

9160 G2

Беспроводной шлюз

Руководство пользователя

2 ноября 2009 г.

Номер по каталогу 8000348.A



Сертификация ISO 9001
Система управления качеством



© 2009 Psion Teklogix Inc.

2100 Meadowvale Boulevard, Mississauga, Ontario, Canada L5N 7J9

<http://www.psionteklogix.com>

Настоящий документ и содержащаяся в нем информация является собственностью компании Psion Teklogix Inc., носит строго конфиденциальный характер и не подлежит воспроизведению и копированию, полностью или частично, за исключением случаев, направленных на стимулирование продаж произведенных компанией Psion Teklogix продуктов и услуг. Кроме того, настоящий документ не может быть использован для создания, производства, заключения договоров на основе субподряда или любым другим способом, нарушающим интересы компании Psion Teklogix Inc.

Заявление об ограничении ответственности

Были приложены все усилия для того, чтобы настоящий документ содержал полную, точную и актуальную информацию. Кроме того, представленная информация периодически изменяется; все изменения будут включены в новые версии документа.

Компания Psion Teklogix Inc. оставляет за собой право вносить улучшения и/или изменения в продукты и/или программы, описанные в настоящем документе, без предварительного уведомления, и не несет ответственность за убытки, включая помимо прочего косвенные убытки, понесенные в связи с использованием представленного материала, включая помимо прочего опечатки.

Windows[®] и логотип Windows являются торговыми марками или зарегистрированными торговыми марками корпорации Microsoft в Соединенных Штатах Америки и/или других странах.

Все торговые марки и коммерческие названия являются собственностью соответствующих компаний.

Гарантия возврата изделий

Компания Psion Teklogix Inc. предоставляет гарантию возврата данного продукта в течение 12 (двенадцати) месяцев в соответствии с Заявлением об ограниченных гарантийных обязательствах и Ограничением ответственности, которые можно найти на веб-сайте:

www.pSIONteklogix.com/warranty

Гарантия на оборудование, произведенное компанией Psion Teklogix, не распространяется на продукты, которые были модифицированы, изменены или отремонтированы кем-либо другим, кроме специалистов авторизованных сервисных центров компании Psion Teklogix. Для получения дополнительной информации ознакомьтесь с положениями и условиями продаж компании Psion Teklogix.



Важно! *Гарантия компании Psion Teklogix вступает в силу со дня поставки.*

Техническое и информационное обслуживание

Компания Psion Teklogix предоставляет полный спектр услуг по технической и информационной поддержке продуктов для клиентов по всему миру. Эти услуги охватывают техническую поддержку и ремонт продуктов. Список центров службы поддержки находится по адресу www.pSIONteklogix.com/service-and-support.htm

Для получения дополнительной информации о текущих и снятых с производства продуктах перейдите по ссылке <https://teknet.pSIONteklogix.com> и выполните вход в систему. Если вы не зарегистрированы в Teknet, нажмите «Not Registered?» (Нет регистрации?). Раздел с информацией об архивных продуктах доступен в интерактивном формате.



Директива по утилизации электрического и электронного оборудования (WEEE) 2002/96/EC

Настоящий продукт и его аксессуары соответствуют требованиям Директивы по утилизации электрического и электронного оборудования (WEEE) 2002/96/EC. По завершении срока службы продукта или аксессуара компании Psion Teklogix, маркированного указанной ниже меткой, обратитесь к местному представителю компании по вопросу утилизации.

Список международных филиалов находится по адресу

www.pSIONteklogix.com/EnvironmentalCompliance

Директива, ограничивающая содержание вредных веществ (RoHS) 2002/95/EC

Что такое RoHS?

По постановлению Европейского Союза, созданная и произведенная для продажи на территории Европы электронная и электротехническая продукция должна соответствовать высоким стандартам охраны окружающей среды, направленным на снижение загрязнения окружающей среды вредными веществами. Директива, ограничивающая содержание вредных веществ (RoHS), устанавливает максимальное содержание в продуктах следовых количеств свинца, кадмия, ртути, шестивалентного хрома и ингибиторов горения (полиброминированных бифенилов и полиброминированных дифениловых эфиров). После 1 июля 2006 года на рынках стран-членов ЕС могут продаваться только продукты, соответствующие этим высоким стандартам охраны окружающей среды.



Логотип RoHS

Несмотря на отсутствие юридических требований к маркировке продукции, соответствующей стандартам RoHS, компания Psion Teklogix Inc. обозначает соответствие своих продуктов с требованиями Директивы следующим образом.

На задней панели продукта или ниже аккумуляторного отсека (или на соответствующем аксессуаре, например зарядном устройстве или стыковочном узле) расположен логотип RoHS, подтверждающий соответствие продукта требованиям RoHS, изложенным в Директиве ЕС. Помимо указанных ниже случаев, отсутствие маркировки с логотипом RoHS на продукте компании Psion Teklogix означает, что продукт был выпущен на рынок ЕС до 1 июля 2006 г. и не попадает под действие Директивы.



Примечание. На некоторых аксессуарах и периферийных устройствах логотип RoHS будет отсутствовать в связи с ограниченным физическим пространством или как следствие освобождения продуктов от действия Директивы.

СОДЕРЖАНИЕ

| | |
|--|------|
| Краткие сведения о разрешениях и стандартах безопасности . . . | xiii |
|--|------|

Глава 1: Введение

| | | |
|---------|--|----|
| 1.1 | О руководстве | 3 |
| 1.2 | Интерактивная справка, поддерживаемые браузеры и ограничения | 6 |
| 1.3 | Условные обозначения в тексте | 7 |
| 1.4 | Обзор беспроводного шлюза 9160 G2 Wireless Gateway | 8 |
| 1.4.1 | Радиомодули | 9 |
| 1.4.2 | Функции точки доступа | 10 |
| 1.4.3 | Функции базовой станции | 10 |
| 1.4.4 | Функции мини-контроллера | 11 |
| 1.5 | Функции и преимущества | 11 |
| 1.5.1 | Поддержка стандартов IEEE и соответствие стандартам Wi-Fi | 11 |
| 1.5.2 | Функции беспроводной связи | 11 |
| 1.5.2.1 | Протокол Psion Teklogix 802.IQ | 12 |
| 1.5.3 | Функции безопасности | 13 |
| 1.5.4 | Встроенный гостевой интерфейс | 14 |
| 1.5.5 | Кластеризация и автоматическое управление | 14 |
| 1.5.6 | Сеть | 15 |
| 1.5.7 | Поддержка SNMP | 15 |
| 1.5.8 | Возможности обслуживания | 15 |
| 1.6 | Что дальше? | 16 |

Глава 2: Требования к установке

| | | |
|-------|------------------------------------|----|
| 2.1 | Выбор местоположения | 19 |
| 2.1.1 | Условия эксплуатации | 19 |
| 2.1.2 | Обслуживание | 20 |
| 2.1.3 | Радиомодули | 20 |
| 2.1.4 | Кабели питания и антенны | 21 |

| | | |
|---------|---|----|
| 2.1.4.1 | Питание | 21 |
| 2.1.4.2 | Антенны | 21 |
| 2.2 | Подключение к внешним устройствам | 23 |
| 2.2.1 | Порты | 23 |
| 2.2.2 | Установка LAN: обзор | 24 |
| 2.2.3 | Установка LAN: Ethernet | 24 |
| 2.2.3.1 | Кабель Ethernet | 24 |
| 2.2.3.2 | Волоконно-оптический порт Ethernet 100Base-FX | 25 |
| 2.2.4 | Индикаторы статуса (LED) | 25 |
| 2.2.5 | Подключение видеотерминала | 26 |
| 2.3 | Изменение конфигурации с помощью веб-браузера | 26 |

Глава 3: Подготовка к запуску

| | | |
|-------|---|----|
| 3.1 | Беспроводной шлюз 9160 G2 Wireless Gateway | 29 |
| 3.1.1 | Значения по умолчанию беспроводного шлюза 9160 G2 Wireless Gateway | 29 |
| 3.1.2 | Функции, которые не поддерживаются точками доступа | 33 |
| 3.2 | Компьютер администратора | 33 |
| 3.3 | Компьютеры беспроводного клиента | 35 |
| 3.4 | Общие сведения о динамической и статической IP-адресации на беспроводном шлюзе 9160 G2 Wireless Gateway | 36 |
| 3.4.1 | Как точка доступа получает IP-адрес при запуске? | 36 |
| 3.4.2 | Динамическая IP-адресация | 37 |
| 3.4.3 | Статическая IP-адресация | 37 |
| 3.4.4 | Восстановление IP-адреса | 38 |

Глава 4: Быстрые действия по настройке и запуску оборудования

| | | |
|---------|---|----|
| 4.1 | Распаковка беспроводного шлюза 9160 G2 Wireless Gateway | 41 |
| 4.1.1 | Оборудование и порты беспроводного шлюза 9160 G2 Wireless Gateway | 41 |
| 4.1.2 | Составные части беспроводного шлюза 9160 G2 Wireless Gateway | 41 |
| 4.2 | Подключение точки доступа к сети и питанию | 42 |
| 4.2.1 | Примечание о настройке подключений для гостевой сети | 44 |
| 4.2.1.1 | Аппаратные подключения для гостевого VLAN | 44 |
| 4.3 | Включение точки доступа | 45 |

| | | |
|-------|--|----|
| 4.4 | Доступ к веб-страницам администрирования | 45 |
| 4.4.1 | Просмотр базовых параметров точки доступа | 45 |
| 4.5 | Настройка базовых параметров и запуск беспроводной сети | 46 |
| 4.5.1 | Конфигурация по умолчанию | 47 |
| 4.6 | Дальнейшие действия | 47 |
| 4.6.1 | Убедитесь, что точка доступа подключена к LAN | 47 |
| 4.6.2 | Тестирование подключения беспроводных клиентов к LAN | 47 |
| 4.6.3 | Включение дополнительных функций безопасности и точной настройки точки доступа с помощью расширенных настроек | 48 |

Глава 5: Настройка базовых параметров

| | | |
|-----|---|----|
| 5.1 | Переход к базовым параметрам | 51 |
| 5.2 | Обзор и описание точки доступа | 52 |
| 5.3 | Настройка сетевых параметров | 53 |
| 5.4 | Обновление базовых параметров | 54 |
| 5.5 | Базовые параметры автономной точки доступа | 54 |
| 5.6 | Краткий обзор сети: значки индикаторов | 54 |
| 5.7 | Изменение цветов и стиля пользовательского интерфейса | 55 |

Глава 6: Управление точками доступа и кластерами

| | | |
|---------|--|----|
| 6.1 | Обзор | 59 |
| 6.2 | Переход к управлению точками доступа | 59 |
| 6.3 | Общие сведения о кластеризации | 60 |
| 6.3.1 | Что такое кластер? | 60 |
| 6.3.2 | Сколько точек доступа может поддерживать кластер? | 60 |
| 6.3.3 | Какие типы точек доступа могут быть кластеризованы? | 60 |
| 6.3.4 | Какова взаимосвязь координирующей точки доступа с другими членами кластера? | 61 |
| 6.3.5 | Какие параметры являются/не являются общими в конфигурации кластера? | 61 |
| 6.3.5.1 | Общие параметры в конфигурации кластера | 61 |
| 6.3.5.2 | Параметры, не являющиеся общими для кластера | 62 |
| 6.3.6 | Формирование кластера | 62 |
| 6.3.7 | Размер кластера и членство в кластере | 63 |
| 6.3.8 | Безопасность внутри кластера | 63 |

| | | |
|-------|--|----|
| 6.4 | Общие сведения о параметрах точек доступа | 63 |
| 6.4.1 | Изменения описания местоположения | 65 |
| 6.4.2 | Настройка имени кластера | 65 |
| 6.5 | Запуск кластеризации | 65 |
| 6.6 | Остановка кластеризации | 66 |
| 6.7 | Конфигурационная информация определенной точки доступа и управление автономными точками доступа | 66 |
| 6.7.1 | Переход к точке доступа с использованием ее IP-адреса в URL-адресе. | 67 |
| 6.8 | Мониторинг сеансов | 67 |
| 6.8.1 | Переход к мониторингу сеансов | 67 |
| 6.8.2 | Общие сведения о мониторинге сеансов | 68 |
| 6.8.3 | Просмотр информации о сеансах точек доступа | 69 |
| 6.8.4 | Сортировка информации о сеансах | 70 |
| 6.8.5 | Обновление информации о сеансах | 70 |

Глава 7: Управление учетными записями пользователей

| | | |
|-------|--|----|
| 7.1 | Обзор | 73 |
| 7.2 | Переход к управлению пользователями | 73 |
| 7.2.1 | Просмотр учетных записей пользователей | 74 |
| 7.2.2 | Добавление пользователя | 74 |
| 7.2.3 | Редактирование учетной записи пользователя | 75 |
| 7.2.4 | Включение и отключение учетных записей пользователей | 76 |
| 7.2.5 | Включение учетной записи пользователя | 76 |
| 7.2.6 | Отключение учетной записи пользователя | 77 |
| 7.2.7 | Удаление учетной записи пользователя | 77 |
| 7.3 | Резервное копирование и восстановление базы данных пользователей | 77 |
| 7.3.1 | Резервное копирование базы данных пользователей | 77 |
| 7.3.2 | Восстановление базы данных пользователей из резервного файла | 78 |

Глава 8: Управление каналами

| | | |
|-------|---|----|
| 8.1 | Переход к управлению каналами | 81 |
| 8.2 | Общие сведения об управлении каналами | 81 |
| 8.2.1 | Краткое описание процесса | 82 |
| 8.2.2 | Дополнительная информация о перекрывающихся каналах | 82 |
| 8.2.3 | Пример. Сеть до и после управления каналами | 82 |

| | | |
|---------|---|----|
| 8.3 | Настройка и просмотр параметров управления каналами..... | 83 |
| 8.3.1 | Остановка/запуск автоматического назначения каналов | 84 |
| 8.3.2 | Просмотр текущих назначений каналов и настройка блокировок..... | 85 |
| 8.3.2.1 | Ручное обновление текущих параметров канала | 86 |
| 8.3.3 | Просмотр последнего рекомендованного набора изменений..... | 86 |
| 8.3.4 | Настройка расширенных параметров (изменение и составление графика планов каналов)..... | 86 |
| 8.3.4.1 | Обновление расширенных параметров | 88 |

Глава 9: Беспроводное окружение

| | | |
|-----|--|----|
| 9.1 | Переход к экрану беспроводного окружения | 91 |
| 9.2 | Общие сведения о беспроводном окружении..... | 91 |
| 9.3 | Просмотр беспроводного окружения | 92 |
| 9.4 | Просмотр сведений о члене кластера | 94 |

Глава 10: Настройка режимов безопасности

| | | |
|----------|--|-----|
| 10.1 | Общие сведения о проблемах безопасности в беспроводных сетях | 99 |
| 10.1.1 | Какой режим безопасности использовать?..... | 99 |
| 10.1.2 | Сравнение режимов безопасности для алгоритмов управления ключами, аутентификации и шифрования | 100 |
| 10.1.2.1 | Использование режима без шифрования (система безопасности отключена)..... | 101 |
| 10.1.2.2 | Использование статического WEP-шифрования..... | 101 |
| 10.1.2.3 | Использование стандарта IEEE 802.1x..... | 103 |
| 10.1.2.4 | Использование режима безопасности WPA Personal | 104 |
| 10.1.2.5 | Использование режима безопасности WPA Enterprise | 105 |
| 10.1.3 | Повышается ли уровень защиты при запрете широковещательного идентификатора SSID?..... | 107 |
| 10.1.4 | Как изоляция станции защищает сеть?..... | 107 |
| 10.2 | Настройка параметров безопасности | 107 |
| 10.2.1 | Широковещательный SSID, изоляция станции и режим безопасности | 108 |
| 10.2.2 | Режимы безопасности | 110 |
| 10.2.2.1 | None (Plain-text) (Нет (Простой текст)) | 110 |
| 10.2.2.2 | Static WEP (Статическое WEP-шифрование) | 111 |
| 10.2.2.3 | IEEE 802.1x | 116 |
| 10.2.2.4 | WPA Personal | 119 |

| | |
|---|-----|
| 10.2.2.5 WPA Enterprise | 122 |
| 10.3 Обновление параметров..... | 127 |
| Глава 11: Обслуживание и мониторинг оборудования | |
| 11.1 Интерфейсы | 131 |
| 11.1.1 Параметры проводной сети Ethernet..... | 132 |
| 11.1.2 Параметры беспроводной сети | 132 |
| 11.2 Журналы регистрации событий..... | 132 |
| 11.2.1 Настройка режима «Persistence» (Непрерывный) | 133 |
| 11.2.2 Уровень критичности событий | 134 |
| 11.2.3 Глубина регистрации событий | 135 |
| 11.2.4 Узел ретрансляции журнала событий для сообщений ядра системы..... | 135 |
| 11.2.4.1 Общие сведения о регистрации событий..... | 135 |
| 11.2.4.2 Настройка узла ретрансляции журнала | 136 |
| 11.2.4.3 Включение и отключение узла ретрансляции журнала на экране «Status» (Статус), «Events» (События)..... | 137 |
| 11.2.5 Журнал регистрации событий | 138 |
| 11.3 Статистика передачи и получения данных..... | 139 |
| 11.4 Ассоциированные беспроводные клиенты | 140 |
| 11.4.1 Мониторинг целостности соединения..... | 141 |
| 11.5 Соседние точки доступа..... | 141 |
| Глава 12: Интерфейс Ethernet (проводной) | |
| 12.1 Переход к параметрам Ethernet/проводной сети..... | 149 |
| 12.1.1 Имя хоста DNS..... | 151 |
| 12.1.2 Гостевой доступ..... | 151 |
| 12.1.2.1 Настройка внутренней сети LAN и гостевой сети | 151 |
| 12.1.2.2 Включение и отключение гостевого доступа | 152 |
| 12.1.2.3 Настройка виртуальной гостевой сети | 152 |
| 12.1.3 Виртуальные беспроводные сети..... | 153 |
| 12.1.4 Параметры внутреннего интерфейса | 154 |
| 12.1.5 Параметры гостевого интерфейса | 157 |
| 12.1.6 Обновление параметров | 158 |

Глава 13: Настройка беспроводного интерфейса

| | | |
|------|--|-----|
| 13.1 | Переход к параметрам беспроводной сети..... | 161 |
| 13.2 | Настройка поддержки регулятивного домена 802.11d..... | 162 |
| 13.3 | Управление регулятивным доменом 802.11h | 163 |
| 13.4 | Настройка радиоинтерфейса | 164 |
| 13.5 | Настройка параметров «внутренней» беспроводной сети..... | 166 |
| 13.6 | Настройка параметров «гостевой» беспроводной сети..... | 166 |
| 13.7 | Обновление параметров беспроводной сети..... | 167 |

Глава 14: Настройка гостевого доступа

| | | |
|--------|---|-----|
| 14.1 | Общие сведения о гостевом интерфейсе..... | 171 |
| 14.2 | Настройка гостевого интерфейса | 172 |
| 14.2.1 | Настройка гостевой сети в виртуальной LAN..... | 172 |
| 14.2.2 | Настройка экрана приветствия (каптивный портал) | 173 |
| 14.3 | Клиентский доступ в гостевую сеть | 174 |
| 14.4 | Пример развертывания | 175 |

Глава 15: Настройка VLAN

| | | |
|------|--|-----|
| 15.1 | Переход к параметрам виртуальных беспроводных сетей..... | 179 |
| 15.2 | Настройка VLAN..... | 179 |
| 15.3 | Обновление параметров..... | 182 |

Глава 16: Настройка параметров радиомодуля 802.11

| | | |
|------|--|-----|
| 16.1 | Общие сведения о параметрах радиомодуля..... | 185 |
| 16.2 | Переход к параметрам радиомодуля | 185 |
| 16.3 | Настройка параметров радиомодуля | 187 |
| 16.4 | Обновление параметров..... | 194 |

Глава 17: Фильтрация MAC-адресов

| | | |
|------|---|-----|
| 17.1 | Переход к параметрам фильтрации MAC-адресов | 197 |
| 17.2 | Использование фильтрации MAC-адресов | 198 |
| 17.3 | Обновление параметров..... | 199 |

Глава 18: Балансировка нагрузки

| | | |
|------|---|-----|
| 18.1 | Общие сведения о балансировке нагрузки..... | 203 |
|------|---|-----|

| | | |
|--------|---|-----|
| 18.1.1 | Выявление нарушений баланса. Точки доступа с чрезмерной и недостаточной нагрузкой | 203 |
| 18.1.2 | Настройка ограничений для использования и клиентских соединений | 204 |
| 18.1.3 | Балансировка нагрузки и QoS | 204 |
| 18.2 | Переход к параметрам балансировки нагрузки | 204 |
| 18.3 | Настройка балансировки нагрузки | 205 |
| 18.4 | Обновление параметров | 207 |

Глава 19: Качество обслуживания (QoS)

| | | |
|----------|--|-----|
| 19.1 | Общие сведения о QoS | 211 |
| 19.1.1 | QoS и балансировка нагрузки | 211 |
| 19.1.2 | Поддержка стандартов 802.11e и WMM | 212 |
| 19.1.3 | Очереди QoS и параметры для координирования потоков трафика | 212 |
| 19.1.3.1 | Очереди QoS и типы обслуживания пакетов (ToS) | 213 |
| 19.1.3.2 | EDCF — управление кадрами данных и арбитражными межкадровыми интервалами | 215 |
| 19.1.3.3 | Произвольная задержка и минимальные/максимальные окна коллизии | 216 |
| 19.1.3.4 | Импульсная передача пакетов для повышения производительности | 217 |
| 19.1.3.5 | Интервал потенциальной передачи (TXOP) для клиентских станций | 217 |
| 19.1.4 | 802.1p и теги DSCP | 217 |
| 19.1.4.1 | Приоритет VLAN | 219 |
| 19.1.4.2 | Приоритет DSCP | 220 |
| 19.2 | Настройка очередей QoS | 221 |
| 19.2.1 | Настройка параметров EDCA для точки доступа | 222 |
| 19.2.2 | Включение/отключение поддержки Wi-Fi Multimedia | 225 |
| 19.2.3 | Настройка параметров EDCA для станции | 225 |
| 19.3 | Обновление параметров | 228 |

Глава 20: Распределенная беспроводная система

| | | |
|--------|---|-----|
| 20.1 | Общие сведения о распределенной беспроводной системе | 231 |
| 20.1.1 | Использование WDS для коммутации отдаленных проводных LAN | 231 |
| 20.1.2 | Расширение сети за пределы зоны проводного покрытия с помощью WDS | 232 |

| | | |
|--------|---|-----|
| 20.1.3 | Создание резервных подключений с помощью WDS | 233 |
| 20.2 | Рекомендации по обеспечению безопасности соединений WDS | 233 |
| 20.2.1 | Общие сведения о статическом WEP-шифровании данных | 234 |
| 20.2.2 | Общие сведения о шифровании данных ключом WPA (PSK) | 234 |
| 20.3 | Настройка параметров WDS | 235 |
| 20.3.1 | Пример настройки соединения WDS | 239 |
| 20.4 | Обновление параметров | 240 |

Глава 21: Настройка SNMP

| | | |
|--------|--|-----|
| 21.1 | Общие сведения о параметрах SNMP | 243 |
| 21.2 | Переход к параметрам SNMP | 244 |
| 21.3 | Настройка параметров SNMP | 245 |
| 21.3.1 | Настройка SNMP-ловушек | 248 |
| 21.3.2 | Обновление параметров SNMP | 249 |

Глава 22: 9160 G2 в режиме базовой станции

| | | |
|----------|---|-----|
| 22.1 | Обзор | 253 |
| 22.2 | Протоколы радиосвязи | 254 |
| 22.2.1 | Протокол адаптивного опроса/коллизии | 254 |
| 22.3 | Меню узкополосного радиомодуля | 255 |
| 22.3.1 | Параметры настройки узкополосного радиомодуля | 255 |
| 22.3.1.1 | Параметры радиомодуля RA1001A | 257 |
| 22.3.2 | Параметры подключений | 258 |
| 22.3.3 | Параметры подключений: режим базовой станции | 258 |
| 22.3.3.1 | Параметры протокола опроса | 260 |
| 22.3.3.2 | Параметры радиомодуля | 263 |
| 22.3.4 | Параметры подключений: режим RRM | 264 |
| 22.4 | Меню подключений | 265 |
| 22.4.1 | Параметры настройки базовой станции | 267 |
| 22.4.2 | Параметры настройки групп RRM | 268 |
| 22.4.2.1 | Группы RRM | 270 |
| 22.4.2.2 | Параметры протокола опроса | 271 |
| 22.4.2.3 | Параметры радиомодуля | 273 |
| 22.4.2.4 | Параметры группы | 274 |
| 22.4.2.5 | Удаленные радиомодули | 275 |

| | | |
|----------|---|-----|
| 22.4.3 | Параметры настройки функций радиоканала | 275 |
| 22.4.3.1 | Функции радиоканала | 277 |
| 22.4.3.2 | Автоматическое назначение адреса радиомодуля..... | 278 |
| 22.4.3.3 | Automatic Terminal Number (Автоматическое назначение номера терминала) | 280 |
| 22.4.4 | Меню Hosts (Главные устройства) | 281 |
| 22.4.4.1 | Конфигурация 9010..... | 284 |

Глава 23: Конфигурация мини-контроллера

| | | |
|----------|---|-----|
| 23.1 | Обзор | 287 |
| 23.2 | Меню настройки мини-контроллера | 288 |
| 23.3 | Меню Hosts (Главные устройства) | 288 |
| 23.4 | Параметры меню Host (Главное устройство) | 292 |
| 23.4.1 | Эмуляция 3274 | 292 |
| 23.4.1.1 | Параметры эмуляции | 292 |
| 23.4.1.2 | Параметры TESS..... | 294 |
| 23.4.1.3 | Параметры протокола Telnet..... | 305 |
| 23.4.1.4 | Параметры функциональных клавиш | 309 |
| 23.4.2 | Эмуляция 5250 | 310 |
| 23.4.2.1 | Параметры эмуляции | 310 |
| 23.4.2.2 | Параметры TESS..... | 311 |
| 23.4.2.3 | Параметры протокола Telnet..... | 323 |
| 23.4.2.4 | Параметры функциональных клавиш | 327 |
| 23.4.3 | Эмуляция ANSI | 328 |
| 23.4.3.1 | Параметры эмуляции | 328 |
| 23.4.3.2 | Параметры протокола Telnet..... | 333 |
| 23.4.3.3 | Auto-Telnet/Auto-login (Автоматическое подключение Telnet/Автоматический вход) | 335 |
| 23.4.3.4 | Параметры функциональных клавиш | 340 |

