованием временного подключения (TCP/IP или другого).
PPTP	TCP	1723	Протокол туннелирования «точка-точка» обеспечивает защищенную передачу данных через общедоступные сети. Этот порт используется для управляющего канала.
PPTP_TUNNEL (GRE)	Определяется пользователем	47	Протокол туннелирования «точка-точка» PPTP обеспечивает защищенную передачу данных через общедоступные сети. Этот порт используется для канала передачи данных.
RCMD	TCP	512	Служба удаленных команд.
REAL_AUDIO	TCP	7070	Служба потоковой передачи аудио обеспечивает трансляцию звука через Интернет в реальном времени.
REXEC	TCP	514	Демон удаленного исполнения.
RLOGIN	TCP	513	Удаленный вход в систему.
RTELNET	TCP	107	Удаленный Telnet.
RTSP	TCP/UDP	554	Протокол потоковой передачи реального времени (управления средой передачи) RTSP обеспечивает удаленное управление потоками мультимедиа в Интернете.
SFTP	TCP	115	Простой протокол передачи файлов.
SMTP	TCP	25	Простой протокол пересылки почты представляет собой стандарт обмена сообщениями через Интернет. SMTP позволяет передавать сообщения с одного сервера электронной почты на другой.
SNMP	TCP/UDP	161	Простой протокол сетевого управления.
SNMP-TRAPS	TCP/UDP	162	«Ловушки», используемые в протоколе SNMP (RFC:1215).
SQL-NET	TCP	1521	Язык структурированных запросов SQL – интерфейс доступа к данным в различных системах баз данных, в том числе на мейнфреймах, системах среднего уровня, UNIX-системах и сетевых серверах.
SSH	TCP/UDP	22	Программа удаленного входа в систему через защищенную оболочку.
STRM WORKS	UDP	1558	Протокол Stream Works.

Таблица 136 Часто используемые службы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
SYSLOG	UDP	514	Syslog обеспечивает передачу системных контрольных журналов на сервер UNIX.
TACACS	UDP	49	Протокол входа в систему, используемый для систем TACACS (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet – протокол входа в систему и эмуляции терминала, часто используемый в Интернете и UNIX-системах. Работает в сетях TCP/IP. Основное назначение данного протокола – удаленный вход пользователей на хост-системы.
TFTP	UDP	69	Тривиальный протокол передачи файлов – сходный с FTP протокол передачи файлов в Интернете, отличается от FTP использованием протокола UDP (User Datagram Protocol) вместо TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Еще одно решение для видеоконференций.

Импорт сертификатов

В данном приложении описаны процедуры импорта сертификатов в браузерах Netscape Navigator и Internet Explorer 5. Примеры экранов в данном приложении приводятся для устройства ZyWALL 70. В других моделях эти экраны практически аналогичны.

Импорт сертификатов коммутатора в Netscape Navigator

В Netscape Navigator можно указать серверный сертификат коммутатора в качестве постоянного доверенного сертификата, импортировав его в свою операционную систему в качестве доверенного центра сертификации.

Для этого на приведенном ниже экране выберите **Accept This Certificate Permanently**.

Рисунок 217 Сертификат безопасности



Импорт сертификатов коммутатора в Internet Explorer

С помощью браузера Internet Explorer можно сделать самоподписанный сертификат коммутатора доверенным, просто импортировав самоподписанный сертификат в операционную систему в качестве доверенного центра сертификации.

Чтобы с помощью браузера Internet Explorer сделать доверенным сертификат коммутатора, выданный центром сертификации, необходимо импортировать в операционную систему сертификат центра сертификации в качестве доверенного центра сертификации.

Процедура импорта (самоподписанного) серверного сертификата коммутатора в операционную систему в качестве доверенного центра сертификации описана в следующем примере.

- 1 Дважды щелкните в браузере Internet Explorer на значок замка, показанный на следующем экране.

Рисунок 218 Экран входа в систему



- 2 Нажмите **Install Certificate**, чтобы открыть «мастер» установки сертификата **Install Certificate**.

Рисунок 219 Общая информация о сертификате, отображаемая перед импортом



- 3 Нажмите на **Next**, чтобы запустить «мастер» **Install Certificate**.

Рисунок 220 «Мастер» импорта сертификата, шаг 1



4 Выберите, куда необходимо сохранить сертификат, и нажмите **Next**.

Рисунок 221 «Мастер» импорта сертификата, шаг 2



5 Нажмите на **Finish**, чтобы закрыть «мастер» **Import Certificate**.

Рисунок 222 «Мастер» импорта сертификата, шаг 3



- 6 Нажмите **Yes**, чтобы добавить сертификат коммутатора в хранилище корневых сертификатов.