Глава 24: Параметры 802.IQ

| | | |
|--------|--|-----|
| 24.1 | Функции 802.IQ | 343 |
| 24.1.1 | Общие функции протоколов 802.IQ v1/v2..... | 343 |
| 24.1.2 | Функции 802.IQ v1 | 346 |
| 24.1.3 | Меню функций 802.IQ v2..... | 347 |
| 24.2 | Обновление параметров 802.IQ | 347 |

Глава 25: Сетевой протокол синхронизации времени

| | | |
|------|---|-----|
| 25.1 | Переход к параметрам времени | 351 |
| 25.2 | Включение и отключение сервера сетевого протокола синхронизации времени (NTP)..... | 352 |
| 25.3 | Обновление параметров..... | 353 |

Глава 26: Создание резервной копии и восстановление конфигурации

| | | |
|--------|--|-----|
| 26.1 | Переход к параметрам настройки точки доступа | 357 |
| 26.2 | Сброс конфигурации до заводских настроек по умолчанию | 358 |
| 26.3 | Сохранение текущей конфигурации в резервный файл | 358 |
| 26.4 | Восстановление конфигурации из предыдущего сохраненного файла..... | 359 |
| 26.5 | Перезагрузка точки доступа..... | 359 |
| 26.6 | Обновление прошивки | 360 |
| 26.6.1 | Установка обновления | 361 |
| 26.6.2 | Проверка обновления прошивки | 362 |

Глава 27: Технические характеристики

| | | |
|------|--|-----|
| 27.1 | Физические характеристики | 365 |
| 27.2 | Условия эксплуатации | 365 |
| 27.3 | Требования к питанию от источника переменного тока | 365 |
| 27.4 | Требования к питанию через Ethernet..... | 366 |
| 27.5 | Процессор и память | 366 |
| 27.6 | Сетевые интерфейсы | 366 |
| 27.7 | Радиомодули..... | 366 |

Приложение А. Конфигурации портов и схемы кабельных соединений

| | | |
|-----|--|-----|
| A.1 | Консольный порт | A-1 |
| A.2 | Описание последовательных кабелей..... | A-1 |
| A.3 | Выводы разъема RJ-45 (10BaseT/100BaseT Ethernet) | A-3 |

Приложение В. Параметры безопасности на беспроводных клиентах/RADIUS-сервере

| | | |
|-------|---|-----|
| B.1 | Сетевая инфраструктура; выбор между встроенным и внешним сервером аутентификации | B-8 |
| B.1.1 | Использование встроенного сервера аутентификации (EAP-PEAP)..... | B-8 |

| | | |
|--------|--|------|
| B.1.2 | Использование внешнего RADIUS-сервера с сертификатами EAP-TLS или EAP-PEAP | B-9 |
| B.2 | Убедитесь, что у вас установлена последняя версия беспроводного клиентского ПО | B-9 |
| B.3 | Доступ к параметрам безопасности беспроводных клиентов Microsoft Windows.... | B-9 |
| B.4 | Настройка доступа клиента к незащищенной сети (с отключенным режимом безопасности)..... | B-12 |
| B.5 | Настройка статического WEP-шифрования на клиенте | B-14 |
| B.6 | Настройка режима безопасности IEEE 802.1x на клиенте | B-17 |
| B.6.1 | Клиенты с режимом безопасности IEEE 802.1x и протоколом EAP/PEAP | B-17 |
| B.6.2 | Клиенты с режимом безопасности IEEE 802.1x, использующим сертификат EAP/TLS | B-21 |
| B.7 | Настройка режима безопасности WPA/WPA2 Enterprise (RADIUS) на клиенте | B-25 |
| B.7.1 | Клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) с использованием протокола EAP/PEAP | B-25 |
| B.7.2 | Клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) с использованием сертификата EAP-TLS | B-30 |
| B.8 | Настройка режима безопасности WPA/WPA2 Personal (PSK) на клиенте | B-34 |
| B.9 | Настройка внешнего RADIUS-сервера для распознавания 9160 G2 | B-37 |
| B.10 | Получение сертификата TLS-EAP для клиента | B-41 |
| B.11 | Настройка RADIUS-сервера для тегов VLAN..... | B-47 |
| B.11.1 | Настройка RADIUS-сервера..... | B-47 |

Приложение С. Поиск и устранение неисправностей

| | | |
|-------|---|------|
| C.1 | Устранение проблем, связанных с распределенной беспроводной системой (WDS)..... | C-51 |
| C.2 | Восстановление кластера | C-52 |
| C.2.1 | Перезагрузка или сброс настроек точки доступа | C-52 |

Приложение D. Глоссарий

| | |
|-----------------|---|
| Указатель | 1 |
|-----------------|---|

КРАТКИЕ СВЕДЕНИЯ О РАЗРЕШЕНИЯХ И СТАНДАРТАХ БЕЗОПАСНОСТИ

ДЕКЛАРАЦИЯ О СООТВЕТСТВИИ

| | | | |
|---------------------------|---|-------------|--|
| Продукт: | Беспроводной шлюз 9160 G2 Wireless Gateway – RA2050, RA2060 и RA1001A | | |
| Применение | | | |
| Директив Совета ЕС: | Директива ЭМС: | 2004/108/EC | |
| | Директива на | | |
| | низковольтное оборудование: | 2006/95/EC | |
| | Директива RoHS: | 2002/95/EC | |
| | Директива R&TTE: | 1999/5/EEC | |
| Декларация о соответствии | | | |
| стандартам: | EN 55022: класс B | | |
| | EN 61000-3-2; EN 61000-3-3 | | |
| | EN 55024 | | |
| | ETSI EN 300 113-1: V1.6.1 (2006-08) | | |
| | EN 301 893: 2003-08 V1.2.3 | | |
| | EN 300 328: 2004-11 V1.6.1 | | |
| | EN 301 489-1/17: 2004-11 V1.5.1/2002-08 V1.2.1 | | |
| | ETSI EN 301 489-5 V1.3.1 (2002-08) | | |
| | EN 60950-1 | | |
| Производитель: | PSION TEKLOGIX INC. | | |
| | 2100 Meadowvale Blvd. | | |
| | Mississauga, Ontario; Canada L5N 7J9 | | |
| Год выпуска: | 2006 | | |
| Адрес производителя в ЕС: | PSION TEKLOGIX | | |
| | Bourne End Business Centre | | |
| | Cores End Road, Bourne End, SL8 5AR | | |
| | United Kingdom | | |
| Тип оборудования: | Информационное оборудование | | |
| Класс оборудования: | Коммерческое оборудование и оборудование легкой промышленности | | |

Заявление Федеральной комиссии по связи США

ДЕКЛАРАЦИЯ О СООТВЕТСТВИИ ФЕДЕРАЛЬНОЙ КОМИССИИ ПО СВЯЗИ США

| | |
|---|--|
| Имя и адрес заявителя: | PSION TEKLOGIX 2100 Meadowvale Blvd. Mississauga, Ontario; Canada L5N 7J9 Тел.: (905) 813-9900 |
| Представитель в США Имя и адрес: | Psion Teklogix Corp. 1810 Airport Exchange Blvd., Suite 500 Erlanger, Kentucky, 41018, USA Тел.: (859) 372-4329 |
| Тип оборудования/условия эксплуатации: | Вычислительные устройства |
| Торговое наименование/номер модели: | Беспроводной шлюз 9160 G2 Wireless Gateway |
| Год выпуска: | 2005 |

Соответствие заявленным стандартам:

Беспроводной шлюз 9160 G2 Wireless Gateway, поставляемый компанией Psion Teklogix, прошел испытания и был признан соответствующим требованиям в соответствии с **ПОДРАЗДЕЛОМ В РАЗДЕЛА 15 ПРАВИЛ FCC — ИЗЛУЧАТЕЛИ НЕПРЕДНАМЕРЕННЫХ ПОМЕХ, ВЫЧИСЛИТЕЛЬНЫЕ УСТРОЙСТВА КЛАССА В ДЛЯ ДОМАШНЕГО И ОФИСНОГО ИСПОЛЬЗОВАНИЯ.**

| | |
|----------------------------------|---|
| Заявитель: | Psion Teklogix Inc. Mississauga, Ontario, Canada |
| Официальный представитель в США: | Psion Teklogix Corp. Erlanger, Kentucky, USA |

Беспроводной шлюз 9160 G2 Wireless Gateway прошел испытания и был признан соответствующим спецификациям цифровых устройств класса В в соответствии с разделом 15 Правил FCC. Эксплуатация устройства зависит от следующих двух условий.

1. Данное устройство не должно создавать вредных помех; и
2. Данное устройство должно принимать любые помехи, включая помехи, которые могут вызывать сбои в работе.

Данные ограничения предназначены для обеспечения надлежащей защиты от вредных помех при установке в жилых зонах. Данное изделие генерирует, использует и может излучать электромагнитные волны в радиодиапазоне, и, если оно установлено и используется с отклонением от требований инструкций, может стать источником сильных помех для радиосвязи. Однако отсутствие помех в каждой конкретной установке не гарантируется. Если оборудование вызывает помехи теле- и радиоприема, наличие которых определяется путем включения и выключения оборудования, пользователь может попытаться уменьшить влияние помех, выполнив следующие действия:

- Изменить направление или местоположение принимающей антенны.
- Увеличить расстояние между оборудованием или устройствами.
- Подключить оборудование и приемник к разным розеткам.
- Обратиться за помощью к поставщику или техническим специалистам в области радио- и телеаппаратуры.



Важно! Любые изменения или модификации изделия, не одобренные в прямом виде компанией Psion Teklogix, могут привести к лишению прав на эксплуатацию данного устройства.

Заявление о воздействии радиочастотного излучения

Для соответствия нормам FCC и ANSI C95.1 в отношении предельно допустимого воздействия радиочастотного излучения антенны устройства должны соответствовать следующим требованиям:

- Все рабочие антенны точек доступа должны находиться на расстоянии не менее 25 см (9,8 дюймов) от людей, использующих предоставляемый кабель, и не должны быть расположены рядом или эксплуатироваться вместе с любыми другими антеннами или передатчиками.
- Минимальное расстояние для параболической антенны Gabriel (номер по каталогу 9002006) составляет 63,2 см (24,9 дюйма).



Примечание. Двойные антенны, используемые для режима с разнесением по частоте, не считаются используемыми совместно.

Заявление управления связи Министерства промышленности Канады

Это цифровое устройство класса В удовлетворяет требованиям канадских стандартов ICES-003 и RSS-210.

«Данный прибор предназначен для эксплуатации внутри помещения вдали от окон с целью максимального экранирования и предотвращения появления радиопомех для лицензированных услуг. Оборудование (или его передающая антенна), устанавливаемое на улице, подлежит лицензированию».

Cet appareil numérique de la classe B est conforme à la norme NMB-003 et CNR-210 du Canada. «Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé à l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence».

Требования к безопасности

CSA, NRTL/C и CB.

Маркировка CE

Данный продукт и его одобренные в Великобритании и Европе периферийные устройства соответствуют всем требованиям маркировки CE при использовании в жилых помещениях, коммерческих помещениях и легкой промышленности.

Директива R&TTE 1999/5/EC

This equipment complies with the essential requirements of EU Directive 1999/5/EC (Declaration available: www.pSIONteklogix.com).

Cet équipement est conforme aux principales caractéristiques définies dans la Directive européenne RTTE 1999/5/CE. (Déclaration disponible sur le site: www.pSIONteklogix.com).

Die Geräte erfüllen die grundlegenden Anforderungen der RTTE-Richtlinie (1999/5/EG). (Den Wortlaut der Richtlinie finden Sie unter: www.pSIONteklogix.com).

Questa apparecchiatura è conforme ai requisiti essenziali della Direttiva Europea R&TTE 1999/5/CE. (Dichiarazione disponibile sul sito: www.pSIONteklogix.com).

Este equipo cumple los requisitos principales de la Directiva 1995/5/CE de la UE, “Equipos de Terminales de Radio y Telecomunicaciones”. (Declaración disponible en: www.pSIONteklogix.com).

Este equipamento cumpre os requisitos essenciais da Directiva 1999/5/CE do Parlamento Europeu e do Conselho (Directiva RTT). (Declaração disponível no endereço: www.pSIONteklogix.com).

Ο εξοπλισμός αυτός πληροί τις βασικές απαιτήσεις της κοινοτικής οδηγίας EU R&TTE 1999/5/ΕΚ. (Η δήλωση συμμόρφωσης διατίθεται στη διεύθυνση: www.pSIONteklogix.com)

Deze apparatuur voldoet aan de noodzakelijke vereisten van EU-richtlijn betreffende radioapparatuur en telecommunicatie-eindapparatuur 199/5/EG. (verklaring beschikbaar: www.pSIONteklogix.com).

Dette udstyr opfylder de Væsentlige krav i EU's direktiv 1999/5/EC om Radio- og teleterminaludstyr. (Erklæring findes på: www.pSIONteklogix.com).

Dette utstyret er i overensstemmelse med hovedkravene i R&TTE-direktivet (1999/5/EC) fra EU. (Erklæring finnes på: www.pSIONteklogix.com).

Utrustningen uppfyller kraven för EU-direktivet 1999/5/EC om ansluten teleutrustning och ömsesidigt erkännande av utrustningens överensstämmelse (R&TTE). (Förklaringen finns att läsa på: www.pSIONteklogix.com).

Tämä laite vastaa EU:n radio- ja telepäätelaitedirektiivin (EU R&TTE Directive 1999/5/EC) vaatimuksia. (Julkilausuma nähtävillä osoitteessa: www.pSIONteklogix.com).

Psion Teklogix tímto prohlašuje, že 9160 G2 Wireless Gateway je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1995/5/ES (NV č. 426/2000 Sb.) a Prohlášení o shodě je k dispozici na www.pSIONteklogix.com.

Toto zařízení lze provozovat v České republice na základě generální licence č. GL-12/R/2000.

Psion Teklogix týmto vyhlasuje, že 9160 G2 Wireless Gateway spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1995/5/ES (NV č. 443/2001 Z.z.) a Vyhlásenie o zhode je k dispozícii na www.pSIONteklogix.com.

Toto zariadenie je možné prevádzkovať v Slovenskej republike na základe Všeobecného povolenia č. VPR-01/2001.



Правила техники безопасности

Данные инструкции по технике безопасности предназначены для обеспечения защиты пользователей и технического персонала.

- Установка беспроводного шлюза 9160 G2 должна проводиться квалифицированным специалистом компании Psion Teklogix. При неправильной установке беспроводного шлюза 9160 G2 оборудование лишается гарантии производителя.
- Шнур питания (если он продается отдельно) должен соответствовать нормам техники безопасности страны, в которой будет использоваться оборудование.
- Использование комплектующих, не рекомендованных или не продаваемых производителем, может привести к возгоранию, поражению электрическим током или травме.
- Для снижения риска повреждения штепселя или шнура питания отключайте беспроводной шлюз 9160 G2 от сети, потянув за штепсель, а не за шнур.
- Расположите шнур так, чтобы не наступить на него, не запнуться и защитить его от других возможных ударов и воздействий.

- Не пользуйтесь беспроводным шлюзом 9160 G2, если поврежден шнур питания или штепсель. Немедленно замените неисправные детали.
- Не пользуйтесь беспроводным шлюзом 9160 G2, если он подвергся резкому удару, падению или получил другие повреждения. Передайте устройство для осмотра квалифицированным техническим специалистам.
- Не разбирайте беспроводной шлюз 9160 G2. Ремонт устройства должен производиться квалифицированными техническими специалистами. Неправильная сборка устройства может привести к поражению электрическим током или возгоранию.
- Для снижения риска поражения электрическим током при проведении обслуживания или очистки отключите шнур питания беспроводного шлюза 9160 G2 от розетки.
- Использование удлинителя возможно только в случае крайней необходимости. Использование неисправного удлинителя может привести к возгоранию или поражению электрическим током. При использовании удлинителя убедитесь в следующем:
 - Штыри штепсельной вилки удлинителя должны совпадать по количеству, размеру и форме со штырями адаптера.
 - Удлинитель технически должен быть исправен, проводка удлинителя не должна быть повреждена, а калибр провода не должен превышать AWG 16.
- Беспроводной шлюз 9160 G2 предназначен для использования только в помещениях; не подвергайте 9160 G2 воздействию дождя или снега.

Волоконно-оптические характеристики беспроводного шлюза 9160 G2 Wireless Gateway:

СВЕТОДИОДНЫЙ ПРОДУКТ КЛАССА 1
APPAREIL À LED DE CLASSE 1

Не пользуйтесь устройством в условиях взрывоопасной атмосферы

Использование оборудования компании Psion Teklogix в условиях присутствия взрывоопасных газовых смесей может привести к взрыву.

Не открывайте крышку и корпус оборудования

Во избежание несчастных случаев крышка и корпус оборудования могут быть открыты только квалифицированными техническими специалистами. Не пользуйтесь оборудованием с некорректно установленной крышкой или корпусом.

Не прикасайтесь к антенне

Во избежание ощущения дискомфорта вследствие эффекта локального нагрева от излучения радиоволн не дотрагивайтесь до антенны во время передачи данных по беспроводному шлюзу 9160 G2.

Подключение к внешней антенне

Установка внешней антенны должна производиться только техническими специалистами компании Psion Teklogix.

Подача питания через Ethernet и установка внешней антенны



Заземление

Предупреждение. *Перед подключением внешней антенны или питания через Ethernet необходимо присоединить провод заземления.*

1. Необходимо выполнить установку вспомогательного заземляющего провода между беспроводным шлюзом 9160 и подключением к заземлению (в дополнение к заземлению шнура питания).
2. Размер вспомогательного заземляющего провода не должен быть меньше размера незаземленных силовых проводов параллельной цепи (мин. номинальная площадь сечения 0,75 кв. мм или AWG 18). Вспомогательный заземляющий провод должен быть подключен к предоставляемому терминалу беспроводного шлюза 9160 и подключен к заземлению таким образом, чтобы подключение к заземлению оставалось при питании беспроводного шлюза 9160 через Ethernet (POE) или использовании внешних антенн. Подключение к заземлению вспомогательного заземляющего провода должно соответствовать правилам замыкания перемычек в стране использования. Замыкание вспомогательного заземляющего провода может быть сделано на строительную сталь, систему металлических кабельных каналов или любой заземляющий элемент, постоянно и надежно подключенный к заземленному электрооборудованию.
3. Допускается использование неизолированных, изолированных и термоизолированных заземляющих проводов. Концы изолированного или термоизолированного провода заземления должны выступать за пределы изоляционного слоя зеленого цвета или зеленого цвета с одной или несколькими желтыми полосками.
4. Не используйте оборудование во время шторма. Существует риск получения электрического шока от молнии.

ВВЕДЕНИЕ

1

| | |
|---|----|
| 1.1 О руководстве | 3 |
| 1.2 Интерактивная справка, поддерживаемые браузеры и ограничения. | 6 |
| 1.3 Условные обозначения в тексте. | 7 |
| 1.4 Обзор беспроводного шлюза 9160 G2 Wireless Gateway | 8 |
| 1.4.1 Радиомодули | 9 |
| 1.4.2 Функции точки доступа | 10 |
| 1.4.3 Функции базовой станции. | 10 |
| 1.4.4 Функции мини-контроллера | 11 |
| 1.5 Функции и преимущества. | 11 |
| 1.5.1 Поддержка стандартов IEEE и соответствие стандартам Wi-Fi | 11 |
| 1.5.2 Функции беспроводной связи. | 11 |
| 1.5.2.1 Протокол Psion Teklogix 802.IQ | 12 |
| 1.5.3 Функции безопасности | 13 |
| 1.5.4 Встроенный гостевой интерфейс | 14 |
| 1.5.5 Кластеризация и автоматическое управление | 14 |
| 1.5.6 Сеть | 15 |
| 1.5.7 Поддержка SNMP | 15 |
| 1.5.8 Возможности обслуживания | 15 |
| 1.6 Что дальше? | 16 |

1.1 О руководстве

В данном руководстве описаны процессы настройки, конфигурации, администрирования и технического обслуживания одного или нескольких беспроводных шлюзов 9160 G2 Wireless Gateway в беспроводной сети.

Гл. 1: Введение

содержит обзор данного руководства и функций беспроводного шлюза 9160 G2 Wireless Gateway.

Гл. 2: «Требования к установке»

описывает процесс физической установки беспроводного шлюза 9160 G2 Wireless Gateway, а также процесс подключения к 9160 G2 для его диагностики.

Гл. 3: «Подготовка к запуску»

описывает процесс проверки необходимых аппаратных компонентов, программного обеспечения, конфигураций клиента и проблем совместимости.

Гл. 4: «Быстрые действия по настройке и запуску оборудования»

содержит пошаговое руководство по настройке беспроводного шлюза 9160 G2 Wireless Gateway и беспроводной сети, созданной в результате настройки.

Гл. 5: «Настройка базовых параметров»

содержит инструкции по настройке доступа администратора и параметров новой точки доступа.

Гл. 6: «Управление точками доступа и кластерами»

описывает кластеры точек доступа и процесс поиска в кластерах определенной точки доступа.

Гл. 7: «Управление учетными записями пользователей»

демонстрирует возможности системы управления пользователями, предназначенной для контроля клиентского доступа к точкам доступа.

Гл. 8: «Управление каналами»

описывает процесс автоматического назначения беспроводным шлюзом 9160 G2 Wireless Gateway радиоканалов, используемых объединенными в кластер точками доступа, с целью снижения уровня взаимных помех, а также помех, вызываемых другими точками доступа, не входящими в кластер.

Гл. 9: «Беспроводное окружение»

содержит подробную информацию о соседних точках доступа, включая идентифицирующие данные, статус кластера и статистическую информацию.

Гл. 10: «Настройка режимов безопасности»

содержит набор схем аутентификации и шифрования, направленных на обеспечение доступа к беспроводной инфраструктуре только авторизованным пользователям. Дается подробная информация о каждом режиме безопасности.

Гл. 11: «Обслуживание и мониторинг оборудования»

описывает задачи технического обслуживания и мониторинга отдельных точек доступа (не входящих в конфигурацию кластера).

Гл. 12: «Интерфейс Ethernet (проводной)»

описывает процесс настройки проводного интерфейса на беспроводном шлюзе 9160 G2 Wireless Gateway.

Гл. 13: «Настройка беспроводного интерфейса»

описывает процесс настройки беспроводного адреса и установки соответствующих параметров на беспроводном шлюзе 9160 G2 Wireless Gateway.

Гл. 14: «Настройка гостевого доступа»

описывает процесс настройки беспроводного шлюза 9160 G2 Wireless Gateway для контролируемого гостевого доступа к изолированной сети.

Гл. 15: «Настройка VLAN»

описывает процесс настройки нескольких беспроводных сетей в виртуальных LAN (VLAN).

Гл. 16: «Настройка параметров радиомодуля 802.11»

описывает процесс настройки параметров радиомодуля на беспроводном шлюзе 9160 G2 Wireless Gateway.

Гл. 17: «Фильтрация MAC-адресов»

содержит инструкции по использованию фильтра MAC-адресов для контроля клиентского доступа к беспроводной сети.

Гл. 18: «Балансировка нагрузки»

описывает настройку балансировки нагрузки в беспроводной сети, позволяющую сбалансированно распределять соединения беспроводных клиентов на нескольких точках доступа.

Гл. 19: «Качество обслуживания (QoS)»

содержит инструкции по настройке параметров многоканальной системы обслуживания, направленной на увеличение пропускной способности и производительности дифференцированного беспроводного трафика.

Гл. 20: «Распределенная беспроводная система»

описывает процесс настройки системы распределения беспроводных сетей (WDS) на беспроводном шлюзе 9160 G2 Wireless Gateway, с помощью которой можно подключить несколько точек доступа, которые затем будут поддерживать связь друг с другом стандартизированным способом.

Гл. 21: «Настройка SNMP»

описывает процесс настройки SNMP и других соответствующих параметров в API Enterprise-Manager беспроводного шлюза 9160 G2 Wireless Gateway.

Гл. 22: «9160 G2 в режиме базовой станции»

описывает процесс настройки беспроводного шлюза 9160 G2 Wireless Gateway в качестве проводной или беспроводной базовой станции, либо в качестве удаленного радиомодуля (RRM). В этой главе также приводятся параметры настройки узкополосной радиосвязи.

Гл. 23: «Конфигурация мини-контроллера»

описывает процесс настройки беспроводного шлюза 9160 G2 Wireless Gateway при его использовании в качестве мини-контроллера.

Гл. 24: «Параметры 802.IQ»

описывает параметры протокола 802.IQ частной беспроводной сети для базовых станций и мини-контроллеров 9160 G2.

Гл. 25: «Сетевой протокол синхронизации времени»

описывает процесс настройки беспроводного шлюза 9160 G2 Wireless Gateway с целью использования определенного сервера сетевого протокола времени (NTP) для синхронизации часов нескольких компьютеров в сети.

Гл. 26: «Создание резервной копии и восстановление конфигурации»

описывает процесс резервного копирования файла конфигурации, который может быть использован в дальнейшем для восстановления точки доступа до предыдущей сохраненной конфигурации.

Гл. 27: «Технические характеристики»

содержит подробную информацию о физических, эксплуатационных и других рабочих характеристиках беспроводного шлюза 9160 G2 Wireless Gateway и его радиомодулей.

Прил. А: Конфигурации портов и схемы кабельных соединений

содержит сведения о выводах и диаграммы портов и кабелей беспроводного шлюза 9160 G2.

Прил. В: Параметры безопасности на беспроводных клиентах/RADIUS-сервере

содержит подробную информацию о настройке параметров безопасности клиента в соответствии с режимом безопасности, используемым каждым соединением сети (точки доступа).

Прил. С: Поиск и устранение неисправностей

описывает способы решения наиболее распространенных проблем, которые могут возникнуть при обновлении сетевых конфигураций в сетях, обслуживаемых несколькими объединенными в кластер точками доступа.

Прил. D: Глоссарий

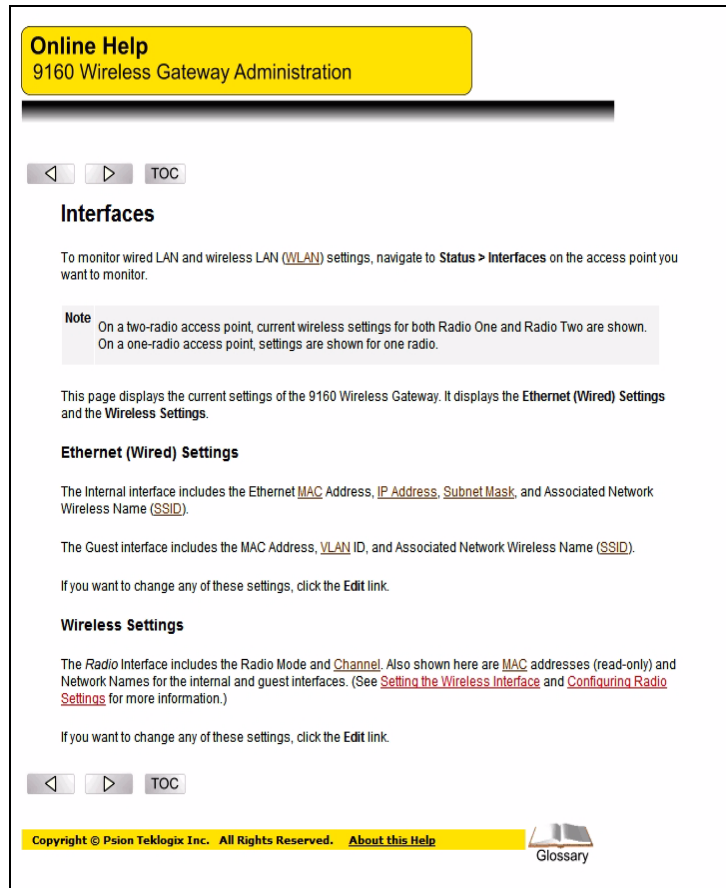
содержит определения и дополнительные сведения о терминах, выделенных полужирным курсивом в данном руководстве.

1.2 Интерактивная справка, поддерживаемые браузеры и ограничения

Интерактивная справка по использованию беспроводного шлюза 9160 G2 Wireless Gateway содержит информацию обо всех полях и функциях, доступных в пользовательском интерфейсе. Информация, представленная в интерактивной справке, входит в состав сведений, содержащихся в полном руководстве пользователя.

Интерактивная справка доступна для каждой вкладки интерфейса администратора беспроводного шлюза 9160 G2 Wireless Gateway. Нажмите кнопку **Help** (Справка) на вкладке или ссылку «More. . .» (Подробнее...) в нижней части панели интерактивной справки в пользовательском интерфейсе, чтобы получить справочную информацию о параметрах текущей вкладки.

Рис. 1.1 Экран интерактивной справки



1.3 Условные обозначения в тексте



Примечание. Примечания содержат дополнительную полезную информацию.



Важно! *Эти утверждения содержат важные инструкции или дополнительную информацию, которая является критически важной для работы компьютеров и другого оборудования.*



Предупреждение. Эти утверждения содержат важную информацию, которая может предотвратить вероятность получения травмы, повреждения оборудования или потери данных.



Стрелка, расположенная рядом с описанием поля (как правило, в таблицах), указывает на рекомендованный параметр настройки для точки доступа (см. *Точка доступа*).

Полужирный курсив

Определения терминов, выделенных *полужирным курсивом*, а также соответствующая дополнительная информация приведена в Прил. D: «Глоссарий». Не все термины, содержащиеся в глоссарии, выделены в руководстве, поэтому рекомендуется обращаться к глоссарию для уточнения определений незнакомых слов и выражений.

1.4 Обзор беспроводного шлюза 9160 G2 Wireless Gateway

Беспроводной шлюз 9160 G2 Wireless Gateway обеспечивает непрерывную высокоскоростную связь между беспроводными устройствами и устройствами Ethernet. Это усовершенствованное стандартизированное решение беспроводных сетей для предприятий малого и среднего бизнеса. Беспроводной шлюз 9160 G2 Wireless Gateway позволяет развернуть беспроводную локальную сеть (*WLAN*), не требующую администрирования и обладающую самыми современными функциями беспроводной сети.

Беспроводной шлюз 9160 G2 Wireless Gateway обеспечивает наивысший уровень безопасности, простоты администрирования и соответствия отраслевым стандартам, позволяя создавать автономную и полностью защищенную беспроводную сеть, которая не нуждается в дополнительном управлении и установке программного обеспечения сервера безопасности.

Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает широкий спектр системных конфигураций. Используя стандарты беспроводной сети IEEE 802.11, беспроводной шлюз 9160 G2 может выполнять функции «прозрачного моста» (точки доступа) между беспроводными и проводными сетями. Благодаря этому беспроводные клиенты получают доступ к сети и возможность плавного переключения в сети от одного беспроводного шлюза 9160 G2 к другому. Беспроводной шлюз 9160 G2 может использоваться в качестве мини-контроллера, базовой станции или удаленного радиомодуля (RRM), а также в составе системы *mapRF*.

1.4.1 Радиомодули

Беспроводной шлюз 9160 G2 может работать с одним или двумя радиомодулями. Доступные радиомодули: 802.11a/g, 802.11g и узкополосный радиомодуль RA1001A. Дополнительные технические характеристики этих радиомодулей приведены в разделе «Радиомодули» на стр. 366.

В зависимости от установленных радиомодулей используются следующие режимы работы точки доступа:

- Режим IEEE **802.11b**.
- Режим IEEE **802.11g**.
- Режим IEEE **802.11a**.
- Atheros Turbo 5 ГГц.
- Atheros Dynamic Turbo 5 ГГц.
- Atheros Turbo 2,4 ГГц.
- Atheros Dynamic Turbo 2,4 ГГц.
- Расширенный диапазон.
- Узкополосный протокол опроса Psion Teklogix.



Важно! Мобильные компьютеры Psion Teklogix не поддерживают режимы Atheros Turbo, поэтому в целях предотвращения передачи ненужных радиосигналов использовать режим Turbo не рекомендуется.

Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает четыре конфигурации радиомодулей: 802.11g, 802.11g + 802.11ag, NB (узкополосный) и NB + 802.11ag.

Вариант конфигурации определяется значением «Model» (Модель), отображаемым на веб-странице *Maintenance (Обслуживание) > Upgrade (Обновить)* (см. Рис. 1.2 на стр. 10). Модели определяются следующим образом:

- 9160 Wireless Gateway = 802.11g.
- 9160 Wireless Gateway (Dual Radio) = 802.11g + 802.11ag.
- 9160 Wireless Gateway NB = NB.
- 9160 Wireless Gateway NB (Dual Radio) = NB + 802.11ag.



Примечание. При использовании одного узкополосного радиомодуля («NB only») на веб-странице может отображаться экран настройки для одного радиомодуля 802.11. Это значение можно не изменять, однако попытка настройки этого несуществующего радиомодуля не отразится на работе беспроводного шлюза 9160 G2.

Рис. 1.2 Веб-страница Upgrade Firmware (Обновить прошивку)

Upgrade firmware

| | |
|------------------|---------------------------------------|
| Model | 9160 Wireless Gateway NB (Dual Radio) |
| Platform | PTX9160G2 |
| Firmware Version | E187k |

New Firmware Image [Browse...](#)

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

[Upgrade](#)

1.4.2 Функции точки доступа

При работе в качестве точки доступа, подключенной к проводной сети, беспроводной шлюз 9160 G2 Wireless Gateway создает канал связи между мобильными компьютерами Psion Teklogix RF или клиентами беспроводной точки доступа и сетевым контроллером Psion Teklogix или главным компьютером. Связь с мобильными компьютерами осуществляется по радиоканалу передачи данных IEEE 802.11, а связь с сетевым контроллером или главным компьютером — по кабелю. Беспроводной шлюз 9160 G2 можно подключить к сети через Ethernet.

1.4.3 Функции базовой станции

При работе в качестве базовой станции или удаленного радиомодуля (RRM) беспроводной шлюз 9160 G2 устанавливает связь между локальной сетью и беспроводными мобильными компьютерами, используя частные протоколы радиосвязи Psion Teklogix. В локальной сети базовая станция (или RRM) 9160 G2 взаимодействует с сервером связи 9500 (или главным устройством, использующим комплект для разработки ПО Psion Teklogix Software Development Kit) с помощью частного протокола 9010 через TCP/IP.

Для получения информации о настройке беспроводного шлюза 9160 G2 для работы в качестве базовой станции или RRM см. Гл. 22: «9160 G2 в режиме базовой станции».

1.4.4 Функции мини-контроллера

Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает функции эмуляции, что позволяет использовать его в качестве мини-контроллера. Если устройство 9160 G2 настроено для работы в качестве мини-контроллера, мобильные компьютеры Psion Teklogix могут эмулировать мобильные компьютеры ANSI, 5250 или 3274, используя устройство 9160 G2 вместо сервера связи 9500.

Для получения информации о настройке беспроводного шлюза 9160 G2 Wireless Gateway для работы в качестве мини-контроллера см. Гл. 23: «Конфигурация мини-контроллера».

1.5 Функции и преимущества

1.5.1 Поддержка стандартов IEEE и соответствие стандартам Wi-Fi

- Поддержка беспроводных сетевых стандартов *IEEE 802.11a*, *IEEE 802.11b*, *IEEE 802.11g*, *IEEE 802.11i* и *IEEE 802.3af*.
- Полоса пропускания до 54 Мбит/с для *IEEE 802.11a* и *IEEE 802.11g* (11 Мбит/с для *IEEE 802.11b*, 108 Мбит/с для *Atheros 802.11a Turbo*).
- Соответствие стандартам Wi-Fi необходимо для сертификации.

1.5.2 Функции беспроводной связи

- Автоматический выбор канала при запуске.
- Регулировка мощности передачи.
- Система распределения беспроводных сетей (*WDS*) для беспроводного подключения нескольких точек доступа. Расширение сети с меньшим количеством кабелей.
- Уровень качества обслуживания (*QoS*), обеспечивающий более высокую пропускную способность и улучшенную производительность при передаче времязависимого беспроводного трафика: видео- и аудиозаписей, мультимедийных потоков, а также голоса по протоколу IP (VoIP). QoS соответствует стандартам Wi-Fi Multimedia (WMM).
- Балансировка нагрузки.
- Встроенная поддержка множественных *SSID* (сетевых имен) и *BSSID* (идентификаторов основного набора служб) на одной точке доступа. Поддержка двух специализированных идентификаторов BSSID — один для внутренней сети (основной сети и сети управления), другой для гостевой сети. Поддержка шести дополнительных идентификаторов BSSID общего назначения (так называемых виртуальных беспроводных сетей, или VWN) с использованием VLAN.

- Управление каналами для автоматической координации назначений радиоканалов с целью снижения помех между точками доступа в сети и максимального увеличения полосы пропускания Wi-Fi.
- Обнаружение соседних точек доступа (так называемых «мошеннических» точек доступа).
- Поддержка выбора регулятивного домена **IEEE 802.11d** (кодов страны для глобальных операций).
- Поддержка **IEEE 802.11h**, включая TPC и DFS.
Стандарт IEEE 802.11h включает две службы, необходимые для использования определенных регулятивных доменов на частоте 5 ГГц. Это служба управления мощностью передачи (TPC) и служба поддержки динамического выбора частоты (DFS).
- Поддержка расширенного диапазона (XR).
- Определение приоритетов голосовых данных SpectraLink (SVP).
Определение приоритетов голосовых данных SpectraLink (SVP) — это одна из методик QoS для развертывания сетей Wi-Fi. SVP является открытой спецификацией, соответствующей стандарту IEEE 802.11b. SVP сокращает время задержки передачи голосовых пакетов, повышая их приоритет по сравнению с пакетами данных в беспроводной сети, тем самым увеличивая потенциальную производительность сети.

1.5.2.1 Протокол Psion Teklogix 802.IQ

Протокол 802.IQ — это частный протокол Psion Teklogix, позволяющий мобильным компьютерам работать в беспроводной сети, поддерживающей одновременное использование протоколов TCP/IP и 802.IQ. Доступны две версии протокола 802.IQ: 802.IQ v1 и 802.IQ v2. Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает одновременное использование обеих версий протокола (мобильные компьютеры должны использовать только одну версию).

Протокол 802.IQ v1 представляет собой схему маршрутизации беспроводной сети, обеспечивающей большую производительность беспроводной сети 802.11 по сравнению с маршрутизацией через TCP/IP. Мобильный компьютер может взаимодействовать с точкой доступа 9160 G2 по протоколу TCP/IP или 802.IQ v1, реализуя систему с двойной функциональностью.

Протокол 802.IQ v2 является расширенной версией протокола 802.IQ v1, обеспечивающей передачу пакетов на уровне UDP. Он поддерживает все возможности протокола 802.IQ v1, функции обновления программного обеспечения по радиоканалу, возможность добавления сторонних точек доступа между контроллерами и мобильными компьютерами, а также интеграцию в систему MapRF (при необходимости).

Для получения дополнительной информации и ознакомления с меню настройки протокола 802.IQ см. Гл. 24: «Параметры 802.IQ».

1.5.3 Функции безопасности

- Блокировка передачи SSID.
- Игнорирование передачи SSID.
- Предотвращение слабых IV.
- Поддержка алгоритма Wireless Equivalent Privacy (*WEP*).
- Сертификация Wi-Fi для следующих стандартов:
 - Стандарты IEEE: 802.11b, 802.11g, 802.11d
 - Безопасность:
 - WPA™ - Personal
 - WPA™ - Enterprise
 - WPA2™ - Personal
 - WPA2™ - Enterprise
 - Типы EAP:
 - EAP-TLS
 - EAP-TTLS/MSCHAPv2
 - PEAPv0/EAP-MSCHAPv2
 - PEAPv1/EAP-GTC
 - EAP-SIM
- Поддержка усовершенствованного стандарта шифрования (*AES*).
- Ориентированный на пользователя контроль доступа с помощью сервера локальной аутентификации.
- Управление локальной базой данных пользователей и жизненным циклом пользователей.
- Фильтрация MAC-адресов.
- WPA/WPA2 через *WDS*.
- Поддержка протокола Secure Sockets Shell (SSH).
- Поддержка протокола Secure Sockets Layer (SSL).

1.5.4 Встроенный гостевой интерфейс

- Уникальное сетевое имя (**SSID**) для гостевого интерфейса.
- Каптивный портал для перехода гостей на настраиваемые веб-страницы, предназначенные только для гостевого доступа.
- Опции VLAN и Ethernet.

1.5.5 Кластеризация и автоматическое управление

- Подготовка и автоматическая конфигурация точек доступа через кластеризацию и взаимодействие кластеров.

Администратор может указать, как должны быть настроены новые точки доступа до их добавления к сети. При добавлении новых точек доступа они могут автоматически взаимодействовать с кластером и безопасно загружать правильную конфигурацию. Этот процесс не требует вмешательства пользователя, но находится под контролем администратора.

- Просмотр объединенных в кластер точек доступа и параметров настройки кластера в одном окне.

Настройкой всех точек доступа в кластере можно управлять в одном интерфейсе. Изменения общих параметров автоматически применяются ко всем членам кластера.

- Самоуправляемые точки доступа с автоматической синхронизацией настройки.

Точки доступа в кластере периодически проверяют целостность конфигурации кластера, а также присутствие и доступность других членов кластера. Администратор может выполнять мониторинг этой информации посредством пользовательского интерфейса.

- Усовершенствованный процесс локальной аутентификации с использованием протокола 802.1x без дополнительной настройки.

Кластер может обслуживать сервер аутентификации пользователей и базу данных, сохраненную в точках доступа. Это избавляет вас от необходимости устанавливать, настраивать и поддерживать инфраструктуру **RADIUS**, а также упрощает административную задачу по развертыванию безопасной беспроводной сети.

1.5.6 Сеть

- Протокол динамического конфигурирования хоста (**DHCP**) обеспечивает поддержку динамического получения информации о конфигурации сети.
- Поддержка виртуальной локальной сети (VLAN).
- Поддержка виртуальных беспроводных сетей (динамических VLAN).
- Протокол связующего дерева (**STP**).
- **802.1p**.
- Поддержка 100Base-FX с использованием волоконно-оптического кабеля.

1.5.7 Поддержка SNMP

Беспроводной шлюз 9160 G2 Wireless Gateway включает следующие стандартные информационные базы управления (**MIB**), связанные с простым протоколом сетевого управления (**SNMP**):

- Bridge MIB 802.1d (RFC 1493).
- MIB SNMPv2 (RFC 3418).
- MIB стандарта IEEE 802.11 (база).
- MIB группы интерфейсов (RFC 2233).
- Две частных MIB (беспроводная и системная) на основе будущей MIB IEEE 802.11k. Они предоставляют информацию об ассоциативном списке и таблице обнаружения точек доступа клиента беспроводного шлюза 9160 G2 Wireless Gateway соответственно. Частная системная MIB обеспечивает функции технического обслуживания, такие как перезагрузка системы или обновление прошивки.

1.5.8 Возможности обслуживания

- Просмотр статуса, событий мониторинга и отслеживания сети, в том числе мониторинга сеансов, ассоциаций клиента, статистику приема и передачи данных, а также журнала событий.
- Мониторинг целостности соединения с целью постоянной проверки соединения с клиентом, вне зависимости от уровней активности сетевого трафика.
- Возможность сброса конфигурации.
- Обновление прошивки.
- Резервное копирование и восстановление конфигурации точки доступа.

- Резервное копирование и восстановление базы данных пользователей для встроенного RADIUS-сервера (для режимов безопасности IEEE 802.1x и WPA/WPA2 Enterprise (RADIUS)).

1.6 Что дальше?

Готовы приступить к созданию беспроводной сети? После установки беспроводного шлюза 9160 G2 Wireless Gateway (см. Гл. 2: «Требования к установке») ознакомьтесь с Гл. 3: «Подготовка к запуску», а затем выполните действия, описанные в Гл. 4: «Быстрые действия по настройке и запуску оборудования».

ТРЕБОВАНИЯ К УСТАНОВКЕ

2

| | |
|---|----|
| 2.1 Выбор местоположения | 19 |
| 2.1.1 Условия эксплуатации | 19 |
| 2.1.2 Обслуживание | 20 |
| 2.1.3 Радиомодули | 20 |
| 2.1.4 Кабели питания и антенны | 21 |
| 2.1.4.1 Питание | 21 |
| 2.1.4.2 Антенны | 21 |
| 2.2 Подключение к внешним устройствам. | 23 |
| 2.2.1 Порты | 23 |
| 2.2.2 Установка LAN: обзор | 24 |
| 2.2.3 Установка LAN: Ethernet | 24 |
| 2.2.3.1 Кабель Ethernet | 24 |
| 2.2.3.2 Волоконно-оптический порт Ethernet 100Base-FX | 25 |
| 2.2.4 Индикаторы статуса (LED) | 25 |
| 2.2.5 Подключение видеотерминала | 26 |
| 2.3 Изменение конфигурации с помощью веб-браузера | 26 |



Предупреждение. Установка беспроводного шлюза 9160 G2 должна проводиться квалифицированным специалистом компании Psion Teklogix.

2.1 Выбор местоположения

Как правило, специалисты Psion Teklogix производят осмотр помещения и дают рекомендации по предпочтительному месту установки беспроводного шлюза 9160 G2. Подходящие места установки обеспечивают хорошую зону радиопокрытия, находятся на минимальном расстоянии от главного компьютера или сетевого контроллера и отвечают эксплуатационным требованиям.

2.1.1 Условия эксплуатации

Беспроводной шлюз 9160 G2 должен быть установлен в хорошо проветриваемом помещении и должен быть защищен от воздействия экстремальных температур (т.е. вдали от приборов нагревания воздуха, дверей и открытых солнечных лучей). Если необходимо использовать защитное покрытие, оно должно обеспечивать достаточное поступление воздуха для обеспечения нормальной работы устройства.

Для получения дополнительной информации о требованиях к охране окружающей среды см. Гл. 27: «Технические характеристики». Помните, что долговременная стабильная работа оборудования будет обеспечена при поддержании менее суровых внешних условий по сравнению с условиями, приведенными в данном руководстве.

Беспроводной шлюз 9160 G2 должен находиться вдали от дорожных магистралей и источников распыления воды и пыли. Беспроводной шлюз 9160 G2 должен устанавливаться в строго вертикальном положении, как показано на Рис. 2.1 на стр. 20. При таком положении снижается риск попадания воды в беспроводной шлюз 9160 G2 при случайном ее распылении.

Беспроводной шлюз 9160 G2 крепится к вертикальной поверхности с помощью четырех крепежных деталей на задней крышке (тип крепежных деталей зависит от монтажной поверхности). Два верхних отверстия на задней крышке — это пазы, на которых устройство крепится до установки других болтов, облегчая процесс монтажа. Для установки используются болты SAE 1/4-20.

Рис. 2.1 Позиция установки беспроводного шлюза 9160 G2



2.1.2 Обслуживание

Беспроводной шлюз 9160 G2 не имеет внутреннего переключателя режимов и не требует физического доступа; все параметры настраиваются удаленно (см. «Переход к базовым параметрам» на стр. 51). Тем не менее, необходимо соблюдать все требования к охране окружающей среды и регламенты радиосвязи.

2.1.3 Радиомодули

- Радиомодуль 802.11g без интегрированной антенны (стандарт).
- Радиомодуль 802.11a/g без интегрированной антенны (дополнительный радиомодуль).
- Узкополосный радиомодуль RA1001A.

2.1.4 Кабели питания и антенны

2.1.4.1 Питание

Для предотвращения случайного отключения или механического воздействия на беспроводной шлюз 9160 G2, кабели антенны и питания должны быть закреплены на протяжении 30 см от устройства. Прикрепите кабели стяжкой к креплению кабельной стяжки на беспроводном шлюзе 9160 G2 (см. Рис. 2.1). Однофазная розетка питания (от 100 до 240 В переменного тока, минимум 1 А) должна быть установлена на расстоянии не более 1 метра от беспроводного шлюза 9160 G2. Беспроводной шлюз 9160 G2 автоматически настраивается в рамках этого диапазона мощности. Кабель питания является съемным и доступен для местного вида электропитания. Источник питания переменного тока беспроводного шлюза 9160 G2 имеет универсальный вход через стандартный разъем IEC320.

Чтобы исключить необходимость монтажа электропроводки переменного тока, беспроводной шлюз 9160 G2 Wireless Gateway совместим со стандартом IEEE 802.3af и может питаться через подключение Ethernet. Для получения дополнительной информации см. «Требования к питанию через Ethernet» на стр. 366.



Предупреждение. Во избежание риска электрического шока провод защитного заземления шнура питания всегда должен быть подключен к заземлению.

2.1.4.2 Антенны

Тип антенны для каждой установки зависит от требований к зоне покрытия и используемым частотам. Можно использовать не более четырех антенных элементов. Это может быть комбинацией разнесенных антенн или антенн с высоким усилением WDS. Компания Psion Teklogix предлагает несколько ненаправленных антенн и специальных, направленных антенн. Как правило, тип антенны определяется при осмотре помещения. Для получения дополнительной информации обратитесь к техническому персоналу компании Psion Teklogix.



Предупреждение. Не используйте беспроводной шлюз 9160 G2 без подходящей антенны или с эквивалентом антенны.

Подключение к внешней антенне (№ комплекта по каталогу: 1916641)

Антенна должна быть установлена квалифицированным специалистом в соответствии с местными электротехническими нормами. Антенна должна быть установлена таким образом, чтобы она всегда была на высоте как минимум 4,6 м и на расстоянии 3 м от пользователя и других людей, работающих в данном месте.

При подключении 9160 G2 к внешней антенне соблюдайте следующие правила:

1. Щиток коаксиального кабеля внешней антенны должен быть заземлен (независимо от 9160 G2) при монтаже на здании, если монтаж разрешен в стране использования.
2. Необходимо выполнить установку вспомогательного заземляющего провода между беспроводным шлюзом 9160 G2 и заземлением, в дополнение к проводу заземления в шнуре питания.
3. Размер вспомогательного заземляющего провода не должен быть меньше размера незаземленных силовых проводов параллельной цепи (мин. номинальная площадь сечения 0,75 кв. мм или AWG 18). Вспомогательный заземляющий провод должен быть подключен к предоставляемому терминалу беспроводного шлюза 9160 G2 и подключен к заземлению таким образом, чтобы при отключении шнура питания оставалось соединение с заземлением. Подключение к заземлению вспомогательного заземляющего провода должно соответствовать правилам замыкания перемычек в стране использования. Замыкание вспомогательного заземляющего провода может быть сделано на строительную сталь, систему металлических кабельных каналов или любой заземляющий элемент, постоянно и надежно подключенный к заземленному электрооборудованию.
4. Допускается использование неизолированных, изолированных и термоизолированных заземляющих проводов. Концы изолированного или термоизолированного провода заземления должны выступать за пределы изоляционного слоя зеленого цвета (только для Канады и США) или зеленого цвета с одной или несколькими желтыми полосками (для других стран).
5. Не используйте оборудование во время шторма. Существует риск получения электрического шока от молнии.
6. В Финляндии, Норвегии и Швеции оборудование должно использоваться в ПОМЕЩЕНИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ в условиях уравнивания потенциалов. Постоянно подключенный ПРОВОД ЗАЩИТНОГО ЗАЗЕМЛЕНИЯ должен быть установлен ТЕХНИЧЕСКИМ СПЕЦИАЛИСТОМ.



Предупреждение. Для обеспечения безопасности радиочастот, пользователям запрещено приближаться к антеннам.

Компания Psion Teklogix поставляет коаксиальный кабель, необходимый для подключения беспроводного шлюза 9160 G2 к антенне. При определении местоположения для антенны необходимо учитывать требования к зоне покрытия, а также требования к охране окружающей среды для беспроводного шлюза 9160 G2.

Коаксиальный кабель должен быть маршрутизирован и закреплен с помощью анкеров и/или клипс для крепления (коаксиального) кабеля. Необходимо оставить несколько сантиметров кабеля около антенны и беспроводного шлюза 9160 G2 для простоты отключения.