Рисунок 223 Хранилище корневых сертификатов

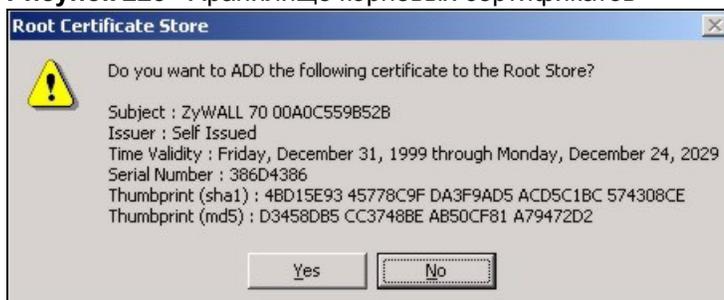


Рисунок 224 Общая информация о сертификате, отображаемая после импорта



Правовая информация

Уведомление об авторских правах

Copyright © 2007 ZyXEL Communications Corporation.

Воспроизводить в любой форме полностью или в любой его части, цитировать, сохранять в системе поиска информации, переводить на любой язык или передавать в любой форме и любым способом, включая, в том числе, электронный, механический, магнитный, оптический, химический, фотокопировальный или ручной, содержание настоящей публикации без предварительного письменного согласия ZyXEL Communications Corporation не разрешается.

Издано ZyXEL Communications Corporation. С сохранением всех прав.

Уведомление

ZyXEL снимает с себя любую ответственность за последствия использования любых продуктов или программного обеспечения, описанных в настоящем документе. Кроме того, ZyXEL не передает никаких лицензий в отношении принадлежащих ZyXEL патентов или патентов третьих лиц. ZyXEL оставляет за собой право вносить изменения в описанные ниже продукты без какого-либо предварительного уведомления. Данная публикация может быть изменена без уведомления.

Товарные знаки

ZyNOS (ZyXEL Network Operating System) является зарегистрированным товарным знаком ZyXEL Communications, Inc. Прочие товарные знаки, упоминающиеся в настоящей публикации, используются исключительно для идентификации и могут представлять собой собственность соответствующих компаний.

Важная информация

Регистрация прав собственника

После завершения установки мы рекомендуем зарегистрировать ваше изделие ZyXEL через Интернет по адресу <http://zyxel.ru>.

Регистрация через Интернет дает дополнительный год бесплатной гарантии, персональную техническую поддержку, уведомление по электронной почте об обновлениях, ряд других преимуществ и льгот.

Информация о сертификации

Коммутаторы ZyXEL серии ES-3124 одобрены для применения государственными органами по сертификации средств связи.

Система сертификации ГОСТ Р, Госстандарт России

Сертификат соответствия № РОСС ТW.АЯ46.В55576 для коммутатора ES-3124. Срок действия с 18.04.2007 по 17.04.2010.

Сертификат соответствия № РОСС-ТW.АЯ46.В55031 для коммутатора ES-3124-4F. Срок действия с 29.03.2007 по 28.03.2010.

Сертификат соответствия РОСС ТW.АЯ46.В56760 для коммутатора ES-3124PWR. Срок действия с 19.06.2007 по 18.06.2010.

Сертификат соответствия РОСС ТW.АЯ46.В11222 для коммутатора ES-3124F. Срок действия с 29.12.2006 по 28.12.2009.

Соответствие требованиям: ГОСТ Р МЭК 60950-2002, ГОСТ 26329-84 п.п.1.2, 1.3, ГОСТ Р 51318.22-99 (класс Б), ГОСТ Р 51318.24-99 (группа 1), ГОСТ Р 51317.3.2-99, ГОСТ Р 51317.3.3-99, ГОСТ Р 51318.3.3-99.

Система сертификации Федерального Агентства Связи

Сертификат соответствия № ОС-1-СПД-0247 для коммутатора ES-3124. Срок действия с 25.09.2006 по 25.09.2009.

Сертификат соответствия № ОС-1-СПД-0337 для коммутатора ES-3124PWR. Срок действия с 01.12.2006 по 01.12.2009.

Соответствие требованиям: РД 45.176-2001.

Декларация соответствия № Д-СПД-1477 для коммутатора ES-3124-4F. Срок действия с 17.09.2007 по 17.09.2012.

Декларация соответствия № Д-СПД-1473 для коммутатора ES-3124F. Срок действия с 17.09.2007 по 17.09.2012.

Соответствие "Правилам применения оборудования, реализующего технологии коммутации кадров", утвержденным Приказом Министерства информационных технологий и связи Российской Федерации от 7 декабря 2006 г. №158 и зарегистрированным в Минюсте России 21 декабря 2006 г., регистрационный №8655.

Государственная Санитарно-эпидемиологическая служба РФ

Санитарно-эпидемиологическое заключение № 77.01.09.650.П.029095.08.05 для коммутаторов ES-3124 и ES-3124PWR. Срок действия с 22.08.2005 по 10.08.2010.

Санитарно-эпидемиологическое заключение № 77.01.09.401.П.087979.12.06 для коммутаторов ES-3124-4F и ES-3124F. Срок действия с 26.12.2006 по 18.12.2011.

Соответствие требованиям: СанПиН 2.2.2./2.4.1340-03, СанПиН 2.1.8./2.2.4.1190-03.