2.2 Подключение к внешним устройствам

В данном разделе содержатся общие руководства по подключению беспроводного шлюза 9160 G2 к внешним устройствам, таким как сетевые контроллеры, базовые станции, главные компьютеры, персональные компьютеры и видеотерминалы.

2.2.1 Порты

Рис. 2.2 на стр. 23 показывает местоположение порта и разъема питания на базе 9160 G2. Конфигурации портов описаны в Прил. А: «Конфигурации портов и схемы кабельных соединений».

Рис. 2.2 Порты и светодиодные индикаторы 9160 G2



** Примечание. Более ранние версии беспроводного шлюза 9160 G2 не имеют волоконно-оптического порта.*

2.2.2 Установка LAN: обзор

Благодаря тому, что беспроводной шлюз 9160 G2 предоставляет связь Ethernet, его можно добавить к существующей локальной сети. Как правило, установка локальной сети производится с помощью сетевого администратора, так как они знакомы с сетью и ее конфигурацией. После установки, подключения и включения беспроводного шлюза 9160 G2 системный администратор может войти в систему устройства для проверки конфигурации и назначения шлюзу 9160 G2 уникального IP-адреса. Это можно сделать через сеть (см. «Изменение конфигурации с помощью веб-браузера» на стр. 26). Последующие изменения в сети, такие как добавление станций или пользователей, также требуют изменений конфигурации беспроводного шлюза 9160 G2.



Важно! После первой настройки и перезагрузки беспроводного шлюза 9160 G2 следует отключить DHCP, если 9160 G2 не получает IP-адрес от сервера.

2.2.3 Установка LAN: Ethernet

Беспроводной шлюз 9160 G2 — это высокопроизводительная точка доступа, которая поддерживает высокоскоростные локальные сети Ethernet со скоростью 100 Мбит/с и 10 Мбит/с, в полнодуплексном и полудуплексном режиме работы. Он оборудован следующими компонентами:

- Карта 10BaseT/100BaseT с использованием витой пары категории 5, разъема RJ-45, работающая на скорости 10 или 100 Мбит/с. Для получения информации о конфигурации портов см. Прил. А: «Конфигурации портов и схемы кабельных соединений».
- Волоконно-оптический порт 100Base-FX (для получения подробной информации см. Разд. 2.2.3.2).



Примечание. Беспроводной шлюз 9160 G2 поддерживает только следующие типы подключения: Ethernet 10BaseT, 100BaseT и 100Base-FX.

2.2.3.1 Кабель Ethernet

Максимальная длина кабельного сегмента между ретрансляторами для 9160 G2 (кабель Ethernet 10BaseT/100BaseT) должна составлять 100 м.

2.2.3.2 Волоконно-оптический порт Ethernet 100Base-FX

Беспроводной шлюз 9160 G2 Wireless Gateway обеспечивает поддержку волоконно-оптической сети 100Base-FX. Для использования волоконно-оптического порта Ethernet пользователь должен установить модуль 100Base-FX Small Form Pluggable (SFP) в порт волоконно-оптического расширения беспроводного шлюза 9160 G2. SFP — это компактные оптические модульные приемопередатчики, обеспечивающие высокую скорость передачи данных.

После установки оборудования функция активируется. Настройка порта не требуется — ПО беспроводного шлюза 9160 G2 автоматически обнаруживает SFP-модуль при запуске и использует его вместо стандартного порта 10/100BaseT.

Модуль вставляется в электрический интерфейс нажатием пальца. SFP-модуль не поддерживает замену в «горячем» режиме. Вставляйте и удаляйте модуль только при выключенном беспроводном шлюзе 9160 G2.

При запуске беспроводной шлюз 9160 G2 напечатает одно из следующих сообщений на последовательном консольном порте, в зависимости от того, установлен ли SFP-модуль:

ixp425_eth: 100BASE-FX SFP fiber module detected (ixp425_eth: обнаружен SFP-модуль 100BASE-FX)

ixp425_eth: 100BASE-FX SFP fiber module not detected (ixp425_eth: SFP-модуль 100BASE-FX не обнаружен)

При использовании волоконно-оптического интерфейса беспроводной шлюз 9160 G2 работает только на скорости 100 Мбит/с. Вне зависимости от того, какой используется порт Ethernet, 9160 G2 использует один и тот же проводной MAC-адрес.

Одновременная работа обоих портов Ethernet не поддерживается. Поддерживается использование PoE (через порт 10/100BaseT) и волоконно-оптического интерфейса. В данной конфигурации порт 10/100BaseT используется только для питания.

2.2.4 Индикаторы статуса (LED)

Высокопроизводительный беспроводной шлюз 9160 G2 имеет шесть индикаторов статуса на передней панели корпуса (см. Рис. 2.2 на стр. 23). Пронумерованные цветные светодиодные индикаторы на передней панели устройства показывают статус работы каждого порта (см. описание в Табл. 2.1 на стр. 26).

Табл. 2.1 Функции светодиодных индикаторов на передней панели 9160 G2

| № индикатора | Название | Функция | Цвет |
|--------------|-----------------------------------|--|---------|
| 1 | Связь Ethernet | Индикатор связи для 10BaseT/100BaseT: Горит = хорошая связь; не горит = нет связи | желтый* |
| 2 | Работа Ethernet | Работа локальной сети Ethernet (Rx/Tx) | зеленый |
| 3 | Статус первого радиомодуля 802.11 | Работа первого радиомодуля 802.11 (Rx/Tx) | зеленый |
| 4 | Статус второго радиомодуля 802.11 | Работа второго радиомодуля 802.11 (Rx/Tx) | зеленый |
| 5 | Статус узкополосного радиомодуля | Работа узкополосного радиомодуля (Rx/Tx) | зеленый |
| 6 | Питание | Индикатор горит = питание включено Индикатор не горит = питание отключено | зеленый |

* Цвет светодиодного индикатора 1 показывает ориентацию индикаторов при взгляде издалека.

2.2.5 Подключение видеотерминала

Видеотерминал ANSI (например, DEC VT220 или выше) или компьютерная эмуляция терминала используется для диагностики.

Терминал подключается к порту RS-232 на беспроводном шлюзе 9160 G2 (см. Рис. 2.2.2 на стр. 24). Обычно этот порт используется для работы со следующими параметрами: 115200 бод, 8 бит, 1 стоп-бит, без бита четности. В целях соответствия разделом 15 Правил FCC для вычислительных устройств класса В должен использоваться только поставляемый кабель (№ по каталогу 19387).

2.3 Изменение конфигурации с помощью веб-браузера

Конфигурацию флэш-памяти беспроводного шлюза 9160 G2 можно изменить удаленно, используя стандартный веб-браузер HTML, например MS Internet Explorer (версия 4.0 или более поздняя) или Firefox. См. Гл. 4: «Быстрые действия по настройке и запуску оборудования» для ознакомления с инструкциями по изменению параметров и общих настроек.

| | |
|--|----|
| 3.1 Беспроводной шлюз 9160 G2 Wireless Gateway | 29 |
| 3.1.1 Значения по умолчанию беспроводного шлюза 9160 G2 Wireless Gateway | 29 |
| 3.1.2 Функции, которые не поддерживаются точками доступа | 33 |
| 3.2 Компьютер администратора | 33 |
| 3.3 Компьютеры беспроводного клиента | 35 |
| 3.4 Общие сведения о динамической и статической IP-адресации на беспроводном шлюзе 9160 G2 Wireless Gateway | 36 |
| 3.4.1 Как точка доступа получает IP-адрес при запуске? | 36 |
| 3.4.2 Динамическая IP-адресация | 37 |
| 3.4.3 Статическая IP-адресация | 37 |
| 3.4.4 Восстановление IP-адреса | 38 |

Перед подключением и загрузкой новой точки доступа (см. *Точка доступа*) ознакомьтесь с данным разделом и убедитесь в наличии требуемых аппаратных компонентов, программного обеспечения, конфигураций клиентов и отсутствии проблем совместимости. Подготовьте все необходимое для успешного запуска и тестирования новой (или расширенной) беспроводной сети.

3.1 Беспроводной шлюз 9160 G2 Wireless Gateway

Беспроводной шлюз 9160 G2 Wireless Gateway — это беспроводной узел связи для устройств вашей сети. Он обеспечивает непрерывную высокоскоростную связь между беспроводными устройствами и устройствами Ethernet в режимах *IEEE 802.11a*, *802.11b*, *802.11g* и *802.11a Turbo*.

Беспроводной шлюз 9160 G2 Wireless Gateway снабжен встроенной функцией *гостевого интерфейса*, с помощью которой можно настраивать точки доступа для контролируемого гостевого пользования беспроводной сетью через виртуальные локальные сети.

Для получения дополнительной информации о гостевом интерфейсе см. Гл. 14: «Настройка гостевого доступа» и «Примечание о настройке подключений для гостевой сети» на стр. 44.

3.1.1 Значения по умолчанию беспроводного шлюза 9160 G2 Wireless Gateway

Табл. 3.1 Значения по умолчанию 9160 G2

| Параметр | Значения по умолчанию | Дополнительная информация |
|--|--|---|
| <i>System Name</i> (Системное имя) | PTX9160-Wireless-AP | «Имя хоста DNS» на стр. 151 в разделе «Интерфейс Ethernet (проводной)» на стр. 147 |
| <i>User Name</i> (Имя пользователя) | admin Имя пользователя доступно только для чтения. Его нельзя изменить. | |
| <i>Password</i> (Пароль) | admin | «Настройка сетевых параметров» на стр. 53 в разделе «Настройка базовых параметров» на стр. 49 |

Табл. 3.1 Значения по умолчанию 9160 G2 (Продолжение)

| Параметр | Значения по умолчанию | Дополнительная информация |
|---|--|---|
| <i>Network Name (SSID)</i> <i>(Сетевое имя (SSID))</i> | «TEKLOGIX» для внутреннего интерфейса «TEKLOGIX Guest» для гостевого интерфейса | «Обзор и описание точки доступа» на стр. 52 в разделе «Настройка базовых параметров» на стр. 49 «Настройка параметров «внутренней» беспроводной сети» на стр. 166 в разделе «Настройка беспроводного интерфейса» на стр. 159 «Настройка параметров «гостевой» беспроводной сети» на стр. 166 в разделе «Настройка беспроводного интерфейса» на стр. 159 |
| <i>Network Time Protocol (NTP)</i> <i>(Сетевой протокол синхронизации времени)</i> | None (Нет) | «Сетевой протокол синхронизации времени» на стр. 349 |
| <i>IP Address</i> <i>(IP-адрес)</i> | 192.168.1.10 IP-адрес по умолчанию используется, если не используется сервер <i>протокола динамического конфигурирования хоста (DHCP)</i> . Новый статический IP-адрес можно назначить на веб-страницах администрирования. При наличии в сети сервера DHCP IP-адрес динамически присваивается сервером при запуске точки доступа. | «Общие сведения о динамической и статической IP-адресации на беспроводном шлюзе 9160 G2 Wireless Gateway» на стр. 36 |

Табл. 3.1 Значения по умолчанию 9160 G2 (Продолжение)

| Параметр | Значения по умолчанию | Дополнительная информация |
|---|---|---|
| <i>Connection Type</i> (Тип подключения) | <p>Протокол динамического конфигурирования хоста (DHCP)</p> <p>Если во внутренней сети отсутствует сервер DHCP и его использование не планируется, сразу же после загрузки точки доступа смените значение «Connection Type» (Тип подключения) с «DHCP» на «Static IP» (Статический IP-адрес).</p> <p>Сервер DHCP должен присутствовать в гостевой сети.</p> | <p>«Общие сведения о динамической и статической IP-адресации на беспроводном шлюзе 9160 G2 Wireless Gateway» на стр. 36</p> <p>Для получения информации о повторной настройке типа подключения см. раздел «Параметры внутреннего интерфейса» на стр. 154.</p> |
| <i>Subnet Mask</i> (Маска подсети) | <p>None (Нет)</p> <p>Этот параметр определяется настройками сети и конфигурацией сервера DHCP.</p> | «Интерфейс Ethernet (проводной)» на стр. 147 |
| <i>Radio</i> (Радиомодуль) | Оп (Вкл.) | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>IEEE 802.11 Mode</i> (Режим IEEE 802.11) | 802.11g или 802.11a+g | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>802.11g Channel</i> (Канал 802.11g) | Auto (Автоматический) | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>Beacon Interval</i> (Интервал маячка) | 100 | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>DTIM Period</i> (Период DTIM) | 2 | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>Fragmentation Threshold</i> (Порог фрагментации) | 2346 | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>Regulatory Domain</i> (Регулятивный домен) | FCC | «Настройка параметров радиомодуля 802.11» на стр. 183 |

Табл. 3.1 Значения по умолчанию 9160 G2 (Продолжение)

| Параметр | Значения по умолчанию | Дополнительная информация |
|--|---|---|
| <i>RTS Threshold</i> (Порог RTS) | 2347 | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>MAX Stations</i> (Макс. число станций) | 2007 | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>Transmit Power</i> (Мощность передачи) | 100% | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>Rate Sets Supported</i> (Mbps) (Поддерживаемые диапазоны скорости (Мбит/с)) | <ul style="list-style-type: none"> • IEEE 802.1a: 54, 48, 36, 24, 18, 12, 9, 6 • IEEE 802.1g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5,5, 2, 1 • IEEE 802.1b: 11, 5,5, 2, 1 | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>Rate Sets (Mbps)</i> (Диапазоны скорости (Мбит/с)) (Базовые/заявленные) | <ul style="list-style-type: none"> • IEEE 802.1a: 24, 12, 6 • IEEE 802.1g: 11, 5,5, 2, 1 • IEEE 802.1b: 2, 1 | «Настройка параметров радиомодуля 802.11» на стр. 183 |
| <i>Broadcast SSID</i> (Широковещательный идентификатор SSID) | Allow (Разрешить) | «Настройка параметров безопасности» на стр. 107. |
| <i>Security Mode</i> (Режим безопасности) | None (plain-text) (Нет (простой текст)) | «Настройка параметров безопасности» на стр. 107. |
| <i>Authentication Type</i> (Тип аутентификации) | None (Нет) | |
| <i>MAC Filtering</i> (Фильтрация MAC-адресов) | Allow any station unless in list (Разрешить все станции, кроме указанных в списке) | «Фильтрация MAC-адресов» на стр. 195 |
| <i>Guest Login and Management</i> (Гостевой вход и управление гостевыми подключениями) | Disabled (Отключено) | «Настройка гостевого доступа» на стр. 169 |

Табл. 3.1 Значения по умолчанию 9160 G2 (Продолжение)

| Параметр | Значения по умолчанию | Дополнительная информация |
|--|-----------------------|---|
| <i>Load Balancing</i> (Балансировка нагрузки) | Disabled (Отключено) | «Балансировка нагрузки» на стр. 201 |
| <i>WDS Settings</i> (Параметры WDS) | None (Нет) | «Распределенная беспроводная система» на стр. 229 |

3.1.2 Функции, которые не поддерживаются точками доступа

Беспроводной шлюз 9160 G2 Wireless Gateway не предназначен для использования в качестве интернет-шлюза (см. *Шлюз*). Для подключения беспроводной сети (*WLAN*) к другим *LAN* или к сети Интернет требуется использовать интернет-шлюз.

3.2 Компьютер администратора

Конфигурирование и администрирование беспроводного шлюза 9160 G2 Wireless Gateway осуществляется с помощью пользовательского веб-интерфейса. В Табл. 3.2 приводятся минимальные требования для компьютера администратора.

Табл. 3.2 Необходимое аппаратное и программное обеспечение администратора точки доступа

| Требуемые компоненты | Описание |
|--|--|
| <i>Подключение Ethernet к первой точке доступа</i> | <p>Компьютер, на котором выполняется конфигурация первой точки доступа, должен быть подключен к точке доступа посредством кабеля Ethernet (напрямую или через сетевой концентратор).</p> <p>Для получения дополнительной информации см. параграф «Подключение точки доступа к сети и питанию» на стр. 42 в разделе «Быстрые действия по настройке и запуску оборудования».</p> |

Табл. 3.2 Необходимое аппаратное и программное обеспечение администратора точки доступа (Продолжение)

| Требуемые компоненты | Описание |
|---|--|
| <i>Беспроводное подключение к сети</i> | <p>После настройки начальной конфигурации и запуска первой точки доступа в новой беспроводной сети вы можете внести последующие изменения в конфигурацию на веб-страницах администрирования, используя беспроводное подключение к «внутренней» сети. Для беспроводного подключения к точке доступа устройство, с которого осуществляется администрирование, должно обладать функциями Wi-Fi, подобно любому беспроводному клиенту:</p> <ul style="list-style-type: none">• Портативный или встроенный адаптер клиента Wi-Fi, поддерживающий один или несколько режимов IEEE 802.11, в которых будет работать точка доступа. (Поддерживаются следующие режимы: IEEE 802.11a, 802.11b802.11a, 802.11g802.11b, 802.11a Turbo802.11g 802.11a Turbo.)• Программное обеспечение беспроводного клиента, например беспроводной клиент Microsoft® Windows® XP или Funk Odyssey с конфигурацией, обеспечивающей подключение к беспроводному шлюзу 9160 G2 Wireless Gateway. <p>Для получения дополнительной информации о настройке клиента Wi-Fi см. «Компьютеры беспроводного клиента» на стр. 35.</p> |
| <i>Веб-браузер и операционная система</i> | <p>Настройка и администрирование беспроводного шлюза 9160 G2 Wireless Gateway выполняется на веб-страницах пользовательского интерфейса, размещенного на точке доступа. Для доступа к веб-страницам администрирования точки доступа рекомендуется использовать один из следующих поддерживаемых веб-браузеров:</p> <ul style="list-style-type: none">• Microsoft Internet Explorer 5.5 или 6.x (с обновлениями для основной версии) для ОС Microsoft Windows XP или Microsoft Windows 2000• Netscape® Mozilla 1.7.x для ОС Redhat Linux 2.4 <p>В используемом для администрирования веб-браузере должна быть включена поддержка JavaScript для отображения интерактивных средств административного интерфейса. Он также должен поддерживать загрузку данных по протоколу HTTP для использования функции обновления прошивки.</p> |
| <i>Параметры безопасности</i> | <p>Убедитесь, что режим безопасности на беспроводном клиенте, используемом для начальной конфигурации точки доступа, отключен.</p> |

3.3 Компьютеры беспроводного клиента

Беспроводной шлюз 9160 G2 Wireless Gateway обеспечивает беспроводной доступ к клиентам с правильно настроенным адаптером клиента Wi-Fi, используя режим 802.11, в котором работает точка доступа.

Поддерживаются различные клиентские операционные системы. В качестве клиентов могут выступать ноутбуки, стационарные компьютеры, карманные персональные компьютеры (КПК) и любое другое карманное, портативное или стационарное, устройство, оснащенное адаптером Wi-Fi и соответствующими драйверами.

Для подключения к точке доступа беспроводные клиенты должны соответствовать программным и аппаратным требованиям, описанным в Табл. 3.3.

Табл. 3.3 Необходимое программное и аппаратное обеспечение клиента точки доступа

| Требуемые компоненты | Описание |
|--|---|
| <i>Адаптер клиента Wi-Fi</i> | <p>Портативный или встроенный адаптер клиента Wi-Fi, поддерживающий один или несколько режимов IEEE 802.11, в которых будет работать точка доступа. (Поддерживаются следующие режимы: IEEE 802.11a, 802.11b и 802.11g.)</p> <p>Адаптеры клиентов Wi-Fi могут значительно отличаться друг от друга. В качестве адаптера может выступать PC-карта, встроенная в клиентское устройство, портативная карта PCMCIA или PCI (типа NIC) или внешнее устройство, такое как адаптер USB или Ethernet, подключаемое к клиенту через кабель.</p> <p>Точка доступа поддерживает режимы 802.11a/b/g, однако решение об использовании того или иного режима, вероятно, будет принято на этапе проектирования сети. Основное требование, предъявляемое к клиентам, — наличие адаптеров, настроенных на работу в режиме 802.11, для работы в котором настроены точки доступа.</p> |
| <i>Программное обеспечение беспроводного клиента</i> | <p>Программное обеспечение беспроводного клиента, например Microsoft Windows Supplicant или Funk Odyssey, с конфигурацией, обеспечивающей подключение к беспроводному шлюзу 9160 G2 Wireless Gateway.</p> |

Табл. 3.3 Необходимое программное и аппаратное обеспечение клиента точки доступа (Продолжение)


| Требуемые компоненты | Описание |
|--------------------------------|---|
| Параметры безопасности клиента | <p>Перед настройкой начальной конфигурации точки доступа необходимо отключить систему безопасности используемого для этой цели клиента.</p> <p>Если режим безопасности точки доступа имеет любое другое значение, кроме «простой текст», на беспроводном клиенте потребуется настроить профиль режима аутентификации, используемого точкой доступа, и указать действующее имя пользователя и пароль, сертификат или другой подобный идентификатор пользователя. Режимы безопасности: статический WEP, IEEE 802.1x, WPA с сервером RADIUS и WPA2PSK.</p> <p>Для получения информации о конфигурации системы безопасности на точке доступа см. раздел «Настройка режимов безопасности» на стр. 97.</p> |

3.4 Общие сведения о динамической и статической IP-адресации на беспроводном шлюзе 9160 G2 Wireless Gateway

9160 G2 Wireless Gateway настроен на автоматический выбор конфигурации, предусматривает всего нескольких действий со стороны пользователя для настройки первой точки доступа и не требует настройки дополнительных точек доступа при их последующем подключении к предварительно настроенному *кластеру*.

3.4.1 Как точка доступа получает IP-адрес при запуске?

В процессе развертывания точки доступа выполняется поиск в сети сервера **DHCP** и при его обнаружении точке доступа присваивается **IP-адрес**. Если сервер DHCP в сети не найден, точка доступа будет продолжать использовать свой статический IP-адрес (см. **Статический IP-адрес**) по умолчанию (192.168.1.10), пока ей не будет назначен новый статический IP-адрес (с указанием политики статической IP-адресации) или пока в сети не появится сервер DHCP.



Примечания. Если вы настроили внутреннюю и гостевую сети и планируете использовать для них политику динамической адресации, в каждой сети должен работать свой сервер DHCP.

Наличие сервера DHCP является необходимым для гостевой сети.

3.4.2 Динамическая IP-адресация

Как правило, беспроводной шлюз 9160 G2 Wireless Gateway предусматривает наличие в сети с развернутой точкой доступа сервера **DHCP**. В большинстве домашних сетей и сетей малого бизнеса уже используется сервис DHCP, предоставляемый через шлюз или централизованный сервер. Однако если во внутренней сети отсутствует сервер DHCP, для первого запуска точка доступа будет использовать статический IP-адрес (см. *Статический IP-адрес*) по умолчанию.

Аналогичным образом, если сервер DHCP присутствует в сети, он назначает IP-адреса беспроводным клиентам и другим сетевым устройствам (например, принтерам). Если в сети нет сервера DHCP, необходимо назначить статические IP-адреса беспроводным клиентам и другим сетевым устройствам вручную.

Сервер DHCP должен присутствовать в гостевой сети.

3.4.3 Статическая IP-адресация

Беспроводной шлюз 9160 G2 Wireless Gateway поставляется со следующим статическим IP-адресом (см. *Статический IP-адрес*) по умолчанию: 192.168.1.10 (см. раздел «Значения по умолчанию беспроводного шлюза 9160 G2 Wireless Gateway» на стр. 29). Если в сети не найден сервер **DHCP**, точка доступа сохраняет за собой этот статический IP-адрес при первом запуске.

После запуска точки доступа можно указать политику статической IP-адресации на беспроводных шлюзах 9160 G2 Wireless Gateway и назначить статические IP-адреса точкам доступа во внутренней сети через веб-страницы администрирования точек доступа (для получения информации о поле «Connection Type» (Тип подключения) и связанных с ним полей см. раздел «Параметры внутреннего интерфейса» на стр. 154.)



Важно! *Если во внутренней сети отсутствует сервер DHCP и его использование не планируется, сразу же после загрузки точки доступа смените значение поля «Connection Type» (Тип подключения) с «DHCP» на «Static IP» (Статический IP-адрес). Вы можете назначить точке доступа новый статический IP-адрес или использовать адрес по умолчанию. Рекомендуется назначить новый статический IP-адрес. В этом случае при запуске другого беспроводного шлюза 9160 G2 Wireless Gateway в той же сети в будущем IP-адреса для каждой точки доступа будут разными.*

3.4.4 Восстановление IP-адреса

При возникновении проблем установки связи с точкой доступа вы можете восстановить статический IP-адрес (см. *Статический IP-адрес*), сбросив конфигурацию точки доступа до заводских настроек по умолчанию (см. раздел «Сброс конфигурации до заводских настроек по умолчанию» на стр. 358), или получить динамически назначаемый адрес, подключив точку доступа к сети с сервером *DHCP*.

БЫСТРЫЕ ДЕЙСТВИЯ ПО НАСТРОЙКЕ И ЗАПУСКУ ОБОРУДОВАНИЯ

4

| | |
|--|----|
| 4.1 Распаковка беспроводного шлюза 9160 G2 Wireless Gateway | 41 |
| 4.1.1 Оборудование и порты беспроводного шлюза 9160 G2 Wireless Gateway | 41 |
| 4.1.2 Составные части беспроводного шлюза 9160 G2 Wireless Gateway | 41 |
| 4.2 Подключение точки доступа к сети и питанию. | 42 |
| 4.2.1 Примечание о настройке подключений для гостевой сети | 44 |
| 4.2.1.1 Аппаратные подключения для гостевого VLAN | 44 |
| 4.3 Включение точки доступа | 45 |
| 4.4 Доступ к веб-страницам администрирования. | 45 |
| 4.4.1 Просмотр базовых параметров точки доступа | 45 |
| 4.5 Настройка базовых параметров и запуск беспроводной сети | 46 |
| 4.5.1 Конфигурация по умолчанию | 47 |
| 4.6 Дальнейшие действия. | 47 |
| 4.6.1 Убедитесь, что точка доступа подключена к LAN | 47 |
| 4.6.2 Тестирование подключения беспроводных клиентов к LAN | 47 |
| 4.6.3 Включение дополнительных функций безопасности и точной настройки точки доступа с помощью расширенных настроек | 48 |

Настройка и развертывание одного или нескольких беспроводных шлюзов 9160 G2 Wireless Gateway в сущности представляют собой процесс создания и запуска *беспроводной сети*. Для упрощения этого процесса используется веб-страница администрирования *Basic Settings (Базовые параметры)*. Ниже представлено пошаговое руководство по настройке беспроводных шлюзов 9160 G2 Wireless Gateway и беспроводной сети. Сначала рекомендуется ознакомиться с Гл. 3: «Подготовка к запуску».

В данной главе описываются следующие действия:

- Шаг 1. *Распаковка беспроводного шлюза 9160 G2 Wireless Gateway.*
- Шаг 2. *Подключение точки доступа к сети и питанию.*
- Шаг 3. *Включение точки доступа.*
- Шаг 5. *Доступ к веб-страницам администрирования.*
- Шаг 6. *Настройка базовых параметров и запуск беспроводной сети.*
- *Дальнейшие действия*

4.1 Распаковка беспроводного шлюза 9160 G2 Wireless Gateway

Распакуйте беспроводной шлюз 9160 G2 Wireless Gateway, осмотрите аппаратные порты и проверьте наличие кабелей и аксессуаров.

4.1.1 Оборудование и порты беспроводного шлюза 9160 G2 Wireless Gateway

Комплект поставки беспроводного шлюза 9160 G2 Wireless Gateway:

- порт Ethernet для подключения к локальной сети (LAN) через сетевой кабель Ethernet;
- порт питания и адаптер питания;
- кнопка включения устройства;
- один или два радиомодуля (в зависимости от модели продукта).

4.1.2 Составные части беспроводного шлюза 9160 G2 Wireless Gateway

Беспроводной шлюз 9160 G2 Wireless Gateway, являясь точкой доступа (см. *Точка доступа*), представляет собой специализированный компьютер, предназначенный для использования в качестве беспроводного сетевого концентратора. Точка доступа состоит из системы радиосвязи Wi-Fi и микропроцессора. Точка доступа загружается с флэш-памяти, используя встроенную прошивку с настраиваемыми функциями среды выполнения, описанными в разделе «Обзор беспроводного шлюза 9160 G2 Wireless Gateway» на стр. 8.

При выпуске новых функций и расширений функциональных возможностей вы можете обновить прошивку и добавить новые функции, а также повысить производительность точек доступа, из которых состоит ваша беспроводная сеть (см. раздел «Обновление прошивки» на стр. 360).

4.2 Подключение точки доступа к сети и питанию

Следующим шагом является настройка подключений к сети и питанию.

1. Выполните одно из следующих действий для создания подключения Ethernet между точкой доступа и компьютером.

Подключите один конец кабеля Ethernet к сетевому порту точки доступа, а другой — к концентратору, к которому подключен ваш компьютер (см. Рис. 4.2 на стр. 44).

или

Подключите один конец перекрестного¹ кабеля к сетевому порту точки доступа, а другой — к порту Ethernet компьютера (см. Рис. 2 на стр. 44).



Примечания. При использовании сетевого концентратора устройство должно разрешить передачу сигналов от точки доступа ко всем устройствам сети. Как правило, стандартные концентраторы справляются с этой задачей. Однако некоторые коммутаторы не поддерживают направленное вещание и передачу сигналов в подсети. Поэтому может потребоваться настройка коммутатора на поддержку направленного вещания.

При настройке начальной конфигурации с прямым подключением Ethernet без использования сервера DHCP статический IP-адрес компьютера должен находиться в той же подсети, что и IP-адрес по умолчанию, назначенный точке доступа (IP-адрес по умолчанию для точки доступа: 192.168.1.10).

¹ Если аппаратное обеспечение точки доступа поддерживает автоматические функции **MDI** и **MDI-X**, можно использовать стандартный кабель Ethernet для прямого подключения компьютера к точке доступа. В этом случае также можно использовать перекрестный кабель, но в нем нет необходимости, если имеются автоматические сенсорные порты MDI и MDI-X.

Если начальная конфигурация выполняется с использованием прямого (проводного) подключения Ethernet через перекрестный кабель между точкой доступа и компьютером, необходимо изменить конфигурацию кабельного соединения для последующего запуска и развертывания точки доступа таким образом, чтобы точка доступа была подключена не к компьютеру, а к локальной сети (через сетевой концентратор, как показано на Рис. 4.2, или напрямую).

Рис. 4.1 Подключение Ethernet с использованием сервера DHCP

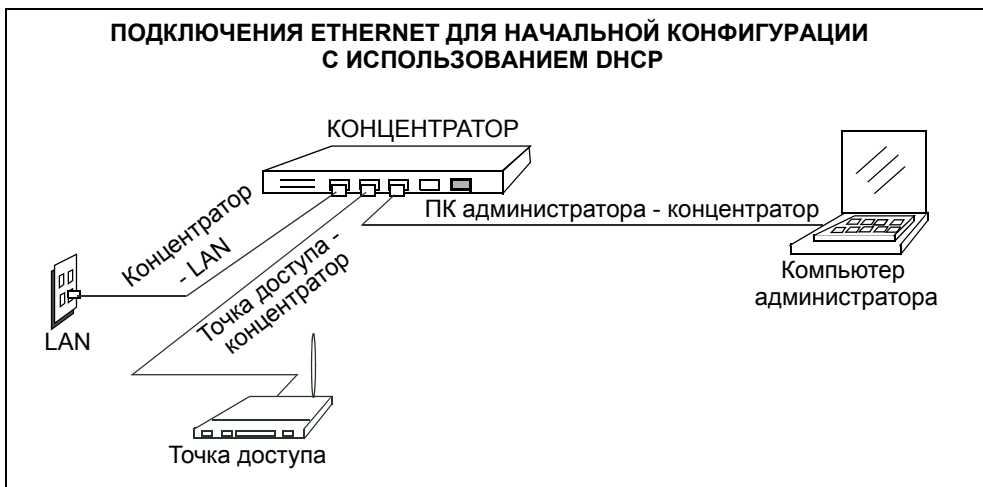
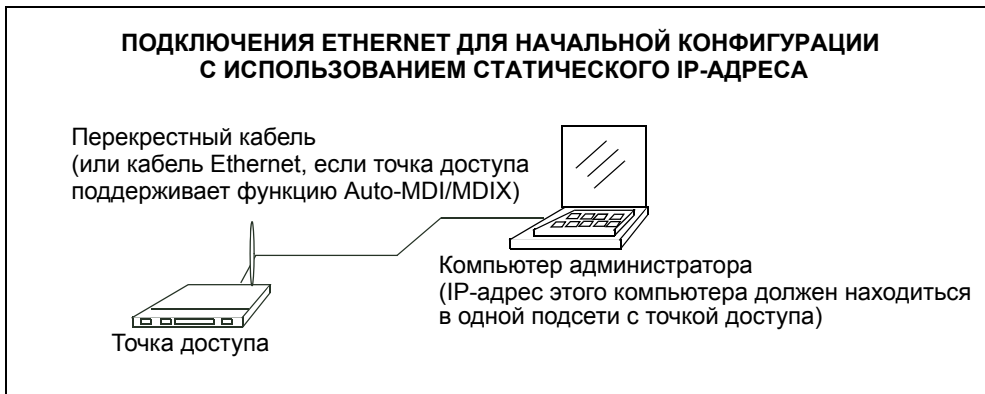


Рис. 4.2 Подключение Ethernet с использованием статического IP-адреса



2. Подключите адаптер питания к порту питания на задней панели точки доступа и подключите другой конец шнура питания к розетке (рекомендуется использовать стабилизатор напряжения).

4.2.1 Примечание о настройке подключений для гостевой сети

Беспроводной шлюз 9160 G2 Wireless Gateway имеет встроенный гостевой интерфейс, позволяющий настраивать точку доступа для контролируемого гостевого доступа к сети. Одна точка доступа может функционировать в качестве моста для двух разных беспроводных сетей: безопасной «внутренней» LAN и общедоступной «гостевой» сети. Это может быть сделано виртуально, путем определения двух разных виртуальных LAN через административный интерфейс.

Для получения информации о настройке параметров гостевого интерфейса через административный интерфейс см. Гл. 14: «Настройка гостевого доступа».

4.2.1.1 Аппаратные подключения для гостевого VLAN

Чтобы настроить гостевую сеть с использованием VLAN, выполните следующие действия.

- Подключите сетевой порт точки доступа к коммутатору с поддержкой VLAN.
- Определите VLAN для коммутатора.

4.3 Включение точки доступа

Включение и инициализация беспроводного шлюза 9160 G2 Wireless Gateway происходит в момент его подключения к сети питания.

4.4 Доступ к веб-страницам администрирования

При переходе на IP-адрес веб-страниц администрирования беспроводного шлюза 9160 G2 Wireless Gateway появляется запрос на ввод имени пользователя и пароля.



Для имени пользователя и пароля используются следующие значения по умолчанию.

Табл. 4.1 Имя пользователя и пароль

| Поле | Значение по умолчанию |
|-------------------------------------|--|
| <i>User name (Имя пользователя)</i> | admin |
| <i>Password (Пароль)</i> | admin (имя пользователя доступно только для чтения; его нельзя изменить) |

Введите имя пользователя и пароль и нажмите **ОК**.

4.4.1 Просмотр базовых параметров точки доступа

При первом входе в систему отображается экран *Basic Settings (Базовые параметры)* для администрирования беспроводного шлюза 9160 G2 Wireless Gateway. Здесь представлены глобальные параметры для всех точек доступа, объединенных в кластер, и, если выбрана автоматическая конфигурация, для всех новых точек доступа, которые будут добавлены позже.

Рис. 4.3 Базовые параметры точки доступа

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Provide basic settings

1

Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address:10.128.75.4

MAC Address:00:08:A2:01:4B:52

Firmware Version:E187k

2

Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password

New Password

Confirm new password

Network Name (SSID)Psion Teklogix

3

Settings ...

Click "Update" to save the new settings.

Update

4.5 Настройка базовых параметров и запуск беспроводной сети

Укажите минимальный набор конфигурационных данных, определив базовые параметры для своей беспроводной сети. Эти параметры доступны на экране *Basic Settings* (Базовые параметры) веб-интерфейса администрирования и разделены на 3 этапа.

Для получения дополнительной информации о базовых параметрах и их настройке см. Гл. 5: «Настройка базовых параметров». Ниже представлен краткий обзор этапов настройки.

1. Обзор описания точки доступа.
Настройка IP-адресации. Для получения дополнительной информации см. раздел «Обзор и описание точки доступа» на стр. 52.
2. Настройка сетевых параметров.
Изменение пароля администратора для объединенных в кластер точек доступа. Для получения дополнительной информации см. раздел «Настройка сетевых параметров» на стр. 53.

3. Параметры.

Нажмите кнопку **Update** (Обновить) для активации беспроводной сети с новыми параметрами. Для получения дополнительной информации см. раздел «Обновление базовых параметров» на стр. 54.

4.5.1 Конфигурация по умолчанию

При выборе значений по умолчанию на предыдущих этапах настройки точка доступа будет сконфигурирована по умолчанию, описанную в разделе «Значения по умолчанию беспроводного шлюза 9160 G2 Wireless Gateway» на стр. 29.

4.6 Дальнейшие действия

Убедитесь, что точка доступа подключена к LAN, запустите несколько беспроводных клиентов и подключите их к сети. После базового тестирования беспроводной сети вы можете активировать дополнительные функции безопасности и точной настройки, изменив расширенные функции конфигурации точки доступа.

4.6.1 Убедитесь, что точка доступа подключена к LAN

Если конфигурация точки доступа и компьютера администратора выполнялась через их подключение к сетевому концентратору, это значит, что точка доступа уже подключена к LAN. Теперь ваше оборудование запущено и работает! Следующий шаг — тестирование беспроводных клиентов.

Если конфигурация точки доступа выполнялась с помощью прямого проводного подключения через перекрестный кабель от компьютера к точке доступа, выполните следующие действия.

1. Отключите перекрестный кабель от компьютера и точки доступа.
2. Подключите стандартный кабель Ethernet к точке доступа и *LAN*.
3. Подключите компьютер к LAN через кабель Ethernet или карту беспроводного клиента.

4.6.2 Тестирование подключения беспроводных клиентов к LAN

Протестируйте беспроводной шлюз 9160 G2 Wireless Gateway путем поиска и подключения к нему любого беспроводного клиентского устройства (для получения информации о требованиях к клиентам см. параграф «Компьютеры беспроводного клиента» на стр. 35 в разделе *Подготовка к запуску*).

4.6.3 Включение дополнительных функций безопасности и точной настройки точки доступа с помощью расширенных настроек

После запуска беспроводной сети и тестирования работы точек доступа с несколькими беспроводными клиентами можно включать дополнительные уровни безопасности, добавлять пользователей, настраивать гостевой интерфейс и регулировать параметры производительности оборудования.

НАСТРОЙКА БАЗОВЫХ ПАРАМЕТРОВ

5

| | |
|--|----|
| 5.1 Переход к базовым параметрам. | 51 |
| 5.2 Обзор и описание точки доступа | 52 |
| 5.3 Настройка сетевых параметров. | 53 |
| 5.4 Обновление базовых параметров. | 54 |
| 5.5 Базовые параметры автономной точки доступа | 54 |
| 5.6 Краткий обзор сети: значки индикаторов | 54 |

5.1 Переход к базовым параметрам

Для настройки первоначальных параметров нажмите **Basic Settings** (Базовые параметры).

Если вы ввели IP-адрес точки доступа в адресную строку браузера, по умолчанию открывается экран *Basic Settings* (Базовые параметры).

Рис. 5.1 Базовые параметры

PSION TEKLOGIX
Information in motion

9160 Wireless Gateway

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Provide basic settings

1 Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 10.128.75.4

MAC Address: 00:08:A2:01:4B:52

Firmware Version: E187k

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password

New Password

Confirm new password

Network Name (SSID) Psion Teklogix

3 Settings ...

Click "Update" to save the new settings.

Заполните поля на экране *Basic Settings* (Базовые параметры), следуя инструкциям, приведенным в «Обзор и описание точки доступа» на стр. 52.

5.2 Обзор и описание точки доступа

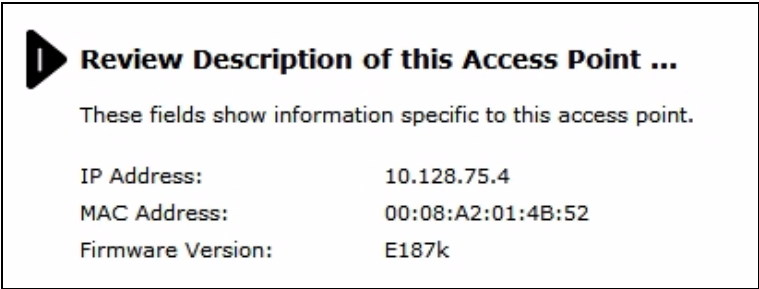


Табл. 5.1 Параметры экрана «Basic Settings» (Базовые параметры)

| Поле | Описание |
|--|---|
| <i>IP Address</i> (IP-адрес) | Показывает IP-адрес, назначенный точке доступа. Значение поля изменить невозможно, так как IP-адрес уже назначен точке доступа (посредством DHCP или статически через параметры Ethernet (проводной сети), как описано в «Параметры гостевого интерфейса» на стр. 157). |
| <i>MAC Address</i> (MAC-адрес) | <p>Показывает MAC-адрес точки доступа.</p> <p>MAC-адрес является постоянным уникальным аппаратным адресом любого устройства, представляющего интерфейс для сети. MAC-адрес присваивается производителем. Этот адрес нельзя изменить. Значение этого адреса как уникального идентификатора интерфейса отображается только в информационных целях.</p> <p>Указанный здесь адрес является MAC-адресом моста (br0). По этому адресу точка доступа распознается другими внешними сетями.</p> <p>Для просмотра MAC-адресов гостевого и внутреннего интерфейсов на точке доступа перейдите на вкладку <i>Status (Смартс)</i>, <i>Interfaces (Интерфейсы)</i>.</p> |
| <i>Firmware Version</i> (Версия прошивки) | <p>Информация о версии прошивки, установленной на точке доступа.</p> <p>По мере выхода новых версий прошивки беспроводного шлюза 9160 G2 Wireless Gateway вы можете обновить прошивку на своей точке доступа, чтобы воспользоваться новыми функциями и улучшениями.</p> <p>Для получения инструкций по обновлению прошивки см. «Обновление прошивки» на стр. 360.</p> |

5.3 Настройка сетевых параметров

2

Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password


New Password

Confirm new password

Network Name (SSID)

Psion Teklogix

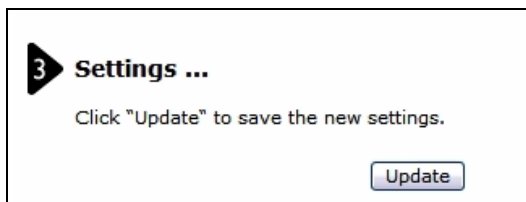
Табл. 5.2 Пароль администратора и беспроводная сеть

| Поле | Описание |
|---|---|
| <i>Current Password</i> (Текущий пароль) | Введите текущий пароль администратора. Прежде чем изменить пароль, необходимо правильно указать текущий пароль. |
| <i>New Password</i> (Новый пароль) | <p>Введите новый пароль администратора. Вводимые символы будут отображаться в виде звездочек («*»), чтобы их не могли увидеть посторонние.</p> <p>Пароль администратора должен состоять из букв и цифр и не должен превышать 8 символов. Нельзя использовать специальные символы и пробелы.</p> <div> Первое, что необходимо сделать для защиты беспроводной сети, — сменить пароль администратора.</div> |
| <i>Confirm New Password</i> (Подтвердить новый пароль) | Повторно введите новый пароль администратора для его подтверждения. |
| <i>Network Name (SSID)</i> (Сетевое имя (SSID)) | <p>Введите имя беспроводной сети в виде строки символов. Это имя будет применяться ко всем точкам доступа в данной сети. По мере добавления новых точек доступа они будут получать этот SSID.</p> <p><i>Идентификатор набора служб (SSID)</i> представляет собой строку, состоящую максимум из 32 буквенно-числовых символов.</p> <p>Примечание. Если вы подключены к администрируемой точке доступа с помощью беспроводного клиента, при сбросе SSID соединение с этой точкой доступа будет потеряно. После сохранения нового параметра потребуется повторное подключение к новому SSID.</p> |



Примечание. Беспроводной шлюз 9160 G2 Wireless Gateway не предназначен для одновременного выполнения нескольких изменений настроек. Если в вашей сети есть несколько точек доступа, и с веб-страницами администрирования одновременно работают несколько администраторов, выполняющих изменения конфигурации, все точки доступа в кластере остаются синхронизированными, но нет гарантии, что все конфигурационные изменения, произведенные несколькими пользователями, будут применены.

5.4 Обновление базовых параметров



После обзора новой конфигурации нажмите **Update** (Обновить) для применения параметров и развертывания точек доступа в качестве беспроводной сети.

5.5 Базовые параметры автономной точки доступа

Вкладка *Basic Settings* (*Базовые параметры*) для автономной точки доступа содержит только информацию о том, что текущий режим работы является автономным. Если вы хотите добавить точку доступа к существующему кластеру, перейдите на вкладку *Cluster* (*Кластер*) > *Access Point* (*Точка доступа*).

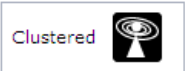
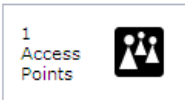
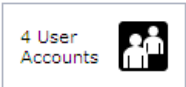
Для получения дополнительной информации см. раздел «Запуск кластеризации» на стр. 65.

5.6 Краткий обзор сети: значки индикаторов

Все вкладки с параметрами кластера на веб-страницах администрирования имеют значки визуальных индикаторов, показывающих текущую активность сети.

5.7 Изменение цветов и стиля пользовательского интерфейса

Табл. 5.3 Значки индикаторов

| Значок | Описание |
|---|---|
|  | Когда одна или несколько точек доступа доступны для обслуживания, отображается значок «Wireless Network Available» (Доступна беспроводная сеть). Значок кластеризации указывает, является данная точка доступа кластеризованной («Clustered») или нет («Not Clustered») (во втором случае она является автономной или ее состояние в настоящее время меняется). Для получения информации о кластеризации см. «Общие сведения о кластеризации» на стр. 60. |
|  | Количество точек доступа, доступных в данной сети, обозначается значком «Access Points» (Точки доступа). Для получения информации об управлении точками доступа см. Гл. 6: «Управление точками доступа и кластерами». |
|  | Количество учетных записей пользователей клиентов, созданных и включенных в данной сети, обозначается значком «User Accounts» (Учетные записи пользователей). Для получения информации о настройке учетных записей пользователей на точке доступа для использования с встроенным сервером аутентификации см. Гл. 7: «Управление учетными записями пользователей». Также ознакомьтесь с «IEEE 802.1x» на стр. 116 и «WPA Enterprise» на стр. 122, в которых содержатся сведения о двух режимах безопасности, позволяющих использовать встроенный сервер аутентификации. |

Вы можете выбрать один из визуальных стилей для просмотра веб-страниц администрирования беспроводного шлюза 9160 G2 Wireless Gateway: 1) «Corporate» (Корпоративный) и 2) «Home» (Домашний).

Вы можете изменить стиль пользовательского интерфейса в соответствии со своими предпочтениями.

Чтобы сменить стиль, найдите кнопки «Style»: «Corporate», «Home» (Стиль: Корпоративный, Домашний) в нижней части любой веб-страницы администрирования и нажмите кнопку **Corporate** (Корпоративный) или **Home** (Домашний).



УПРАВЛЕНИЕ ТОЧКАМИ ДОСТУПА И КЛАСТЕРАМИ

6

| | |
|---|----|
| 6.1 Обзор | 59 |
| 6.2 Переход к управлению точками доступа | 59 |
| 6.3 Общие сведения о кластеризации | 60 |
| 6.3.1 Что такое кластер? | 60 |
| 6.3.2 Сколько точек доступа может поддерживать кластер? | 60 |
| 6.3.3 Какие типы точек доступа могут быть кластеризованы? | 60 |
| 6.3.4 Какова взаимосвязь координирующей точки доступа с другими членами кластера? | 61 |
| 6.3.5 Какие параметры являются/не являются общими в конфигурации кластера? | 61 |
| 6.3.5.1 Общие параметры в конфигурации кластера | 61 |
| 6.3.5.2 Параметры, не являющиеся общими для кластера | 62 |
| 6.3.6 Формирование кластера | 62 |
| 6.3.7 Размер кластера и членство в кластере | 63 |
| 6.3.8 Безопасность внутри кластера | 63 |
| 6.4 Общие сведения о параметрах точек доступа. | 63 |
| 6.4.1 Изменения описания местоположения | 65 |
| 6.4.2 Настройка имени кластера | 65 |
| 6.5 Запуск кластеризации. | 65 |
| 6.6 Остановка кластеризации. | 66 |
| 6.7 Конфигурационная информация определенной точки доступа и управление автономными точками доступа. | 66 |
| 6.7.1 Переход к точке доступа с использованием ее IP-адреса в URL-адресе | 67 |
| 6.8 Мониторинг сеансов | 67 |
| 6.8.1 Переход к мониторингу сеансов | 67 |
| 6.8.2 Общие сведения о мониторинге сеансов | 68 |
| 6.8.3 Просмотр информации о сеансах точек доступа | 69 |
| 6.8.4 Сортировка информации о сеансах | 70 |
| 6.8.5 Обновление информации о сеансах | 70 |

6.1 Обзор

Беспроводной шлюз 9160 G2 Wireless Gateway показывает текущие основные параметры настройки для объединенных в кластер точек доступа (местоположение, IP-адрес, MAC-адрес, статус и доступность) и дает возможность просмотра полной конфигурации определенных точек доступа, если они входят в кластер.

Автономные точки доступа, а также точки доступа, которые не входят в данный кластер, не отображаются в этом списке. Чтобы настроить автономную точку доступа, необходимо знать ее IP-адрес и использовать его в формате URL

(<http://IPAddressOfAccessPoint>).



Примечание. Беспроводной шлюз 9160 G2 Wireless Gateway не предназначен для одновременного выполнения нескольких изменений настроек. Если в вашей сети есть несколько точек доступа, и с веб-страницами администрирования одновременно работают несколько администраторов, выполняющих изменения конфигурации, все точки доступа в кластере остаются синхронизированными, но нет гарантии, что все конфигурационные изменения, произведенные несколькими пользователями, будут применены.

6.2 Переход к управлению точками доступа

Для просмотра и редактирования информации о точках доступа в кластере перейдите на вкладку **Cluster** (Кластер) > **Access Points** (Точки доступа).

Рис. 6.1 Параметры кластера для точек доступа

Manage access points in the cluster

Access Points...



Status: Clustering is online...

| Location | MAC Address | IP Address |
|------------------------------|-------------------|---------------|
| Vicky's Office - top shelf | 00:0C:41:16:A3:12 | 10.10.100.238 |
| Vicky's Office - lower shelf | 00:00:04:7F:00:00 | 10.10.100.245 |

Clustering Options...

Enter the location of this AP.
Location:

Enter the name of the cluster for this AP to join.
Cluster Name:

Clustered 
1 Access Points 

6.3 Общие сведения о кластеризации

Ключевой функцией беспроводного шлюза 9160 G2 Wireless Gateway является возможность формирования динамических сконфигурированных групп (называемых *кластерами*) с другими беспроводными шлюзами 9160 G2 Wireless Gateway в сети в рамках одной подсети. Точки доступа могут участвовать в самоорганизующемся кластере, что облегчает развертывание, администрирование и обеспечение безопасности беспроводной сети. Кластер предоставляет единый центр администрирования и позволяет рассматривать процесс развертывания точек доступа как единой беспроводной сети, а не набора отдельных беспроводных устройств.

6.3.1 Что такое кластер?

Кластер — это группа точек доступа, управляемых как одна группа посредством администрирования беспроводного шлюза 9160 G2 Wireless Gateway. В одной подсети может быть несколько кластеров с разными «именами».

6.3.2 Сколько точек доступа может поддерживать кластер?

В настоящее время не существует ограничений на количество точек доступа в кластере. В ходе проверочных испытаний в одной подсети была успешно протестирована работа более десяти точек доступа. В кластер можно добавить столько точек доступа, сколько вам необходимо.

6.3.3 Какие типы точек доступа могут быть кластеризованы?