Юридический адрес изготовителя

ZyXEL Communications Corporation, N 6, Innovation Road II, Science-Based Industrial Park, Hsin-Chu, Taiwan, R.O.C.

Установленный производителем в порядке п.2 ст.5 Федерального закона РФ "О защите прав потребителей" срок службы изделия равен 5 годам с даты производства при условии, что изделие используется в строгом соответствии с настоящим руководством и применимыми техническими стандартами.

© ZyxEL, 2007. Все права защищены.

Воспроизведение, передача, распространение или хранение в любой форме данного документа или любой его части без предварительного письменного разрешения ZyxEL запрещено. Названия продуктов или компаний, упоминаемые в данном руководстве, могут быть товарными знаками или товарными именами соответствующих владельцев. ZyxEL придерживается политики непрерывного развития и оставляет за собой право вносить любые изменения и улучшения в любой продукт, описанный в этом документе, без предварительного уведомления. Содержание этого документа предоставлено на условиях "как есть". ZyxEL оставляет за собой право пересматривать или изменять содержимое данного документа в любое время без предварительного уведомления.

Предупреждения по безопасности

В целях вашей безопасности внимательно прочитайте и следуйте всем предупреждениям и указаниям.

- Чтобы снизить риск возникновения пожара, используйте телекоммуникационные кабели с сечением жил №26 согласно Американскому сортаменту проводов AWG или большего сечения.
- НЕ открывайте устройство. В результате вскрытия или снятия защитных кожухов вы подвергаете себя опасности прикосновения к оголенным токоведущим участкам с опасным высоким напряжением и иным рискам. Обслуживать данное устройство разрешается ТОЛЬКО квалифицированному сервисному персоналу. Для получения дополнительной информации свяжитесь с поставщиком.
- Используйте ОТДЕЛЬНЫЙ источник питания для устройства. Подключите шнур питания или адаптер к источнику питания с требуемым номиналом напряжения (110 В перем. тока в Северной Америке или 230 В перем. тока в Европе).
- НЕ используйте устройство, если источник питания поврежден, так как в этом случае существует опасность поражения электрическим током.
- Если источник питания поврежден, выньте его из розетки.
- НЕ пытайтесь починить источник питания. Чтобы заказать новый источник питания, свяжитесь с местным поставщиком.
- Аккуратно расположите соединительные кабели так, чтобы никто не мог наступить или споткнуться о них. НЕ кладите ничего на шнур питания и НЕ располагайте продукт в таком месте, где кто-нибудь может наступить на шнур.
- При креплении устройства на стене убедитесь, что при этом не пострадают электропроводка, трубы газоснабжения или водоснабжения.
- Не занимайтесь установкой и не эксплуатируйте устройство во время грозы. Существует опасность поражения электрическим током в результате удара молнии.

- НЕ подвергайте устройство воздействию сырости, пыли или агрессивных жидкостей.
- НЕ используйте данный продукт вблизи воды, например, в сыром подвале или неподалеку от плавательного бассейна.
- Убедитесь, что кабели подключены к нужным портам.
- НЕ заслоняйте вентиляционные отверстия устройства, так как ограниченный приток воздуха может послужить причиной повреждения устройства.
- НЕ кладите ничего поверх устройства.
- К устройству разрешается подключать ТОЛЬКО подходящие дополнительные модули.

Гарантийное обслуживание ZyXEL

Мы гордимся надежностью и качеством нашей продукции и верим, что это изделие прослужит вам безотказно долгие годы. Тем не менее, если вы столкнетесь с вопросами при использовании этого изделия, пожалуйста, обратитесь за помощью в региональный офис ZyXEL Communications Corporation.

Гарантийные обязательства

1. Настоящая гарантия действует в течение трех лет с даты приобретения изделия ZyXEL и подразумевает гарантийное обслуживание в случае обнаружения дефектов, связанных с материалами и сборкой. В этом случае потребитель имеет право на бесплатный ремонт изделия.
2. При регистрации приобретенного изделия через Интернет на сайте, указанном в таблице, потребитель получает дополнительный год гарантийного обслуживания.
3. Максимальный срок гарантии, предоставляемой компанией ZyXEL, исчисляется с даты производства изделия и составляет четыре с половиной года. Дата производства определяется по серийному номеру на корпусе изделия: SYxWWxxxxx, где Y – последняя цифра года, а WW – номер недели с начала года.
4. Настоящая гарантия распространяется только на изделия ZyXEL, проданные через официальные каналы дистрибуции ZyXEL.
5. Настоящая гарантия предоставляется компанией ZyXEL в дополнение к правам потребителя, установленным действующим законодательством в стране приобретения.

Условия гарантии

1. Гарантийное обслуживание изделия ZyXEL осуществляется в авторизованных сервисных центрах (АСЦ) ZyXEL на приведенных ниже условиях.
2. Настоящая гарантия действительна только при предъявлении вместе с неисправным изделием правильно заполненного фирменного гарантийного талона с проставленной датой продажи. Компания ZyXEL оставляет за собой право отказать в бесплатном гарантийном обслуживании, если гарантийный талон не будет

предоставлен или если содержащаяся в нем информация будет неполной или неразборчивой.