Один беспроводной шлюз 9160 G2 Wireless Gateway может сформировать кластер, включающий только себя или другие беспроводные шлюзы 9160 G2 Wireless Gateway. Чтобы стать членами кластера, точки доступа должны соответствовать следующим требованиям:

- Быть совместимыми устройствами, обозначенными производителем (точки доступа должны иметь совместимые конструктивные особенности).
- У них должны совпадать конфигурации радиомодулей (количество радиомодулей должно быть одинаковым у всех точек доступа).
- У них должны совпадать конфигурации диапазонов (все точки доступа должны быть или однодиапазонными, или двухдиапазонными).
- Они должны находиться в одной *LAN*.

Наличие разных точек доступа в сети в любом случае отрицательно сказывается на кластеризации беспроводного шлюза 9160 G2 Wireless Gateway. Однако для целей администрирования может быть полезным понимание процесса кластеризации:

- Точки доступа, добавляемые в кластер, должны иметь одинаковое имя. Для получения дополнительной информации о настройке имени кластера см. стр. 65.
- Нельзя добавить в кластер точки доступа других производителей. Администрирование таких точек доступа должны осуществляться собственными средствами администрирования.

6.3.4 Какова взаимосвязь координирующей точки доступа с другими членами кластера?

Конфигурация кластера, совместное обновление конфигурации и отслеживание новых точек доступа, добавляемых или удаляемых из группы, управляются *координирующей* точкой доступа, которая выбирается из других членов кластера. Если координирующая точка доступа становится недоступной, обязанности координатора берет на себя новый член кластера. Этот процесс является полностью автоматизированным, он основан на наборе правил, учитывающих при выборе точки доступа, наиболее подходящей для выполнения этих действий, принцип «старшинства», размер кластера и другие факторы.

Нет необходимости следить за тем, какая точка доступа является координирующей, потому что этот статус может меняться в зависимости от потребностей кластера. Мы описываем этот принцип работы только потому, что вы можете заметить небольшую разницу конфигурационной информации, отображаемой на веб-страницах администрирования для координирующей точки и других членов кластера.

6.3.5 Какие параметры являются/не являются общими в конфигурации кластера?

Большая часть параметров настройки, определяемых на веб-страницах администрирования 9160 G2 Wireless Gateway, распространяется для других членов кластера как часть *конфигурации кластера*.

6.3.5.1 Общие параметры в конфигурации кластера

Конфигурация кластера включает следующие параметры:

- Сетевое имя (SSID).
- Пароль администратора.
- Учетные записи и аутентификация пользователей.
- Параметры беспроводного интерфейса.
- Параметры приветственного экрана гостевого входа.
- Параметры сетевого протокола синхронизации времени (NTP).

- Параметры радиомодуля.
В кластере синхронизируются только следующие настройки: «Mode» (Режим), «Channel» (Канал), «Fragmentation Threshold» (Порог фрагментации), «RTS Threshold» (Порог RTS) и «Rate Sets» (Диапазоны скорости). Не кластеризуются следующие настройки: «Beacon Interval» (Интервал маячка), «DTIM Period» (Период DTIM), «Maximum Stations» (Максимальное количество станций) и «Transmit Power» (Мощность передачи).



Примечание. При включенном параметре «Channel Planning» (Планирование канала) настройка «Channel» (Канал) радиомодуля не синхронизируется в кластере. См. раздел «Остановка/запуск автоматического назначения каналов» на стр. 84.

- Параметры безопасности.
- Параметры очереди QoS.
- Фильтрация MAC-адресов.

6.3.5.2 Параметры, не являющиеся общими для кластера

Есть несколько исключений (параметры, не являющиеся общими для кластеризованных точек доступа), большинство из которых должны быть уникальными.

- IP-адреса.
- MAC-адреса.
- Описания местоположений.
- Параметры балансировки нагрузки.
- Мосты WDS.
- Параметры проводной сети Ethernet.
- Конфигурация гостевого интерфейса.

Параметры, не являющиеся общими, настраиваются отдельно для каждой точки доступа с помощью интерфейса администрирования. Чтобы перейти в интерфейс администрирования точки доступа, находящейся в текущем кластере, нажмите на ссылку «IP Address» (IP-адрес) в разделе *Cluster (Кластер) > Access Points (Точки доступа)* на текущей точке доступа.

6.3.6 Формирование кластера

Кластер формируется при развертывании первой точки доступа с включенной функцией кластеризации. Точка доступа пытается найти существующий кластер. Если ей не удалось найти другие точки доступа в подсети с таким же именем кластера, она создает новый кластер самостоятельно.

6.3.7 Размер кластера и членство в кластере

В настоящее время не существует ограничений на количество точек доступа в кластере. В ходе проверочных испытаний в одной подсети была успешно протестирована работа более десяти точек доступа. В кластер можно добавить столько точек доступа, сколько вам необходимо.

Членство в кластере определяется следующими параметрами:

- Имя кластера — точки доступа с одинаковым именем будут добавлены в один кластер (см. «Настройка имени кластера» на стр. 65).
- Включенная функция кластеризации — только точки доступа с включенной функцией кластеризации будут добавлены в кластер (см. «Запуск кластеризации» на стр. 65 и «Остановка кластеризации» на стр. 66).

6.3.8 Безопасность внутри кластера

Для простоты использования компонент кластеризации позволяет добавлять новые устройства в кластер без строгой аутентификации. Однако передача всех данных между точками доступа в кластере защищена от случайного перехвата протоколом защиты информации SSL. Считается, что частная проводная сеть, к которой подключены устройства, является защищенной. Как конфигурационный файл кластера, так и база данных пользователей передается между точками доступа с использованием протокола SSL.

6.4 Общие сведения о параметрах точек доступа

На вкладке «Access Points» (Точки доступа) содержится информация обо всех точках доступа в кластере. На этой вкладке вы можете просматривать описания местоположений, MAC-адреса, IP-адреса, включать (активировать) или отключать (деактивировать) *кластеризованные* точки доступа и удалять точки доступа из кластера. Вы также можете изменять описание местоположения точки доступа. С помощью ссылок IP-адресов можно перейти к параметрам и данным настройки на точке доступа.

Автономные точки доступа (которые не входят в данный кластер) не отображаются на этом экране.

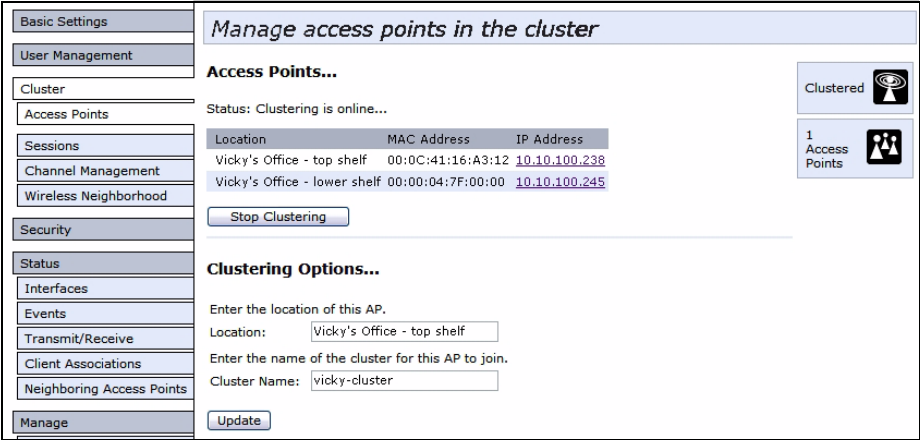


Табл. 6.1 содержит подробную информацию о параметрах точки доступа и отображаемых данных.

Табл. 6.1 Параметры точки доступа

| Поле | Описание |
|------------------------------|---|
| Location (Местоположение) | Описание физического местоположения точки доступа. |
| MAC Address (MAC-адрес) | <p>Адрес управления доступом к среде передачи (MAC) точки доступа.</p> <p>MAC-адрес является постоянным уникальным аппаратным адресом любого устройства, представляющего интерфейс для сети. MAC-адрес присваивается производителем. Этот адрес нельзя изменить. Значение этого адреса как уникального идентификатора точки доступа приведено только в информационных целях.</p> <p>Указанный здесь адрес является MAC-адресом моста (br0). По этому адресу точка доступа распознается другими внешними сетями.</p> <p>Для просмотра MAC-адресов гостевого и внутреннего интерфейсов на точке доступа перейдите на вкладку <i>Status (Сматус)</i> > <i>Interfaces (Интерфейсы)</i>.</p> |
| IP Address (IP-адрес) | IP-адрес точки доступа. Каждый IP-адрес является ссылкой на веб-страницы администрирования данной точки доступа. Используйте ссылки для перехода на веб-страницы администрирования определенной точки доступа. Таким образом вы можете просматривать информацию об определенной точке доступа, чтобы убедиться, что член кластера принимает конфигурационные изменения, настроить расширенные параметры на конкретной точке доступа или переключить автономную точку доступа в режим кластера. |

6.4.1 Изменения описания местоположения

Чтобы изменить описание местоположения:

1. Перейдите на вкладку *Cluster (Кластер)* > *Access Points (Точки доступа)*.
2. В разделе *Clustering Options (Параметры кластеризации)* укажите новое местоположение точки доступа в поле *Location (Местоположение)*.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

6.4.2 Настройка имени кластера

Чтобы настроить имя кластера, к которому вы хотите добавить точку доступа, выполните следующие действия:

1. Перейдите на вкладку «Cluster» (Кластер) > «Access Points» (Точки доступа).
2. В разделе *Clustering Options (Параметры кластеризации)* укажите новое имя кластера в поле *Cluster Name (Имя кластера)*.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.



Примечание. Если к кластеру нужно добавить несколько точек доступа, все они должны иметь имя кластера, указанное в поле «Cluster Name» (Имя кластера). Если точка доступа имеет другое имя кластера, ее нельзя будет добавить к кластеру.

6.5 Запуск кластеризации

Для запуска кластеризации и добавления определенной точки доступа к кластеру выполните следующие действия.

1. Перейдите на веб-страницу администрирования данной автономной точки доступа (см. раздел «Переход к точке доступа с использованием ее IP-адреса в URL-адресе» на стр. 67).
Отобразятся веб-страницы администрирования данной автономной точки доступа.
2. Перейдите на вкладку **Cluster** (Кластер) > **Access Points** (Точки доступа) автономной точки доступа.
3. Нажмите кнопку **Start Clustering** (Начать кластеризацию).
Точка доступа добавлена к кластеру. Она отображается в списке кластеризованных точек доступа на вкладке *Cluster (Кластер)* > *Access Points (Точки доступа)*.



Примечание. В некоторых ситуациях кластер может не синхронизироваться. Если после добавления точки доступа к кластеру она не отображается или частично отображается в списке точек доступа, следуйте инструкциям по восстановлению кластера, приведенным в Прил. С: «Поиск и устранение неисправностей».

6.6 Остановка кластеризации

Для остановки кластеризации и удаления определенной точки доступа из кластера выполните следующие действия.

1. Перейдите на веб-страницы администрирования точки доступа, которую вы хотите удалить из кластера.
2. Перейдите на вкладку **Cluster** (Кластер) > **Access Points** (Точки доступа).
3. Нажмите кнопку **Stop Clustering** (Остановить кластеризацию) для удаления точки доступа из кластера.

Изменения отобразятся в поле *Status* (Статус) этой точки доступа — значение *cluster* (кластер) изменится на *standalone* (автономная).



Примечание. В некоторых ситуациях кластер может не синхронизироваться. Если после удаления точки доступа из кластера она полностью или частично отображается в списке точек доступа, обновите страницу браузера. При повторном возникновении проблемы следуйте инструкциям по восстановлению кластера, приведенным в Прил. С: «Поиск и устранение неисправностей».

6.7 Конфигурационная информация определенной точки доступа и управление автономными точками доступа

Беспроводной шлюз 9160 G2 Wireless Gateway предназначен для централизованного управления *кластеризованными* точками доступа. При кластеризации все точки доступа имеют одинаковую конфигурацию. В этом случае неважно, к какой точки доступа вы подключаетесь для администрирования.

Однако могут возникнуть ситуации, когда необходимо просмотреть или изменить данные конкретной точки доступа. Например, проверить информацию о статусе точки доступа — ассоциациях с клиентами или событиях, настроить или изменить функции точки доступа, работающей в *автономном* режиме. В этих случаях перейдите на административный веб-интерфейс данной точки доступа, нажав на ссылку IP-адреса на вкладке точки доступа.

Все кластеризованные точки доступа отображаются на экране *Cluster (Кластер) > Access Points (Точки доступа)*. Для перехода к кластеризованным точкам доступа просто нажмите на IP-адрес определенного члена кластера в списке.

6.7.1 Переход к точке доступа с использованием ее IP-адреса в URL-адресе

Вы также можете перейти на веб-страницы администрирования точки доступа, указав ее IP-адрес в качестве URL-адреса непосредственно в адресной строке браузера следующим образом:

http://IPAddressOfAccessPoint

где *IPAddressOfAccessPoint* — это IP-адрес точки доступа, которую вы хотите настроить. Таким же образом вы можете перейти к конфигурационной информации автономной точки доступа.

6.8 Мониторинг сеансов

Беспроводной шлюз 9160 G2 Wireless Gateway обеспечивает контроль сеансов в режиме реального времени, в том числе получение информации о том, какие клиенты связаны с определенной точкой доступа, о скорости обмена данными, статистике получения и передачи данных, силе сигнала и времени простоя.

6.8.1 Переход к мониторингу сеансов

Чтобы просмотреть информацию о мониторинге сеансов, нажмите вкладку **Cluster** (Кластер) > **Sessions** (Сеансы).

Рис. 6.2 Информация о мониторинге сеансов

Manage sessions associated with the cluster

Sessions...

You may sort the following table by clicking on any of the column names.

Display

All

Go

| User | AP Location | User MAC | Idle | Rate (Mbps) | Signal | Utilization | Rx Total | Tx Total | Error Rate | Idle |
|-------|-------------|-------------------|------|-------------|--------|-------------|----------|----------|------------|------|
| Ciara | not set | 00:90:4b:93:f4:35 | 150 | 54 | 44 | 0.1 % | 78944 | 107640 | 0 | 150 |
| Sean | not set | 00:0c:f1:3e:99:ae | 190 | 11 | 44 | 0.4 % | 4462 | 3147 | 0 | 190 |

You may restrict the number of columns displayed by selecting a field other than "all" in the choice box above. By selecting a specific field, the table will show only "User", "AP Location", "User MAC" and the selected field for each session. Click the "Go" button to apply the new selection.

Clustered

1 Access Points

0 User Accounts

6.8.2 Общие сведения о мониторинге сеансов

На экране *Sessions (Сеансы)* отображается информация о клиентских станциях, ассоциированных с точками доступа в кластере. Каждый клиент определяется именем и **MAC**-адресом пользователя, а также точкой доступа (местоположением), к которой он подключен в настоящий момент времени.

Чтобы просмотреть определенную статистику клиентских сеансов, выберите пункт раскрывающегося списка «Display» (Показать) и нажмите **Go** (Перейти). Доступна следующая информация: *Idle Time (Время простоя)*, *Data Rate (Скорость передачи данных)*, *Signal (Сигнал)*, *Utilization (Использование)* и другие параметры, описание которых приведено в Табл. 6.2 на стр. 68.

В данном контексте «сеанс» означает период времени, в течение которого пользователь подключен к беспроводной сети через клиентское устройство (станцию) с уникальным MAC-адресом. Сеанс начинается, когда клиент входит в сеть, и заканчивается, когда клиент завершает работу в сети самостоятельно или связь прерывается по другим причинам.



Примечание. Сеанс отличается от ассоциации, под которой понимается подключение клиента к определенной точке доступа. Клиент может быть подключен к сети через разные точки доступа кластера в рамках одного сеанса. Клиентская станция переключается от одной точки доступа к другой и продолжает сеанс.

Для получения информации о мониторинге ассоциаций и целостности связи см. «Ассоциированные беспроводные клиенты» на стр. 140.

Табл. 6.2 Информация о сеансе

| Поле | Описание |
|---|---|
| <i>User Name (Имя пользователя)</i> | Указывает имя пользователя клиента IEEE 802.1x. Примечание. Это поле доступно только для клиентов, подключенных к точкам доступа с использованием режима безопасности IEEE 802.1x и локального сервера аутентификации. Для получения дополнительной информации об этом режиме см. «IEEE 802.1x» на стр. 116. Здесь не отображаются имена пользователей для клиентов точек доступа, использующих режим IEEE 802.1x с RADIUS-сервером или другие режимы безопасности. |
| <i>AP Location (Местоположение точки доступа)</i> | Указывает местоположение точки доступа. Эта информация берется из описания местоположения на вкладке <i>Basic Settings (Базовые параметры)</i> . |

Табл. 6.2 Информация о сеансе (Продолжение)

| Поле | Описание |
|---|---|
| <i>User MAC Address</i> (MAC-адрес пользователя) | Указывает MAC-адрес клиентского устройства (станции) пользователя. MAC -адрес — это аппаратный адрес, являющийся уникальным идентификатором каждого узла сети. |
| <i>Idle Time</i> (Время простоя) | Обозначает период времени, в течение которого данная станция оставалась неактивной. Станция считается неактивной, если она не получает и не передает данные. |
| <i>Data Rate</i> (Скорость передачи данных) | Скорость, с которой точка доступа передает данные указанному клиенту. Скорость передачи данных измеряется в <i>мегабитах в секунду</i> (Мб/с). Это значение должно находиться в диапазоне заявленной скорости для режима IEEE 802.1x , используемого на точке доступа. Например, от 6 до 54 Мб/с для 802.11a. |
| <i>Signal</i> (Сигнал) | Обозначает силу радиосигнала, получаемого клиентами от точки доступа. Показатель измеряется как значение IEEE 802.1x , или <i>индикатор уровня принимаемого сигнала</i> (RSSI), от 0 до 100. Значение RSSI определяется механизмом IEEE 802.1x, реализованным в сетевой плате (NIC) клиентской станции. |
| <i>Utilization</i> (Использование) | Коэффициент использования данной станции. Например, если станция активна (передает и получает данные) 90% времени и неактивна 10% времени, коэффициент ее использования составляет 90%. |
| <i>Receive Total</i> (Всего получено) | Показывает общее количество пакетов, полученных клиентом в течение текущего сеанса. |
| <i>Transmit Total</i> (Всего передано) | Показывает общее количество пакетов, переданных клиенту в течение текущего сеанса. |
| <i>Error Rate</i> (Коэффициент ошибок) | Показывает процент временных кадров, потерянных во время передачи данных на точке доступа. |

6.8.3 Просмотр информации о сеансах точек доступа

Вы можете одновременно просматривать информацию о сеансах для всех точек доступа в сети или настроить просмотр информации о сеансах определенной точки доступа, выбрав ее из раскрывающегося меню в верхней части экрана.

Чтобы просмотреть информацию обо всех точках доступа, установите переключатель **Show all access points** (Показать все точки доступа) в верхней части экрана.

Чтобы просмотреть информацию о сеансах для определенной точки доступа, установите переключатель **Show only this access point** (Показать только эту точку доступа) и выберите имя точки доступа из раскрывающегося списка.

6.8.4 Сортировка информации о сеансах

Чтобы упорядочить (сортировать) показанную в таблицах информацию по определенному параметру, нажмите на заголовок столбца, по которому вы хотите сортировать данные. Например, если вы хотите просмотреть строки таблицы по коэффициенту использования, нажмите заголовок столбца **Utilization** (Использование). Данные будут отсортированы по коэффициенту использования.

6.8.5 Обновление информации о сеансах

Вы можете вручную обновить информацию, отображаемую на экране *Session Monitoring* (Мониторинг сеансов), нажав кнопку **Refresh** (Обновить).

УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЕЙ 7

| | |
|--|----|
| 7.1 Обзор | 73 |
| 7.2 Переход к управлению пользователями | 73 |
| 7.2.1 Просмотр учетных записей пользователей | 74 |
| 7.2.2 Добавление пользователя | 74 |
| 7.2.3 Редактирование учетной записи пользователя. | 75 |
| 7.2.4 Включение и отключение учетных записей пользователей. | 76 |
| 7.2.5 Включение учетной записи пользователя | 76 |
| 7.2.6 Отключение учетной записи пользователя. | 77 |
| 7.2.7 Удаление учетной записи пользователя | 77 |
| 7.3 Резервное копирование и восстановление базы данных пользователей | 77 |
| 7.3.1 Резервное копирование базы данных пользователей | 77 |
| 7.3.2 Восстановление базы данных пользователей из резервного файла | 78 |

7.1 Обзор

Беспроводной шлюз 9160 G2 Wireless Gateway включает функции управления пользователями для контроля клиентского доступа к точкам доступа.

Функция управления и аутентификации пользователей всегда должна использоваться вместе с одним из следующих режимов безопасности, требующих использования сервера **RADIUS** для аутентификации и управления пользователями.

- Режим IEEE 802.1x (см. «IEEE 802.1x» на стр. 116 в Гл. 10: «Настройка режимов безопасности»).
- Режим WPA с RADIUS (см. «WPA Enterprise» на стр. 122 в Гл. 10: «Настройка режимов безопасности»).

Можно использовать внутренний RADIUS-сервер, встроенный в 9160 G2 Wireless Gateway, или любой внешний RADIUS-сервер. При использовании встроенного RADIUS-сервера используйте веб-страницу администрирования точки доступа для настройки и управления учетными записями пользователей. Если вы используете внешний RADIUS-сервер, настройка и управление учетными записями пользователей выполняется в интерфейсе администрирования этого сервера.

На экране «User Management» (Управление пользователями) вы можете создавать, редактировать, удалять и просматривать *учетные записи пользователей* клиентов. Каждая учетная запись состоит из имени пользователя и пароля. Указанный здесь список пользователей представляет собой список *клиентских устройств*, которые при выполненном входе могут использовать одну или несколько точек доступа для получения доступа к локальной, а возможно, и внешней, сети через вашу точку доступа.



Примечание. Указанные здесь пользователи являются клиентами точки (или точек) доступа, использующие точки доступа как сетевой концентратор для подключения, а не администраторами беспроводной сети. Вход от имени администратора, просмотр и изменение параметров настройки возможны только с именем пользователя и пароля администратора, а также URL-адреса страницы администрирования.

7.2 Переход к управлению пользователями

Для настройки и изменения учетных записей пользователей перейдите на вкладку **User Management** (Управление пользователями).

Рис. 7.1 Управление учетными записями пользователей



7.2.1 Просмотр учетных записей пользователей

Учетные записи пользователей отображаются в верхней части экрана в разделе *User Accounts...* (*Учетные записи пользователей...*). Отображаются значения «Username» (Имя пользователя), «Real name» (Настоящее имя) и «Status» (Статус) (включен или отключен) пользователя. Внесите изменения в существующую учетную запись, установив флажок около имени пользователя и затем выбрав действие. (См. «Редактирование учетной записи пользователя» на стр. 75.)

7.2.2 Добавление пользователя

Чтобы создать пользователя, выполните следующие действия.

- 1. В разделе *Add a User...* (*Добавить пользователя...*) заполните следующие поля.

Табл. 7.1 Поля добавления пользователя

| Поле | Описание |
|---------------------------------------|---|
| <i>Username</i> (Имя пользователя) | Укажите имя пользователя. Имя пользователя должно состоять из буквенно-цифровых символов и не должно превышать 237 символов. Не допускается использование специальных символов или пробелов. |
| <i>Real name</i> (Настоящее имя) | Для информации укажите полное настоящее имя пользователя. Длина настоящего имени не должна превышать 256 символов. |
| <i>Password</i> (Пароль) | Укажите пароль пользователя. Пароль должен состоять из буквенно-цифровых символов и не должен превышать 256 символов. Не допускается использование специальных символов или пробелов. |

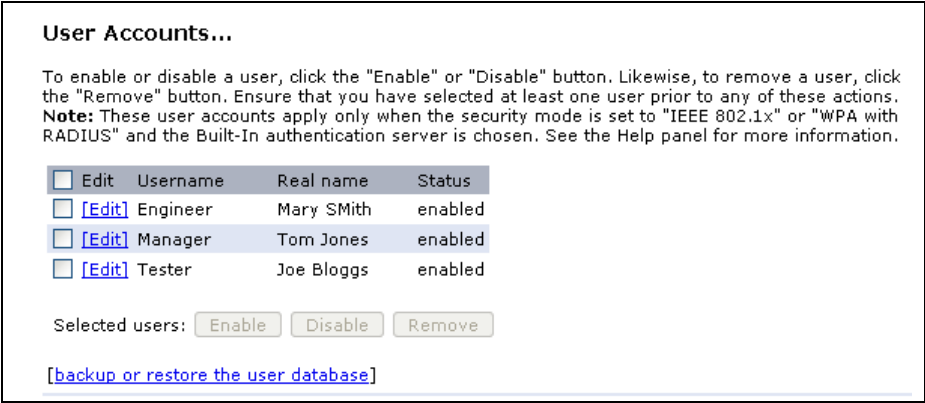
2. После заполнения полей нажмите **Add Account** (Добавить учетную запись).
 Новый пользователь отображается в разделе *User Accounts...* (*Учетные записи пользователей...*). По умолчанию новая учетная запись пользователя **включена**.



Примечание. Лимит учетных записей пользователей для точки доступа, установленный для административного интерфейса, составляет 100 записей. При использовании сети возможен ввод большего количества практических ограничений, в зависимости от требований к каждому пользователю.

7.2.3 Редактирование учетной записи пользователя

После создания учетной записи пользователя она отображается в разделе *User Accounts...* (*Учетные записи пользователей...*) в верхней части веб-страницы администрирования *User Management* (*Управление пользователями*). Чтобы изменить существующую учетную запись пользователя, сначала установите рядом с ней флажок.



Затем выберите одно из следующих действий: **Edit** (Редактировать), **Enable** (Включить), **Disable** (Отключить) или **Remove** (Удалить).

7.2.4 Включение и отключение учетных записей пользователей

Чтобы пользователь мог войти и использовать точку доступа через клиентское устройство, учетная запись пользователя должна быть включена.