3. Настоящая гарантия недействительна в случаях, если:

- серийный номер на изделии изменен, стерт, удален или неразборчив;
- изделие переделывалось без предварительного письменного согласия ZyXEL;
- изделие неправильно эксплуатировалось, в том числе: а) использовалось не по назначению или не в соответствии с руководством ZyXEL; б) устанавливалось или эксплуатировалось в условиях, не соответствующих стандартам и нормам безопасности, действующим в стране использования;
- изделие ремонтировалось не уполномоченными на то сервисными центрами или дилерами;
- изделие вышло из строя по причине несчастного случая, удара молнии, затопления, пожара, неправильной вентиляции и иных причин, находящихся вне контроля ZyXEL;
- изделие пострадало при транспортировке, за исключением случаев, когда она производится АСЦ;
- изделие использовалось в дефектной системе.

Контактная информация

СТРАНА	РОССИЯ	УКРАИНА	КАЗАХСТАН
Поддержка через Интернет	http://zyxel.ru/support	support@ua.zyxel.com	http://zyxel.kz/support
Телефон службы поддержки	(800) 200-8929 (495) 542-8929	(800) 504-0040 (044) 247-6978	(800) 080-0055 (3272) 590-689
Сервер в Интернете	http://zyxel.ru	http://www.ua.zyxel.com	http://zyxel.kz
Почтовый адрес	ZyXEL Россия 117279, Москва ул. Островитянова 37а	ZyXEL Украина 04050, Киев ул. Пимоненко 13	ZyXEL Казахстан 050010, Алматы пр. Достык 43, офис 414

Поддержка пользователей

При обращении в службу поддержки пользователей убедитесь, что у вас имеется следующая информация.

Требуемая информация

- Модель продукта и серийный номер.
- Информация о гарантии.
- Дата получения устройства.
- Краткое описание проблемы и шагов, которые были предприняты для ее решения.

Россия

- Поддержка: <http://zyxel.ru/support>
- E-mail отдела продаж: sales@zyxel.ru
- Телефон: (800) 200-8929, (495) 542-8929
- Факс: (495) 542-8925
- Интернет: www.zyxel.ru
- Обычная почта: ZyXEL Россия, 117279 Москва, ул. Островитянова 37а

Украина

- E-mail поддержки: support@ua.zyxel.com
- E-mail отдела продаж: sales@ua.zyxel.com
- Телефон: (800) 504-0040, (044) 247-6978
- Факс: (044) 494-4932
- Интернет: www.ua.zyxel.com
- Обычная почта: ZyXEL Украина, 04050 Киев, ул. Пимоненко 13

Казахстан

- Поддержка: <http://zyxel.kz/support>
- E-mail отдела продаж: sales@zyxel.kz
- Телефон: (800) 080-0055, (3272) 590-689
- Факс: (3272) 590-689
- Интернет: www.zyxel.kz
- Обычная почта: ZyXEL Казахстан, 050010, Алматы, пр. Достык 43, офис 414

Индекс

Символы

- «ловушки»
 - пункт назначения [279](#)
- «ловушки» SNMP [271](#)
 - поддерживаемые [272, 275, 277](#)
- «резервные» порты [144](#)

А

- автоматическая регистрация VLAN [92](#)
- авторизация
 - уровни привилегий [209](#)
- агрегация каналов [143](#)
 - динамическая [143](#)
 - информация идентификатора [144](#)
 - настройка [145, 147](#)
 - состояние [145](#)
- адрес для широковещательных сообщений Ethernet [305](#)
- age [129](#)
- aggregator ID [145, 147](#)
- алгоритм циклического обслуживания [176](#)
- альтернативный формат записи маски подсети [360](#)
- аппаратное обеспечение
 - в стойку [42](#)
 - кронштейны [42](#)
 - меры предосторожности при установке [42](#)
 - обзор [45](#)
 - передняя панель [45](#)
 - резиновые ножки [41](#)
 - трансиверы [48, 49](#)
- аппаратный монитор [79](#)
- ARP
 - как это работает [305](#)
 - просмотр [305](#)
- ARP (протокол разрешения адресов) [305](#)
- атаки «man-in-the-middle» [218](#)
- атрибут протокола туннелирования, и RADIUS [211](#)
- аутентификация
 - и RADIUS [202](#)
 - настройка [206](#)
- аутентификация по MAC-адресам [152](#)

- время устаревания [156](#)
- аутентификация портов [151](#)
 - аутентификация по MAC-адресам [152](#)
 - и RADIUS [203](#)
 - IEEE802.1x [153, 155, 204, 206](#)

Б

- база данных отслеживания DHCP [216](#)
- база данных фильтрации, таблица MAC-адресов [303](#)
- база управляющей информации (MIB) [270](#)
- безопасность [319](#)
- блоки данных мостового протокола (BPDU) [114](#)
- блокировка [63](#)
- блокировка коммутатора [63](#)
- быстрый протокол покрывающего дерева, См. RSTP [113](#)