Вы можете выбрать действия **Enable** (Включить) и **Disable** (Отключить) для любой учетной записи. С помощью этой функции вы можете управлять несколькими учетными записями и предоставлять доступ (или отказывать в доступе) к сети пользователям без необходимости удалять и заново создавать учетные записи пользователей. Это может быть полезным в ситуациях, когда пользователям необходим нерегулярный доступ в сеть. Например, подрядчикам, которые работают в вашей компании на нерегулярной основе, нужен доступ к сети в течение трех месяцев, затем три месяца они будут отсутствовать, а потом вернуться и будут выполнять новое задание. Учетные записи этих пользователей можно включать и отключать по необходимости и осуществлять контроль за доступом к сети.

7.2.5 Включение учетной записи пользователя

Чтобы включить учетную запись пользователя, установите флажок рядом с именем пользователя и нажмите **Enable** (Включить). Пользователь с включенной учетной записью может подключиться к беспроводной точке доступа вашей сети в качестве клиента.

7.2.6 Отключение учетной записи пользователя

Чтобы отключить учетную запись пользователя, установите флажок рядом с именем пользователя и нажмите **Disable** (Отключить).

Пользователь с *отключенной* учетной записью не сможет подключиться к беспроводной точке доступа вашей сети в качестве клиента. Однако пользователь остается в базе данных и его учетную запись можно будет включить позже по необходимости.

7.2.7 Удаление учетной записи пользователя

Чтобы удалить учетную запись пользователя, установите флажок рядом с именем пользователя и нажмите **Remove** (Удалить).

Если будет необходимо добавить этого пользователя позже, вы можете *отключить* его, а не удалять его учетную запись.

7.3 Резервное копирование и восстановление базы данных пользователей

Вы можете сохранить копию текущего набора учетных записей пользователей в резервный конфигурационный файл. Резервный файл может быть использован позже для восстановления учетных записей пользователей на точке доступа до предыдущей сохраненной конфигурации.

7.3.1 Резервное копирование базы данных пользователей

Чтобы создать резервную копию учетных записей пользователей для данной точки доступа:

1. Нажмите ссылку **[backup or restore the user database]** ([создать или восстановить резервную копию базы данных пользователей]).

Откроется диалоговое окно *File Download or Open (Загрузить или открыть файл)*.

2. Выберите **Save** (Сохранить) в первом диалоговом окне.

Откроется диспетчер файлов.

В диспетчере файлов выберите каталог, в котором вы хотите сохранить файл, и нажмите **ОК** для сохранения файла.

Можно оставить имя резервного файла по умолчанию (wirelessUsers.ubk) или переименовать его и сохранить с расширением .ubk.

7.3.2 Восстановление базы данных пользователей из резервного файла

Чтобы восстановить базу данных пользователей из резервного файла, выполните следующие действия.

1. Выберите нужный резервный конфигурационный файл, указав полный путь к файлу в поле «Restore» (Восстановить), или нажмите **Browse** (Обзор) и выберите файл.

Для восстановления базы данных пользователей могут использоваться только файлы, созданные с помощью функции резервного копирования базы данных пользователей и сохраненные как резервные конфигурационные файлы с расширением .ubk, например wirelessUsers.ubk.

2. Нажмите кнопку **Restore** (Восстановить).

По завершении процесса резервного восстановления появится сообщение, информирующее о том, что база данных пользователей была успешно восстановлена. (Процесс восстановления не занимает много времени и завершается за считанные минуты.)

Нажмите вкладку **User Management** (Управление пользователями) для просмотра учетных записей пользователей.

| | | |
|-------|--|----|
| 8.1 | Переход к управлению каналами | 81 |
| 8.2 | Общие сведения об управлении каналами | 81 |
| 8.2.1 | Краткое описание процесса | 82 |
| 8.2.2 | Дополнительная информация о перекрывающихся каналах | 82 |
| 8.2.3 | Пример. Сеть до и после управления каналами | 82 |
| 8.3 | Настройка и просмотр параметров управления каналами | 83 |
| 8.3.1 | Остановка/запуск автоматического назначения каналов | 84 |
| 8.3.2 | Просмотр текущих назначений каналов и настройка блокировок | 85 |
| 8.3.3 | Просмотр последнего рекомендованного набора изменений. | 86 |
| 8.3.4 | Настройка расширенных параметров (изменение и составление графика планов каналов) | 86 |

8.1 Переход к управлению каналами

Для просмотра информации о мониторинге сеансов перейдите на вкладку **Cluster** (Кластер) > **Channel Management** (Управление каналами).

Рис. 8.1 Управление назначением каналов

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

Automatically manage channel assignments

Channels ...

Start automatically re-assigning channels

Current Channel Assignments

| IP Address | Radio | Band | Channel | Locked |
|---------------|-------------------|------|---------|--------------------------|
| 10.10.100.238 | 00:0C:41:16:A3:12 | G | 2 | <input type="checkbox"/> |
| 10.10.100.245 | 00:00:04:7F:00:00 | G | 3 | <input type="checkbox"/> |

Apply

Proposed Channel Assignments (3 hours, 40 minutes and 52 seconds old)

| IP Address | Radio | Proposed Channel |
|---------------|-------------------|------------------|
| 10.10.100.238 | 00:0C:41:16:A3:12 | 2 |

Advanced

Change channels if interference is reduced by at least

5%

Determine if there is better set of channel settings every

1 Minute

Update

Clustered

2 Access Points

3 User Accounts

8.2 Общие сведения об управлении каналами

При включенной функции *Channel Management* (Управление каналами) беспроводной шлюз 9160 G2 Wireless Gateway автоматически назначает радиоканалы, используемые объединенными в кластер точками доступа, с целью снижения уровня взаимных помех, а также помех, вызываемых другими точками доступа, не входящими в кластер. Это увеличивает полосу пропускания Wi-Fi и способствует поддержке качества связи в вашей беспроводной сети.

(Для автоматического назначения каналов необходимо включить функцию управления каналами; по умолчанию на новой точке доступа эта функция отключена. См. «Остановка/запуск автоматического назначения каналов» на стр. 84.)

8.2.1 Краткое описание процесса

Через определенный интервал (по умолчанию **1 час**) или по требованию (при нажатии **Update** (Обновить)), диспетчер каналов отображает использование точек доступа и каналов и измеряет уровень помех в кластере. При обнаружении значительного уровня межканальных помех диспетчер каналов автоматически переназначает некоторые или все точки доступа новым каналам в соответствии с алгоритмом эффективности (или *automated channel plan* (автоматизированный план каналов)).

8.2.2 Дополнительная информация о перекрывающихся каналах

Канал передачи радиосигналов (см. *Канал*) определяет часть спектра радиоволн, которую радиомодуль точки доступа использует для передачи и получения данных. Диапазон доступных каналов для точки доступа определяется режимом **IEEE 802.11** (также называемым диапазоном частот) точки доступа.

Режимы **IEEE 802.11b/802.11g** (802.11 b/g) поддерживают использование от 1 до 11 каналов включительно, в то время как режим **IEEE 802.11a** поддерживает более широкий набор непоследовательных каналов (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165).

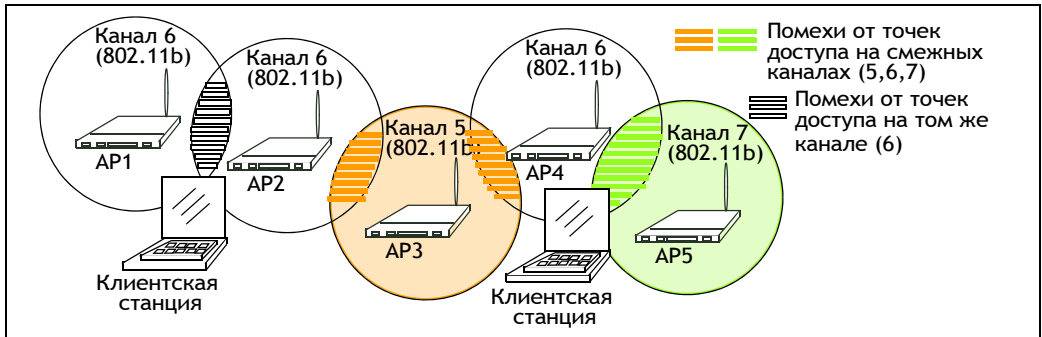
Помехи случаются, когда несколько точек доступа в пределах одного диапазона осуществляют широкополосную передачу на одних и тех же или *перекрывающихся* каналах. Влияние помех на производительность сети может увеличиваться в периоды занятости каналов, когда большое количество данных и мультимедийного трафика конкурируют за полосу пропускания.

Диспетчер каналов определяет, на каких диапазонах частот (b/g или a) находятся кластеризованные точки доступа, и использует заранее заданный набор каналов, которые не будут создавать взаимных помех. Для диапазона радиочастот «b/g» классическим набором каналов без взаимных помех являются 1, 6, 11. Каналы 1, 4, 8, 11 дают минимальное перекрытие. Такой же набор не создающих помех каналов используется для диапазона радиочастот «a», который включает все каналы для данного режима, так как они не перекрываются.

8.2.3 Пример. Сеть до и после управления каналами

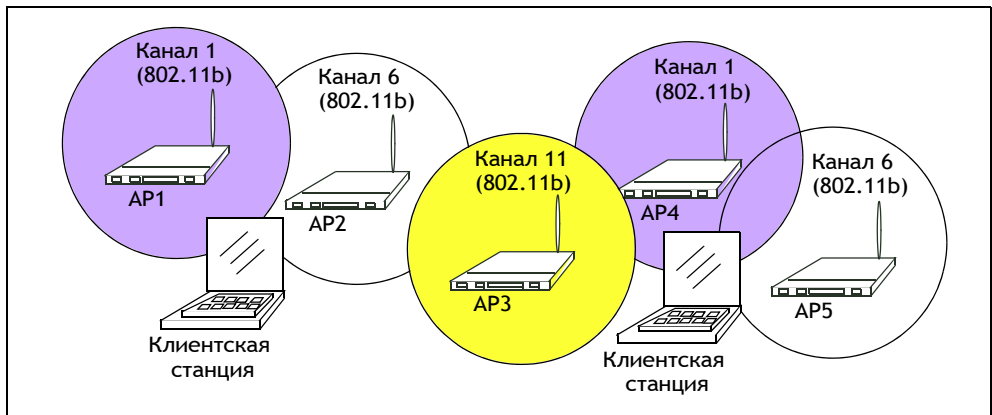
Без автоматизированного управления каналами назначение каналов кластеризованным точкам доступа может выполняться на *последовательных каналах*, которые будут перекрываться и создавать помехи. Например, AP1 и AP2 могут быть назначены каналу 6, а AP3 — каналу 5, как показано на Рис. 8.2.

Рис. 8.2 Без автоматического управления каналами



Благодаря функции автоматического управления каналами, точки доступа в кластере автоматически переназначаются неперекрывающимся каналам, как показано на 8.3.

Рис. 8.3 С включенной функцией управления каналами



8.3 Настройка и просмотр параметров управления каналами

На экране управления каналами показаны предыдущие, текущие и запланированные назначения каналов для кластеризованных точек доступа. По умолчанию автоматическое назначение каналов отключено. Вы можете включить функцию управления каналами, чтобы оптимизировать использование каналов в кластере по заданным интервалам.

На этом экране вы увидите назначения каналов для всех точек доступа в кластере, сможете включить и отключить функцию автоматического управления каналами и вручную обновить текущую карту каналов (сопоставление точек доступа и каналов). При ручном обновлении диспетчер каналов выполнит оценку использования каналов и, при необходимости, переназначит точки доступа новым каналам для снижения уровня помех на основе текущих расширенных параметров.

Используя расширенные параметры, вы можете изменять потенциал снижения помех, запускающий процесс переназначения каналов, менять расписание автоматических обновлений и заново настраивать набор каналов, используемых для назначений.

В следующих разделах описаны процессы настройки и использования функции управления каналами в сети:

- «Остановка/запуск автоматического назначения каналов» на стр. 84.
- «Просмотр текущих назначений каналов и настройка блокировок» на стр. 85.
- «Ручное обновление текущих параметров канала» на стр. 86.
- «Просмотр последнего рекомендованного набора изменений» на стр. 86.
- «Настройка расширенных параметров (изменение и составление графика планов каналов)» на стр. 86.
- «Обновление расширенных параметров» на стр. 88.

8.3.1 Остановка/запуск автоматического назначения каналов

По умолчанию автоматическое назначение каналов отключено («off»).

- Нажмите **Start** (Запустить) для запуска автоматического назначения каналов. Когда автоматическое назначение каналов включено, диспетчер каналов периодически сопоставляет каналы радиосвязи, используемые кластеризованными точками доступа, и при необходимости переназначает каналы на кластеризованных точках доступа для снижения помех (с членами кластера или другими точками доступа вне кластера).



Примечание. При использовании функции управления каналами меняется поведение кластера по умолчанию — синхронизация каналов радиосвязи на всех точках доступа в кластере. При включенном управлении каналами канал радиосвязи не синхронизируется с другими точками доступа в кластере. См. примечание в разделе «Radio Settings» (Параметры радиомодуля) в «Общие параметры в конфигурации кластера» на стр. 61.

- Нажмите **Stop** (Остановить) для отключения автоматического назначения каналов. (При этом не создаются карты использования каналов и не выполняются переназначения каналов. Изменение назначения каналов возможно только при ручном обновлении.)

8.3.2 **Просмотр текущих назначений каналов и настройка блокировок**

На странице *Current Channel Settings (Текущие параметры канала)* отображается список всех точек доступа в кластере по IP-адресу. Показан диапазон частот, на котором ведет трансляцию каждая точка доступа, текущий канал, используемый каждой точкой доступа, и функция «блокировки» точки доступа на текущем канале радиосвязи, благодаря которой точка доступа не может быть переназначена другому каналу. Ниже приведено подробное описание текущих параметров канала.

Табл. 8.1 Текущие параметры канала

| Поле | Описание |
|---------------------------------|--|
| <i>IP Address</i> (IP-адрес) | Указывает IP-адрес точки доступа. |
| <i>Radio</i> (Радиомодуль) | Указывает MAC -адрес точки доступа. |
| <i>Band</i> (Диапазон) | Указывает диапазон радиочастот (b/g или a), на которых осуществляет трансляцию точка доступа. |
| <i>Channel</i> (Канал) | Указывает канал радиосвязи (Канал), на котором осуществляет трансляцию точка доступа. |
| <i>Locked</i> (Блокировка) | <p>Нажмите Locked (Блокировка), если вы хотите, чтобы точка доступа оставалась на текущем канале.</p> <p>Если для точки доступа установлен флажок «Locked» (Блокировка), при автоматическом управлении каналами точка доступа не будет переназначена другому каналу в рамках стратегии оптимизации. Вместо этого точки доступа с заблокированными каналами будут учтены как требование к плану.</p> <p>При нажатии Update (Обновить) вы увидите, что для заблокированных точек доступа значение «Current Channel» (Текущий канал) и «Proposed Channel» (Рекомендуемый канал) не меняются. Заблокированные точки доступа продолжают работать на тех же каналах.</p> |

8.3.2.1 Ручное обновление текущих параметров канала

В любое время вы можете выполнить ручное обновление функции управления каналами, нажав **Update** (Обновить) на странице *Current Channel Settings* (Текущие параметры канала).

8.3.3 Просмотр последнего рекомендованного набора изменений

На странице *Last Proposed Set of Channel Changes* (Последний рекомендованный набор изменений) отображается последний план каналов. В плане перечислены все точки доступа в кластере по IP-адресу и показаны текущие и рекомендованные каналы для каждой точки доступа. Заблокированные каналы не переназначаются и в процессе оптимизации распределения каналов между точками доступа будет учтено, что заблокированные точки доступа должны оставаться на своих текущих каналах. Незаблокированные точки доступа могут быть назначены другим каналам, в зависимости от результатов планирования.

Табл. 8.2 План каналов точки доступа

| Поле | Описание |
|--------------------------------------|--|
| <i>IP Address</i> (IP-адрес) | Указывает IP-адрес точки доступа. |
| <i>Current</i> (Текущий) | Указывает канал радиосвязи, на котором осуществляет трансляцию точка доступа. |
| <i>Proposed</i> (Рекомендованный) | Указывает канал радиосвязи, которому будет переназначена точка доступа при реализации этого плана каналов. |

8.3.4 Настройка расширенных параметров (изменение и составление графика планов каналов)

Если вы используете функцию *Channel Management* (Управление каналами) в простом виде (без обновления *расширенных параметров*), каналы автоматически настраиваются каждый час, если помехи можно снизить на 25% и выше. Каналы будут переназначены, даже если сеть будет занята. Будут использоваться соответствующие наборы каналов («b/g» для точек доступа, работающих в режиме IEEE 802.11b/g, и «a» для точек доступа, работающих в режиме IEEE 802.11a).

Эти значения по умолчанию предназначены для большинства сценариев, которые вы можете использовать для реализации функции управления каналами.

Используя раздел *Advanced Settings (Расширенные параметры)*, вы можете изменять потенциал снижения помех, запускающий процесс переназначения каналов, менять расписание автоматических обновлений и заново настраивать набор каналов, используемых для назначений.

Табл. 8.3 Расширенные параметры

| Поле | Описание |
|---|---|
| <i>Advanced (Дополнительно)</i> | Нажмите переключатель «Advanced» (Дополнительно), чтобы отобразить или скрыть параметры, изменяющие время и подробные сведения об алгоритме планирования каналов. По умолчанию эти параметры скрыты . |
| <i>Change channels if interference is reduced by at least __ (Изменить каналы, если уровень помех снизится по крайней мере на __)</i> | <p>Укажите минимальное процентное значение снижения уровня помех, которое должно быть достигнуто при применении рекомендуемого плана. Значение по умолчанию: 25%.</p> <p>Используйте раскрывающееся меню для выбора значения от 25% до 75%.</p> <p>С помощью этого параметра вы можете установить пропускающее значение для переназначения каналов, чтобы избежать постоянного прерывания связи в сети с минимальным повышением производительности.</p> <p>Например, если необходимо снизить уровень межканальных помех на 75%, а рекомендуемое назначение каналов приведет к их снижению только на 30%, каналы не будут переназначены. Однако если вы установите минимальное снижение уровня помех на 25% и нажмете Update (Обновить), рекомендуемый план использования каналов будет реализован, и каналы будут переназначены в соответствии с этим планом.</p> |
| <i>Determine if there is better set of channel settings every __ (Определять наличие наилучшего набора параметров канала каждые __)</i> | <p>Используйте раскрывающееся меню для выбора расписания автоматического обновления.</p> <p>Доступен диапазон значений от «1 Minute» (1 минута) до «6 Months» (6 месяцев). По умолчанию используется значение «1 Hour» (1 час) (использование каналов оценивается каждый час, и в результате применяется новый план использования каналов).</p> |

Табл. 8.3 Расширенные параметры (Продолжение)

| Поле | Описание |
|---|--|
| <i>Use these channels when applying channel assignments (Использовать эти каналы при назначении)</i> | <p>Выберите набор не создающих взаимных помех каналов в определенном диапазоне радиочастот («b/g» или «a»). Доступны следующие значения:</p> <ul style="list-style-type: none">• каналы b/g 1-6-11• каналы b/g 1-4-8-11• a <p>Режимы IEEE 802.11b/802.11g (802.11 b/g) поддерживаются использование каналов от 1 до 11. Для диапазона радиочастот «b/g» классическим набором каналов без взаимных помех являются 1, 6, 11. Каналы 1, 4, 8, 11 дают минимальное перекрытие.</p> <p>Режим IEEE 802.11a поддерживает использование расширенного набора непоследовательных каналов (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165). Каналы диапазона частот «a» не создают взаимных помех.</p> |
| <i>Apply channel modifications even when the network is busy (Переназначать каналы даже при занятой сети)</i> | <p>Включите или отключите этот параметр.</p> <p>Установленный флажок означает, что параметр включен и каналы будут переназначены даже если сеть будет занята. Отсутствие флажка означает, что при занятой сети каналы переназначаться не будут.</p> <p>Этот параметр (вместе с параметром снижения уровня помех) предназначен для оценки рентабельности производительности сети при переназначении каналов по сравнению с неизбежным прерыванием связи с клиентским устройством в течение периодов пиковой занятости.</p> |

8.3.4.1 Обновление расширенных параметров

Нажмите **Update** (Обновить) в разделе *Advanced Settings (Расширенные параметры)* для применения этих параметров.

Расширенные параметры будут применены и будут оказывать влияние на то, как выполняется управление каналами. Новое минимальное значения снижения уровня помех, график настройки, набор каналов и параметры занятости сети будут учтены при автоматическом и ручном обновлении.

БЕСПРОВОДНОЕ ОКРУЖЕНИЕ

9

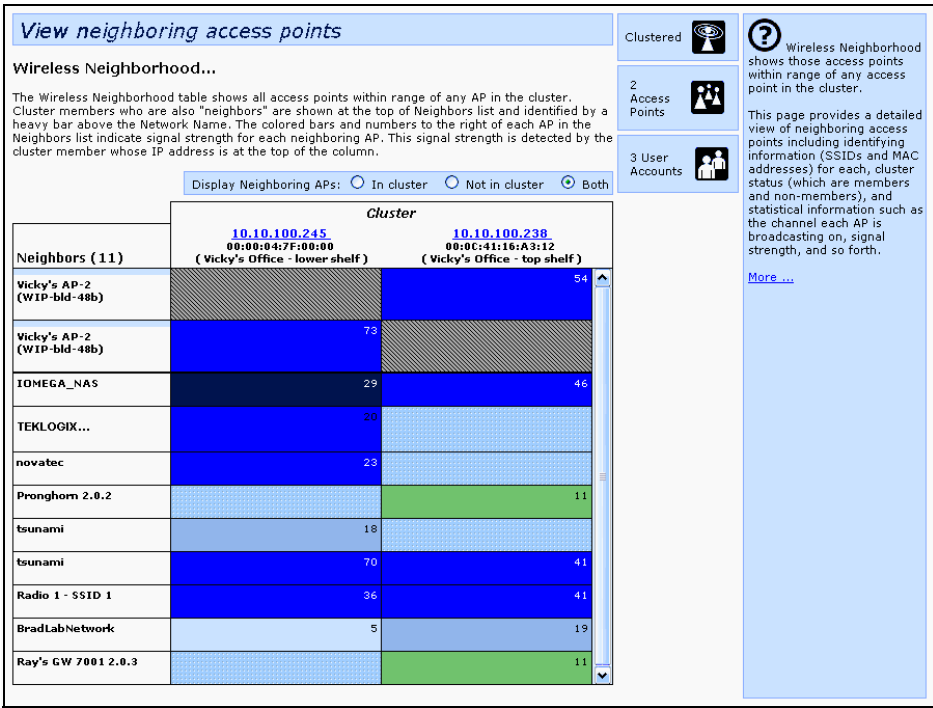
| | |
|--|----|
| 9.1 Переход к экрану беспроводного окружения | 91 |
| 9.2 Общие сведения о беспроводном окружении. | 91 |
| 9.3 Просмотр беспроводного окружения | 92 |
| 9.4 Просмотр сведений о члене кластера | 94 |

На экране *Wireless Neighborhood* (Беспроводное окружение) показаны точки доступа, находящиеся в пределах досягаемости любой точки доступа в кластере. На этом экране представлены подробные сведения о соседних точках доступа, в том числе идентифицирующая информация (идентификаторы SSID и MAC-адреса) для каждой из них, статус кластера (какие из них являются членами кластера, а какие — нет) и статистическая информация: канал, на котором работает каждая точка доступа, мощность сигнала и т.д.

9.1 Переход к экрану беспроводного окружения

Для просмотра страницы *Wireless Neighborhood* (Беспроводное окружение) нажмите вкладку **Cluster** (Кластер) > **Wireless Neighborhood** (Беспроводное окружение).

Рис. 9.1 Соседние точки доступа (кластеризованные и автономные)



9.2 Общие сведения о беспроводном окружении

Страница *Wireless Neighborhood* (Беспроводное окружение) показывает все точки доступа, находящиеся в пределах досягаемости любого члена кластера, а также точки доступа, находящиеся в пределах досягаемости определенных членов кластера, и приводит сведения о кластеризованных и автономных точках доступа.

Для каждой соседней точки доступа на экране «Wireless Neighborhood» (Беспроводное окружение) показана идентифицирующая информация (**SSID** или сетевое имя, **IP-адрес**, **MAC-адрес**), а также статистика радиомодуля (мощность сигнала, канал, интервал маячка). Нажав на любую точку доступа, вы можете получить дополнительную информацию о точках доступа, находящихся в диапазоне радиочастот выбранной точки доступа.

На экране «Wireless Neighborhood» (Беспроводное окружение) вы можете выполнять следующие действия.

- Обнаруживать и устанавливать местоположение незнакомых (или *мошеннических*) точек доступа в беспроводном домене и принимать меры для снижения риска.
- Проверить зону покрытия. Оценив расстояние от видимых точек доступа до других при разной мощности сигнала, вы можете проверить, насколько реализуемым является ваш план развертывания сети.
- Обнаружить ошибки. Непредвиденные изменения зоны покрытия можно увидеть при рассмотрении таблицы с цветовой кодировкой.

9.3 Просмотр беспроводного окружения

Ниже представлена подробная информация, доступная на экране «Wireless Neighborhood» (Беспроводное окружение).