В (С)

- в стойку [42](#)
- вентиляционные отверстия
 - аппаратное обеспечение [42](#)
- вентиляция [42](#)
- вес очереди [176](#)
- вес, очереди [176](#)
- CFI (индикатор канонического формата) [91](#)
- взвешенное циклическое обслуживание (WRR) [176](#)
- виртуальная локальная сеть (VLAN) [82](#)
- CIST [118](#)
- CIST (общее и внутреннее покрывающее дерево) [116](#)
- внешний сервер аутентификации [202](#)
- восстановление конфигурации [64, 264](#)
- время
 - текущее [81](#)
 - часовой пояс [81](#)
- время устаревания [83](#)
- встроенное программное обеспечение [78](#)
 - обновление [263, 300](#)

вход в систему **55**
 пароль **63**
 входящий порт **108**

Г (D)

DHCP **255**
 агент ретрансляции **255**
 варианты настройки **255**
 настройка **258**
 пример ретрансляции **260**
 режимы **255**
 DHCP (протокол динамической конфигурации хоста) **255**
 DiffServ **247**
 активация **250**
 DSCP **247**
 и TRTCM **252**
 отображение маркеров DSCP на приоритеты IEEE802.1p **253**
 PHB **248**
 поле DS **247**
 пример сети **248**
 группа мультивещания **191**
 группа портов **143**
 группирование портов **143, 319**
 пример **148**
 DS (дифференцированное обслуживание) **247**
 DSCP
 как это работает **248**
 отображение маркеров DSCP на приоритеты IEEE802.1p **253**
 уровень обслуживания **247**
 DSCP (кодированный маркер DiffServ) **247**

Д

диагностика **291**
 ping **292**
 системный журнал **292**
 тест Ethernet-порта **292**
 динамическая агрегация каналов **143**
 дифференцированное обслуживание (DiffServ) **247**
 доверенные порты
 инспекция ARP-пакетов **219**
 отслеживание DHCP **216**
 дополнительная документация **3**

Е (F)

forwarding
 delay **129**
 FTP **37, 265**
 ограничения при работе через WAN **267**
 процедура передачи файлов **266**

Ж (G)

GARP **92**
 GARP (Протокол регистрации по общим атрибутам) **92**
 GMT (время по Гринвичу) **81**
 журнал **292**
 GVRP **92, 98**
 и назначение портов **98**
 GVRP (протокол регистрации VLAN по GARP) **92**

З (H)

защита от образования петель **241**
 как это работает **242**
 отключение порта **243**
 пробный пакет **242**
 защита от образования петель, и STP **241**
 защита от подмены IP-адресов **215**
 инспекция ARP-пакетов **215, 218**
 отслеживание DHCP **215**
 статическая привязка **215**
 защищенная оболочка См. SSH **284**
 здание с несколькими арендаторами (MTU) **82**
 зеркальное копирование портов **319, 141, 142**
 исходящий трафик **142**
 направление **142**
 hops **129**
 HTTPS
 реализация **285**
 открытый ключ, секретный ключ **285**
 сертификаты **285**

И (I)

IANA **365**
 IEEE 802.1p, приоритеты **84**
 IEEE 802.1x **151**

активация [153](#), [155](#), [204](#), [206](#)
 повторная аутентификация [154](#)

IGMP
 версия [185](#)

IGMP (межсетевой протокол управления группами) [185](#)

избыточность портов [144](#)

изменение пароля [63](#)

изоляция портов [98](#), [108](#)

имя пользователя и пароль [283](#)

индикаторы [51](#)

индикаторы состояния [51](#)

индикация температуры [79](#)

инспекция ARP-пакетов [215](#), [218](#)
 доверенные порты [219](#)
 и фильтр MAC-адресов [218](#)
 настройка [219](#)
 сообщения syslog [219](#)

интерфейс командной строки [37](#)

информация о системе [77](#)

IP
 интерфейсы [85](#)
 настройка [85](#)
 службы [319](#)
 функции [319](#)

исходящий порт [108](#)

К

кадры
 без тегов [98](#)
 на основе тегов [98](#)

кадры с двумя тегами [179](#)

класс обслуживания (CoS) [247](#)

классификация [161](#), [163](#)
 и QoS [161](#)
 настройка [161](#), [163](#), [164](#)
 обзор [161](#)
 пример [166](#)
 просмотр [164](#)
 редактирование [164](#)

клонирование порта [307](#), [308](#)
 основные настройки [307](#), [308](#)
 расширенные настройки [307](#), [308](#)

коммутация [319](#)

консольный порт
 настройки [47](#)

контактная информация [385](#)

контроль доступа
 ограничения [269](#)
 порты служб [288](#)
 SNMP [270](#)

удаленное управление [289](#)
 учетные записи пользователей [282](#)

контроль доступа к службам [288](#)
 порты служб [289](#)

контрольный порт [141](#), [142](#)

конфигурация
 изменение текущей конфигурации [263](#)
 имена файлов [265](#)

конфигурация, сохранение [63](#)

кронштейны [42](#)

Л (L)

LACP [144](#)
 приоритет системы [148](#)
 тайм-аут [148](#)

летнее время [81](#)

М

MAC (управление доступом к среде) [78](#)

MAC-адрес [78](#), [305](#)
 максимальное количество на порт [159](#)

магистральные порты VLAN [93](#)

маркеры TRTCM (Two Rate Three Color Marker) [249](#)

маркеры Two Rate Three Color Marker, см. TRTCM [249](#)

маска подсети [358](#)

max
 age [129](#)
 hops [129](#)

менеджер кластера [297](#)

метод организации очередей [175](#), [177](#)

MIB
 и SNMP [270](#)
 поддерживаемые базы MIB [271](#)

MIB (база управляющей информации) [270](#)

мостовая конфигурация [319](#)

MSA (MultiSource Agreement) [48](#)

MSTI [118](#)
 MST ID [118](#)

MSTI (экземпляр покрывающего дерева) [116](#)

MSTP [113](#), [116](#)
 настройка [127](#)
 параметр bridge ID [132](#), [133](#)
 параметр configuration digest [133](#)
 параметр forwarding delay [129](#)
 параметр hello time [129](#), [132](#)

параметр max age [129, 132](#)
 параметр max hops [129](#)
 параметр path cost [130](#)
 параметр port priority [130](#)
 параметр revision level [129](#)
 пример сети [116](#)
 регион MST [117](#)
 MSTP (протокол нескольких экземпляров
 покрывающего дерева) [113](#)
 Multiple STP, см. MSTP [116](#)
 мультивещание [185](#)
 и IGMP [185](#)
 IP-адреса [185](#)
 настройка [187, 188](#)
 обзор [185](#)
 приоритет 802.1 [188](#)
 MVR [193](#)
 настройка [194](#)
 настройка группы [197](#)
 пример сети [193](#)
 MVR (регистрация VLAN-сети
 мультивещания) [193](#)

Н (N)

назначение в очередь по приоритету [84](#)
 настройка [246](#)
 настройка коммутатора [83](#)
 настройка политики [171](#)
 настройки портов [87](#)
 NAT [364](#)
 не заслуживающие доверия порты
 инспекция ARP-пакетов [219](#)
 отслеживание DHCP [216](#)

О

обзор функций [58](#)
 обзор экранов меню [58](#)
 обозначения [4](#)
 обслуживание
 резервное копирование конфигурации [264](#)
 восстановление конфигурации [264](#)
 встроенное программное обеспечение [263](#)
 основной экран [261](#)
 текущая конфигурация [261](#)
 общее и внутреннее покрывающее дерево
 (CIST) [116](#)
 общее и внутреннее покрывающее дерево, См.
 CIST [118](#)

общие настройки [80](#)
 общие функции [319](#)
 ограничение получения MAC-адресов [159](#)
 операционная система ZyNOS (ZyXEL Network
 Operating System) [265](#)
 организация очередей [175](#)
 основные настройки [77](#)
 отслеживание DHCP [215](#)
 доверенные порты [216](#)
 настройка [217](#)
 не заслуживающие доверия порты [216](#)
 поле Option 82 при ретрансляции DHCP [217](#)
 отслеживание многоадресного трафика IGMP [186](#)
 MVR [193](#)

П (P)

параметр hello time [129](#)
 пароль [63](#)
 администратора [283](#)
 пароль администратора [283](#)
 передача файлов по протоколу FTP
 пример команды [266](#)
 передняя панель [45](#)
 перезагрузка
 загрузка конфигурации [263](#)
 перезагрузка системы [263](#)
 пересылка на основе статических MAC-
 адресов [99, 102, 109](#)
 PNB (обработка на каждом конкретном
 переходе) [248](#)
 ping, тестирование соединения [292](#)
 питание
 напряжение [79](#)
 поддержка пользователей [385](#)
 подключения
 аппаратное обеспечение [45](#)
 подробная информация [72](#)
 подсеть [357](#)
 поле Option 82 при ретрансляции DHCP [217](#)
 политика [169, 171](#)
 и DiffServ [167](#)
 и классификация [169](#)
 настройка [169](#)
 обзор [167](#)
 правила [167, 168](#)
 пример [172](#)
 просмотр [171](#)
 получение адресов, MAC [99, 102](#)
 получение MAC-адресов [83, 99, 102, 109, 158](#)
 определение лимита [159](#)

получение помощи [65](#)
 пользовательские профили [202](#)
 порты
 «резервные» [144](#)
 диагностика [292](#)
 GBIC [34](#)
 зеркальное копирование [141](#)
 скорость/режим дуплекса [89](#)
 порты Ethernet [47](#)
 настройки по умолчанию [48](#)
 порты GBIC [34, 48](#)
 порты зеркального копирования [141](#)
 порты mini-GBIC [48](#)
 скорость подключения [48](#)
 типы разъемов [48](#)
 удаление трансивера [49](#)
 установка трансивера [48](#)
 порты mini-GBIC, см. также SFP [48](#)
 предупредительные индикаторы [51](#)
 предупреждения по безопасности [6](#)
 привязки [215](#)
 пример подключения по HTTPS [286](#)
 пример статического группирования портов [148](#)
 приоритет 802.1P [89](#)
 простой протокол сетевого управления, См.
 SNMP [270](#)
 протокол MSTP [115](#)
 протокол нескольких экземпляров покрывающего
 дерева [115](#)
 протокол нескольких экземпляров покрывающего
 дерева, См. MSTP. [113](#)
 протокол покрывающего дерева, См. STP [113](#)
 протокол разрешения адресов (ARP) [305, 307,](#)
 [308](#)
 протокол службы времени [80](#)
 формат [80](#)
 протокол управления агрегацией каналов
 (LACP) [144](#)
 протоколы маршрутизации [319](#)
 PVID [92, 98](#)
 PVID (Кадр приоритета) [92](#)

Q

QoS [319](#)
 и классификация [161](#)

P (R)

RADIUS [202](#)
 и аутентификация [202](#)
 настройка [203](#)
 настройки [203](#)
 преимущества [202](#)
 пример сети [201](#)
 сервер [202](#)
 регион MST [117](#)
 резервное копирование, файла
 конфигурации [264](#)
 резиновые ножки
 установка [41](#)
 RFC 3164 [293](#)
 RSTP [113](#)

C (S)

сброс [64, 262](#)
 к заводским настройкам по умолчанию [262](#)
 сброс коммутатора [64](#)
 светодиоды [51](#)
 сервер времени [80](#)
 сертификаты [379](#)
 SFP (Small Form-Factor Pluggable), см. также mini-
 GBIC [48](#)
 система сетевого управления (NMS) [270](#)
 системный журнал [292](#)
 скорость вентилятора [79](#)
 SNMP [37, 270](#)
 «ловушки» [281](#)
 агент [270](#)
 аутентификация [280](#)
 безопасность [280](#)
 версия 3 и безопасность [271](#)
 и MIB [270](#)
 команды Community [279](#)
 компоненты сети [270](#)
 менеджер [270](#)
 MIB [271](#)
 модель управления [270](#)
 настройка [278](#)
 объектные переменные [270](#)
 операции протокола [270](#)
 поддерживаемые версии [270](#)
 соглашения об именовании файлов,
 конфигурация [265](#)
 состояние [56, 71](#)
 агрегация каналов [145](#)
 индикаторы [51](#)
 питание [79](#)

- подробная информация [72](#)
- порт [71](#)
- STP [123](#), [126](#), [131](#)
- VLAN [94](#)
- состояние питания [79](#)
- состояние портов [71](#)
- сохранение конфигурации [63](#), [262](#)
- специальный атрибут производителя, См. VSA [209](#)
- средства безопасности портов [157](#)
 - настройка [157](#), [243](#)
 - обзор [157](#)
 - ограничение получения MAC-адресов [159](#)
 - получение адресов [158](#)
 - получение MAC-адресов [157](#)
- SSH
 - как это работает [284](#)
 - методы шифрования [285](#)
 - реализация [285](#)
- SSH (защищенная оболочка) [284](#)
- SSL (протокол защищенных сокетов) [285](#)
- статическая привязка [215](#)
- статические маршруты [245](#), [246](#)
- статические VLAN [96](#)
 - добавление тегов [97](#)
 - контроль [97](#)
- статический MAC-адрес [109](#)
- стекирование VLAN [179](#), [181](#)
 - настройка [182](#)
 - пример [179](#)
 - приоритет [181](#)
 - роли портов [180](#), [183](#)
 - формат кадра [181](#)
- STP [113](#), [319](#)
 - BPDU-блок Hello [114](#)
 - и защита от образования петель [241](#)
 - как это работает [114](#)
 - корневой порт [114](#)
 - назначенный мост [114](#)
 - настройка [120](#), [124](#), [127](#)
 - параметр bridge ID [123](#), [127](#)
 - параметр bridge priority [121](#), [125](#)
 - параметр forwarding delay [122](#), [125](#)
 - параметр hello time [122](#), [123](#), [125](#), [127](#)
 - параметр max age [122](#), [123](#), [125](#), [127](#)
 - параметр path cost [114](#), [122](#), [126](#)
 - параметр port priority [122](#), [126](#)
 - состояние [123](#), [126](#), [131](#)
 - состояние порта [115](#)
 - терминология [114](#)
- syslog [219](#), [293](#)
 - настройка [293](#)
 - настройка сервера [294](#)
 - настройки [293](#)
 - протокол [293](#)
 - уровни серьезности [293](#)

Т

- таблица MAC-адресов [303](#)
 - как это работает [303](#)
 - просмотр [304](#)
- таблица привязок [215](#)
 - создание [215](#)
- TACACS+ [202](#)
 - настройка [204](#)
- TACACS+ (Terminal Access Controller Access-Control System Plus) [201](#)
- таймер GARP [83](#), [92](#)
- текущая дата [81](#)
- текущее время [81](#)
- терминология GARP [93](#)
- тест Ethernet-порта [292](#)
- тип обслуживания (ToS) [247](#)
- товарные знаки [379](#)
- трансивер
 - удаление [49](#)
 - установка [48](#)
- TRTCM
 - и DiffServ [252](#)
 - и управление пропускной способностью [252](#)
 - настройка [251](#)
 - режим без учета цвета [249](#)
 - режим с учетом цвета [250](#)

У

- уведомление [379](#)
- уведомление об авторских правах [379](#)
- удаленное управление [289](#)
 - доверенные компьютеры [290](#)
 - службы [290](#)
- уполномоченная организация по распределению нумерации в сети Интернет
 - См. IANA [365](#)
- управление кластерами [297](#)
 - и пароли коммутатора [302](#)
 - менеджер кластера [297](#), [301](#)
 - модели коммутаторов [297](#)
 - настройка [301](#)
 - обновление встроенного программного обеспечения коммутатора-члена кластера [300](#)
 - пример сети [297](#)
 - состояние [298](#)
 - спецификация [297](#)
 - VID [302](#)
 - Web-конфигуратор [299](#)
 - член кластера [297](#), [302](#)

- управление потоком **89**
 - обратное давление **89**
 - стандарт IEEE802.3x **89**
 - управление устройством
 - использование FTP. См. FTP.
 - использование интерфейса командной строки. См. интерфейс командной строки.
 - использование SNMP. См. SNMP.
 - использование Web-конфигуратора. См. Web-конфигуратор.
 - полезные советы **37**
 - управляющий порт **108**
 - управляющий порт CPU **106**
 - уровень приоритета **84**
 - установка
 - в стойку **42**
 - кронштейны **42**
 - меры предосторожности **42**
 - на столе **41**
 - резиновые ножки **41**
 - установка аппаратного обеспечения **41**
 - учет
 - настройка **206**
 - учетные записи пользователей **282**
 - Administrator **282**
 - количество **282**
 - несколько **282**
 - обычный пользователь **282**
- Ф (V)**
- файл конфигурации **64**
 - восстановление **64, 264**
 - резервное копирование **264**
 - сохранение **262**
 - VID **91, 95, 181**
 - кадр приоритета **91**
 - количество возможных идентификаторов VLAN **91**
 - VID (идентификатор VLAN) **91**
 - фильтр MAC-адресов
 - и инспекция ARP-пакетов **218**
 - фильтрация **111**
 - правила **111**
 - фильтрация IGMP **185**
 - профили **188**
 - профиль **191**
 - VLA **102**
 - VLAN **82, 91, 319**
 - автоматическая регистрация **92**
 - введение **82**
 - допустимый тип кадра **98**
 - идентификатор **91**
 - изоляция портов **98**
 - количество VLAN **95**
 - магистральные порты **93, 98**
 - на основе портов, «все подключены» **108**
 - на основе портов, «мастер» **108**
 - на основе портов, изоляция портов **108**
 - на основе тегов **91**
 - настройки порта **97**
 - номер порта **95**
 - состояние **94, 95**
 - статические VLAN **96**
 - тип **83, 94**
 - фильтрация входящих кадров **98**
 - VLAN на основе портов **105**
 - VLAN на базе портов **83**
 - VLAN на основе подсетей **99**
 - и DHCP VLAN **100**
 - и приоритеты **99**
 - настройка **99**
 - VLAN на основе портов **105**
 - «все подключены» **108**
 - «мастер» настроек **108**
 - изоляция портов **108**
 - VLAN на основе протоколов **102**
 - и теги IEEE 802.1Q **102**
 - изоляция трафика **102**
 - пример **104**
 - приоритет **100, 103**
 - шестнадцатеричное обозначение протоколов **100, 103**
 - VLAN на основе тегов **91**
 - VLAN, на основе подсетей, См. VLAN на основе подсетей **99**
 - VLAN-сеть мультитевещения **197**
 - формат NTP (RFC-1305) **80**
 - формат Time (RFC-868) **80**
 - формирование подсетей **360**
 - VSA **209**
 - функции уровня 2 **319**
 - функции уровня 3 **319**

X (W)

 - характеристики продукта **317**
 - характеристики управления **320**
 - Web-конфигуратор **36, 55**
 - вход в систему **55**
 - logout **65**
 - начальная страница **56**
 - обзор экранов меню **58**
 - панель навигации **57**
 - получение помощи **65**

WFQ (взвешенная справедливая постановка в очередь) [176](#)

WRR (взвешенное циклическое обслуживание) [176](#)

Ч

член кластера [297](#)

Э

экземпляр MST, См. MSTI [118](#)

экземпляр покрывающего дерева, См. MSTI. [116](#)