Табл. 9.1 Информация о беспроводном окружении

| Поле | Описание |
|--|---|
| <i>Display Neighboring APs (Показывать соседние точки доступа)</i> | Нажмите один из следующих переключателей для изменения вида просмотра: <ul style="list-style-type: none">• <i>In cluster (В кластере)</i> — показывать только те соседние точки доступа, которые являются членами кластера.• <i>Not in cluster (Не в кластере)</i> — показывать только те соседние точки доступа, которые не являются членами кластера.• <i>Both (Все)</i> — показывать все соседние точки доступа (кластеризованные и автономные). |
| <i>Cluster (Кластер)</i> | В списке «Cluster» (Кластер) в верхней части таблицы показаны IP-адреса для всех точек доступа в кластере. (Это тот же список членов кластера, который содержится на вкладке <i>Cluster (Кластер) > Access Points (Точки доступа)</i> и описан в «Переход к управлению точками доступа» на стр. 59.) Если в кластере присутствует только одна точка доступа, будет отображаться один столбец с IP-адресом, указывая на то, что точка доступа «кластеризована сама с собой». Нажмите на IP-адрес конкретной точки доступа, чтобы просмотреть дополнительную информацию о ней, как показано в Рис. 9.2 на стр. 94. |

Табл. 9.1 Информация о беспроводном окружении (Продолжение)

| Поле | Описание | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|----------------------------|----------------------------|--|--|----------------------------|----------------------------|----------------------------|--------------------------|--|---|----|--------------------------|--|--|--|--------------------------|----|---|--|--------------------------|----|---|----|--------------------------|----|--|----|---------------|----|----|----|---------|----|--|----|-------|---|---|----|-----|---|---|----|------------------|----|----|----|
| <i>Neighbors (Соседние точки доступа)</i> | <p>Точки доступа, являющиеся соседними по отношению к одной или нескольким кластеризованным точкам доступа, перечислены в левом столбце по идентификатору SSID (сетевому имени). Точка доступа, определенная как соседняя по отношению к члену кластера, сама может быть членом кластера. Соседние точки доступа, являющиеся членами кластера, всегда отображаются вверху списка под жирной чертой и содержат индикатор местоположения.</p> <p>Цветные полосы справа от каждой соседней точки доступа в списке показывают мощность ее сигнала, определенную членом кластера, чей IP-адрес показан в верхней части столбца:</p> <p>Эту точку доступа (член кластера) может видеть точка доступа с IP-адресом 10.10.100.246 (при мощности сигнала 54). . .</p> <p>. . . но не точка доступа с IP-адресом 10.10.100.223</p> <table><tr><th rowspan="2">Neighbors (88)</th><th colspan="3">Cluster</th></tr><tr><th>10.10.100.246 (not set)</th><th>10.10.100.223 (not set)</th><th>10.10.100.213 (not set)</th></tr><tr><td>TEKLOGIX... (not set)</td><td></td><td>3</td><td>48</td></tr><tr><td>TEKLOGIX... (not set)</td><td></td><td></td><td></td></tr><tr><td>TEKLOGIX... (not set)</td><td>54</td><td>0</td><td></td></tr><tr><td>TEKLOGIX... (not set)</td><td>34</td><td>5</td><td>26</td></tr><tr><td>TEKLOGIX... (not set)</td><td>22</td><td></td><td>50</td></tr><tr><td>Bread Lab 105</td><td>20</td><td>18</td><td>27</td></tr><tr><td>wi-fi-a</td><td>46</td><td></td><td>34</td></tr><tr><td>guest</td><td>4</td><td>6</td><td>48</td></tr><tr><td>int</td><td>4</td><td>5</td><td>48</td></tr><tr><td>g10_wgt624_guest</td><td>21</td><td>14</td><td>33</td></tr></table> | Neighbors (88) | Cluster | | | 10.10.100.246 (not set) | 10.10.100.223 (not set) | 10.10.100.213 (not set) | TEKLOGIX... (not set) | | 3 | 48 | TEKLOGIX... (not set) | | | | TEKLOGIX... (not set) | 54 | 0 | | TEKLOGIX... (not set) | 34 | 5 | 26 | TEKLOGIX... (not set) | 22 | | 50 | Bread Lab 105 | 20 | 18 | 27 | wi-fi-a | 46 | | 34 | guest | 4 | 6 | 48 | int | 4 | 5 | 48 | g10_wgt624_guest | 21 | 14 | 33 |
| Neighbors (88) | Cluster | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 10.10.100.246 (not set) | 10.10.100.223 (not set) | 10.10.100.213 (not set) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TEKLOGIX... (not set) | | 3 | 48 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TEKLOGIX... (not set) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TEKLOGIX... (not set) | 54 | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TEKLOGIX... (not set) | 34 | 5 | 26 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TEKLOGIX... (not set) | 22 | | 50 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bread Lab 105 | 20 | 18 | 27 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| wi-fi-a | 46 | | 34 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| guest | 4 | 6 | 48 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| int | 4 | 5 | 48 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g10_wgt624_guest | 21 | 14 | 33 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <ul style="list-style-type: none">• Темно-синяя полоса — темно-синяя полоса и высокий уровень мощности сигнала (например, 50) означает хороший уровень сигнала, обнаруженный у соседней точки доступа, видимой для точки доступа с IP-адресом, указанным над этим столбцом.• Светло-синяя полоса — светло-синяя полоса и пониженный уровень мощности сигнала (например, 20 или ниже) означает средний или слабый уровень сигнала, обнаруженный у соседней точки доступа, видимой для точки доступа с IP-адресом, указанным над этим столбцом.• Белая полоса — белая полоса и цифра 0 означает, что соседняя точка доступа, обнаруженная одним из членов кластера, не может быть обнаружена точкой доступа IP-адресом, указанным над этим столбцом.• Светло-серая полоса — светло-серая полоса и отсутствие сигнала означает, что соседняя точка доступа была обнаружена другим членом кластера, но не тем, чей IP-адрес указан над этим столбцом.• Темно-серая полоса — темно-серая полоса и отсутствие сигнала означает, что это точка доступа, чей IP-адрес указан над этим столбцом (так как невозможно показать, как точка доступа может обнаружить саму себя). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

9.4 Просмотр сведений о члене кластера

Чтобы просмотреть сведения о точке доступа, являющейся членом кластера, нажмите IP address (IP-адрес) члена кластера вверху экрана.

Рис. 9.2 Просмотр сведений о точке доступа, являющейся членом кластера

View neighboring access points

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ☐ In cluster ☐ Not in cluster ☒ Both

Cluster

10.10.100.245
00:00:04:7F:00:00
(Vicky's Office - lower shelf)

10.10.100.238
00:0C:41:16:A3:12
(Vicky's Office - top shelf)

Neighbors (10)

| | | |
|-------------------------------|----|----|
| Vicky's Network (WIP-bld-48b) | | 45 |
| Vicky's Network (WIP-bld-48b) | 51 | |
| IOMEGA_NAS | 37 | 49 |
| TEKLOGIX... | 22 | |
| novatec | | |
| Pronghorn 2.0.2 | | 20 |
| tsunami | 18 | 10 |
| tsunami | 54 | 42 |
| BradLabNetwork | 11 | |
| Ray's GW 7001 2.0.3 | | 17 |

Neighbor Details

10.10.100.245

| SSID | MAC Address | Channel | Rate | Signal | Beacon Interval | Beacon Age |
|-------------------------------|-------------------|---------|------|--------|-----------------|------------|
| IOMEGA_NAS | 00:03:2F:27:4E:EE | 1 | 10 | 37 | 100 | 74203 |
| TEKLOGIX... | 00:0C:41:0A:30:3E | 6 | 10 | 22 | 100 | 74203 |
| Vicky's Network (WIP-bld-48b) | 00:0C:41:16:A3:12 | 2 | 10 | 51 | 100 | 74203 |
| novatec | 00:0E:81:01:01:1A | 6 | 10 | -4 | 100 | 74203 |
| tsunami | 00:13:5F:56:E8:00 | 10 | 10 | 18 | 100 | 74203 |
| tsunami | 00:14:A8:36:28:40 | 4 | 10 | 54 | 100 | 74203 |

Clustered

2 Access Points

3 User Accounts

В таблице ниже приведены сведения, отображаемые для выбранной точки доступа.

Табл. 9.2 Информация о точке доступа

| Поле | Описание |
|--|--|
| <i>SSID</i> | <p>Идентификатор набора служб (SSID) для точки доступа.</p> <p>SSID — это буквенно-цифровая строка, состоящая не более чем из 32 символов, которая является уникальным идентификатором беспроводной локальной сети. Она также называется «<i>Network Name</i>» (<i>Сетевое имя</i>).</p> <p>Настройка SSID выполняется в разделе «Basic Settings» (Базовые параметры) (Гл. 5: «Настройка базовых параметров») или в меню <i>Manage (Управление) > 802.11 Settings (Параметры 802.11)</i> (Гл. 13: «Настройка беспроводного интерфейса»).</p> <p>Гостевая и внутренняя сети, работающие на той же точке доступа, должны иметь разные сетевые имена.</p> |
| <i>MAC Address (MAC-адрес)</i> | <p>Показывает MAC-адрес соседней точки доступа.</p> <p>MAC-адрес — это аппаратный адрес, являющийся уникальным идентификатором каждого узла сети.</p> |
| <i>Channel (Канал)</i> | <p>Показывает текущий канал вещания точки доступа.</p> <p>Канал определяет часть спектра радиоволн, которую радиомодуль использует для передачи и получения данных.</p> <p>Настройка канала выполняется в меню <i>Manage (Управление) > 802.11 Advanced Settings (Расширенные параметры 802.11)</i>. (См. Гл. 16: «Настройка параметров радиомодуля 802.11».)</p> |
| <i>Rate (Скорость)</i> | <p>Показывает скорость (в мегабитах в секунду) передачи данных точки доступа.</p> <p>Текущая скорость всегда будет одной из скоростей, указанных в разделе <i>Supported Rates (Поддерживаемые скорости)</i>.</p> |
| <i>Signal (Сигнал)</i> | <p>Указывает силу радиосигнала, исходящего из точки доступа, в децибелах (дБ).</p> |
| <i>Beacon Interval (Интервал маячка)</i> | <p>Показывает интервал маячка (см. Маячок), используемый данной точкой доступа.</p> <p>Точка доступа передает кадры маячка через равные промежутки времени, объявляя о существовании беспроводной сети. По умолчанию передается один кадр маячка каждые 100 миллисекунд (или 10 в секунду).</p> <p>Интервал маячка устанавливается на вкладке <i>Manage (Управление) > 802.11 Advanced Settings (Расширенные параметры 802.11)</i> (см. Гл. 16: «Настройка параметров радиомодуля 802.11»).</p> |
| <i>Capability (Емкость)</i> | <p>Шестнадцатеричное число, которое после конвертации в двоичное определяет все функции и возможности IEEE 802.11, а также их состояние («вкл.» или «выкл.») для данной точки доступа.</p> |
| <i>Beacon Age (Последний маячок)</i> | <p>Показывает дату и время последнего маячка, переданного точкой доступа.</p> |

НАСТРОЙКА РЕЖИМОВ БЕЗОПАСНОСТИ

10

| | |
|---|-----|
| 10.1 Общие сведения о проблемах безопасности в беспроводных сетях | 99 |
| 10.1.1 Какой режим безопасности использовать? | 99 |
| 10.1.2 Сравнение режимов безопасности для алгоритмов управления ключами, аутентификации и шифрования | 100 |
| 10.1.2.1 Использование режима без шифрования (система безопасности отключена) | 101 |
| 10.1.2.2 Использование статического WEP-шифрования | 101 |
| 10.1.2.3 Использование стандарта IEEE 802.1x | 103 |
| 10.1.2.4 Использование режима безопасности WPA Personal | 104 |
| 10.1.2.5 Использование режима безопасности WPA Enterprise | 105 |
| 10.1.3 Повышается ли уровень защиты при запрете широковещательного идентификатора SSID? | 107 |
| 10.1.4 Как изоляция станции защищает сеть? | 107 |
| 10.2 Настройка параметров безопасности | 107 |
| 10.2.1 Широковещательный SSID, изоляция станции и режим безопасности | 108 |
| 10.2.2 Режимы безопасности | 110 |
| 10.2.2.1 None (Plain-text) (Нет (Простой текст)) | 110 |
| 10.2.2.2 Static WEP (Статическое WEP-шифрование) | 111 |
| 10.2.2.3 IEEE 802.1x | 116 |
| 10.2.2.4 WPA Personal | 119 |
| 10.2.2.5 WPA Enterprise | 122 |
| 10.3 Обновление параметров | 127 |

В данном разделе представлена информация о настройке параметров безопасности на беспроводном шлюзе 9160 G2 Wireless Gateway.

10.1 Общие сведения о проблемах безопасности в беспроводных сетях

Беспроводные средства связи по определению являются менее безопасными по сравнению с проводными. Например, сетевая плата Ethernet (*NIC*) передает пакеты данных по физическому каналу — коаксиальному кабелю или витой паре. Беспроводная сетевая плата передает радиосигналы в эфире, и подключение к беспроводной сети происходит без физического доступа и сложного оборудования. Даже начинающему хакеру достаточно ноутбука и беспроводной сетевой платы, чтобы взломать беспроводную сеть. Для этого даже не нужно находиться в стандартной зоне покрытия точки доступа. С помощью современной антенны на клиентском устройстве хакер может подключиться к сети на значительном расстоянии.

Беспроводной шлюз 9160 G2 Wireless Gateway предлагает несколько схем аутентификации и шифрования для обеспечения доступа к беспроводной инфраструктуре только авторизованными пользователями. Подробная информация о каждом режиме безопасности представлена в разделах ниже.

См. также Прил. В: «Параметры безопасности на беспроводных клиентах/RADIUS-сервере».

10.1.1 Какой режим безопасности использовать?

Как правило, во внутренней сети рекомендуется использовать самый строгий из доступных режим безопасности. При настройке системы безопасности на точке доступа сначала необходимо выбрать режим безопасности, а затем — алгоритм аутентификации (для некоторых режимов), а также определить, разрешается ли подключение клиентам, не использующим определенный режим безопасности.

Защищенный доступ Wi-Fi (WPA) с наличием службы идентификации удаленных пользователей (*RADIUS*), использующий алгоритм шифрования CCMP (AES), обеспечивает наиболее полную защиту данных и является лучшим выбором, если все клиентские станции оборудованы модулями запроса WPA. Однако во избежание проблем обратной совместимости и взаимодействия с клиентами или другими точками доступа может потребоваться настройка WPA с RADIUS при помощи другого алгоритма шифрования или выбор другого режима безопасности.

Тем не менее, следует учитывать, что в некоторых типах сетей безопасность может не являться приоритетом. Если вы просто предоставляете доступ к сети Интернет или сетевому принтеру, например в гостевой сети, оптимальным выбором может быть выбор значения режима безопасности *None (Plain-text) (Нет (простой текст))*. Чтобы исключить случайное обнаружение и подключение к вашей сети клиентских устройств, можно отключить широковещательный идентификатор SSID для скрытия имени сети в списке доступных сетей. Изоляция сети и предотвращение доступа к конфиденциальной информации может быть достаточной защитой в некоторых ситуациях. Для гостевых сетей предлагается только этот уровень защиты. Он также может быть компромиссным решением для ряда других сценариев, где приоритетом является простота подключения клиентских устройств (см. раздел «Повышается ли уровень защиты при запрете широковещательного идентификатора SSID?» на стр. 107).

Ниже представлен краткий обзор факторов, влияющих на уровень безопасности разных режимов, описание режимов безопасности и условий их использования.

10.1.2 Сравнение режимов безопасности для алгоритмов управления ключами, аутентификации и шифрования

Эффективность протокола безопасности определяется тремя основными факторами:

- способом, который использует протокол для управления ключами;
- наличием или отсутствием в протоколе интегрированной аутентификации пользователей;
- алгоритмом или формулой шифрования, который использует протокол для кодирования и декодирования данных.

Ниже представлен список режимов безопасности, доступных на беспроводном шлюзе 9160 G2 Wireless Gateway, а также описание алгоритмов управления ключами, аутентификации и шифрования, используемых в каждом режиме. Мы включили некоторые рекомендации по использованию режимов безопасности в разных сценариях.

- «Использование режима без шифрования (система безопасности отключена)» на стр. 101.
- «Использование статического WEP-шифрования» на стр. 101.
- «Использование стандарта IEEE 802.1x» на стр. 103.
- «Использование режима безопасности WPA Personal» на стр. 104.
- «Использование режима безопасности WPA Enterprise» на стр. 105.

10.1.2.1 Использование режима без шифрования (система безопасности отключена)

При выборе значения режима безопасности *None (Plain-text)* (*Нет (простой текст)*) система безопасности будет отключена. В этом режиме данные в сети передаются не в зашифрованном виде, а как «простой текст». Алгоритмы управления ключами, шифрования данных и аутентификации пользователей не используются.

Рекомендации

Не рекомендуется использовать режим безопасности без шифрования, т.е. выбирать значение «None (Plain-text)» (Нет (простой текст)), как основной режим для внутренней сети, так как он не является безопасным. Это единственный режим, который можно использовать в гостевой сети, которая по определению является небезопасной LAN, всегда виртуально или физически отделенной от конфиденциальной информации внутренней LAN.

Следовательно, значение режима безопасности *None (Plain-text)* (*Нет (простой текст)*) следует использовать только в гостевой сети, а также во внутренней сети на этапах настройки, тестирования и устранения неисправностей.

Дополнительные сведения

Для получения информации о настройке режима безопасности без шифрования см. раздел «None (Plain-text) (Нет (Простой текст))» на стр. 110.

10.1.2.2 Использование статического WEP-шифрования

Статический эквивалент конфиденциальности проводных сетей (*WEP*) — это протокол шифрования данных для беспроводных сетей 802.11. Все беспроводные станции и точки доступа в сети настраиваются с помощью статического 64-разрядного общего ключа (40-разрядный секретный ключ + 24-разрядный вектор инициализации (IV)) или 128-разрядного общего ключа (104-разрядный секретный ключ + 24-разрядный вектор инициализации) для шифрования данных.

Табл. 10.1 Режим статического WEP-шифрования

| Управление ключами | Алгоритм шифрования | Аутентификация пользователей |
|---|--|---|
| <p>При статическом WEP-шифровании используется фиксированный ключ, предоставляемый администратором. Каждый ключ WEP имеет несколько вариантов порядкового номера (индекса) (на беспроводном шлюзе 9160 G2 Wireless Gateway доступно до четырех вариантов).</p> <p>Чтобы получить доступ к данным на точке доступа, клиентская станция должна иметь аналогичный ключ с тем же индексом.</p> | <p>Поточное шифрование RC4 используется для шифрования тела кадра и периодической проверки резервирования (CRC) каждого кадра 802.11.</p> | <p>При установке значения алгоритма аутентификации «Shared Key» (Общий ключ) данный протокол предоставляет механизм аутентификации пользователя в элементарной форме.</p> <p>При установке значения алгоритма аутентификации «Open System» (Открытая система) аутентификация пользователей не выполняется.</p> <p>При установке значения «Both» (Все) аутентификация выполняется только для WEP-клиентов.</p> |

Рекомендации

Статическое WEP-шифрование предназначалось для обеспечения уровня безопасности, соблюдаемого при отправке незашифрованных данных через подключение Ethernet, однако за счет большого количества уязвимостей этот протокол не обеспечивает должную защиту даже на заявленном уровне.

В связи с этим не рекомендуется использовать **статическое WEP-шифрование** в качестве режима безопасности. Единственным случаем использования статического WEP-шифрования может быть ситуация, когда в силу проблем взаимодействия доступен только этот режим безопасности, и вас не беспокоит потенциальное раскрытие данных в вашей сети.

Дополнительные сведения

Для получения информации о настройке режима безопасности с использованием статического WEP-шифрования см. раздел «Static WEP (Статическое WEP-шифрование)» на стр. 111.

10.1.2.3 Использование стандарта IEEE 802.1x

IEEE 802.1x — это стандарт для передачи расширяемого протокола аутентификации (*EAP*) по беспроводной сети 802.11 с использованием протокола передачи EAP-сообщений в стандарте 802.1x (EAP Encapsulation Over LANs, EAPOL). Это новый, более безопасный стандарт по сравнению со статическим WEP-шифрованием.

Табл. 10.2 Режим безопасности IEEE 801.1x

| Управление ключами | Алгоритм шифрования | Аутентификация пользователей |
|--|--|---|
| <p>В режиме безопасности IEEE 802.1x используются динамически генерируемые ключи, которые периодически обновляются.</p> <p>Для каждой станции используются разные одноадресные ключи (см. Одноадресная передача).</p> | <p>Поточное шифрование RC4 используется для шифрования тела кадра и периодической проверки резервирования (CRC) каждого кадра 802.11.</p> | <p>Режим IEEE 802.1x поддерживает ряд методов аутентификации, таких как сертификаты, Kerberos и аутентификация с использованием открытого ключа через RADIUS-сервер.</p> <p>Вы можете использовать встроенный RADIUS-сервер беспроводного шлюза 9160 G2 Wireless Gateway или внешний RADIUS-сервер. Встроенный RADIUS-сервер поддерживает защищенный расширяемый протокол аутентификации (Protected EAP, PEAP) и протокол MSCHAP V2.</p> |

Рекомендации

Режим IEEE 802.1x является лучшим выбором, чем статическое WEP-шифрование, из-за динамической генерации ключей и их периодического изменения. Однако используемый алгоритм шифрования аналогичен алгоритму, применяемому при статическом WEP-шифровании, и поэтому является менее надежным, чем улучшенные методы шифрования, такие как **TKIP** и **CCMP (AES)**, используемые в стандарте *защищенного доступа Wi-Fi* (Wi-Fi Protected Access, **WPA**) или **WPA2**.

Кроме того, возможно возникновение проблем совместимости из-за различных поддерживаемых методов аутентификации и отсутствия стандартного метода внедрения.

Поэтому режим IEEE 802.1x не является таким же безопасным решением как *защищенный доступ Wi-Fi (WPA)* или **WPA2**. Если вы не можете использовать **WPA** по причине отсутствия WPA на клиентских станциях, лучшим решением вместо применения режима IEEE 802.1x будет использование **режима WPA Enterprise**.

При наличии в сети внешнего RADIUS-сервера рекомендуется использовать его вместо встроенного RADIUS-сервера на точке доступа. Внешний RADIUS-сервер обеспечит более высокий уровень безопасности, чем локальный сервер аутентификации.

Дополнительные сведения

Для получения информации о настройке режима безопасности IEEE 802.1х см. раздел «IEEE 802.1х» на стр. 116.

10.1.2.4 Использование режима безопасности WPA Personal

В режиме безопасности *WPA Personal* *предварительный ключ (PSK)* является реализацией стандарта Wi-Fi Alliance IEEE *802.11h*, который включает в себя *улучшенный алгоритм шифрования (AES)*, *режим гаммирования/протокол CBC-MAC (CCMP)* и *протокол шифрования с использованием временных ключей (TKIP)*. В этом режиме используются те же алгоритмы шифрования, что и в режиме WPA 2 с RADIUS, но без возможности интеграции RADIUS-сервера для аутентификации пользователей.

Данный режим безопасности имеет обратную совместимость для беспроводных клиентов, которые поддерживают только оригинальный *WPA*.

Табл. 10.3 Режим безопасности WPA Personal

| Управление ключами | Алгоритмы шифрования | Аутентификация пользователей |
|---|---|--|
| <p>В режиме безопасности WPA Personal используются динамически генерируемые ключи, которые периодически обновляются.</p> <p>Для каждой станции используются разные одноадресные ключи (см. <i>Одноадресная передача</i>).</p> | <ul style="list-style-type: none">• Протокол шифрования с использованием временных ключей (<i>TKIP</i>).• Режим гаммирования/протокол CBC-MAC (<i>CCMP</i>), усовершенствованный стандарт шифрования (<i>AES</i>). | <p>Использование предварительного ключа (<i>PSK</i>) дает возможность аутентификации пользователей аналогично предварительным ключам в <i>WEP</i>.</p> |

Рекомендации

WPA Personal не рекомендуется использовать с беспроводным шлюзом 9160 G2 Wireless Gateway, если доступен режим WPA Enterprise.

При наличии такой возможности рекомендуется использование режима WPA Enterprise, если нет проблем взаимодействия оборудования при использовании этого режима.

Например, некоторые устройства в сети могут не поддерживать WPA или WPA2 с *EAP*, осуществляющим связь с *RADIUS*-сервером. Встроенные серверы принтеров или другие небольшие клиентские устройства с ограниченными возможностями внедрения могут не поддерживать RADIUS. В таких случаях рекомендуется использовать режим WPA Personal.

Дополнительные сведения

Для получения информации о настройке данного режима безопасности см. раздел «WPA Personal» на стр. 119.

10.1.2.5 Использование режима безопасности WPA Enterprise

Режим безопасности WPA Enterprise с использованием службы идентификации удаленных пользователей (*RADIUS*) является реализацией стандарта Wi-Fi Alliance IEEE 802.11h, который включает в себя усовершенствованный стандарт шифрования (*AES*), режим гаммирования/протокол CBC-MAC (*CCMP*) и протокол шифрования с использованием временных ключей (*TKIP*). Этот режим требует использования RADIUS-сервера для аутентификации пользователей. Режим WPA Enterprise обеспечивает наилучшую защиту беспроводных сетей.

Также данный режим безопасности имеет обратную совместимость для беспроводных клиентов, которые поддерживают только оригинальный *WPA*.

Табл. 10.4 Режим безопасности WPA Enterprise

| Управление ключами | Алгоритмы шифрования | Аутентификация пользователей |
|---|---|--|
| <p>В режиме безопасности WPA Enterprise используются динамически генерируемые ключи, которые периодически обновляются.</p> <p>Для каждой станции используются разные одноадресные ключи (см. <i>Одноадресная передача</i>).</p> | <ul style="list-style-type: none">• Протокол шифрования с использованием временных ключей (<i>TKIP</i>).• Режим гаммирования/протокол CBC-MAC (<i>CCMP</i>), усовершенствованный стандарт шифрования (<i>AES</i>). | <p>Служба идентификации удаленных пользователей (<i>RADIUS</i>)</p> <p>Вы можете использовать встроенный RADIUS-сервер беспроводного шлюза 9160 G2 Wireless Gateway или внешний RADIUS-сервер. Встроенный RADIUS-сервер поддерживает защищенный расширяемый протокол аутентификации (Protected <i>EAP</i>, PEAP) и протокол MSCHAP V2.</p> |

Рекомендации

WPA Enterprise является **рекомендованным режимом безопасности**. Алгоритмы шифрования *CCMP (AES)* и *TKIP*, используемые с режимами WPA, являются намного более совершенными по сравнению с алгоритмом *RC4*, используемым в режимах статического шифрования *WEP* или IEEE 802.1x. Поэтому по возможности должны применяться алгоритмы CCMP (AES) или TKIP. Все режимы WPA позволяют использовать эти схемы шифрования, и поэтому прежде всего рекомендуется использовать эти режимы при наличии варианта WPA. Кроме того, этот режим включает RADIUS-сервер для аутентификации пользователей, что дает ему преимущество перед режимом безопасности WPA Personal.

При наличии в сети внешнего RADIUS-сервера рекомендуется использовать его вместо встроенного RADIUS-сервера на точке доступа. Внешний RADIUS-сервер обеспечит более высокий уровень безопасности, чем локальный сервер аутентификации.

Следуйте изложенным ниже рекомендациям при выборе параметров режима безопасности WPA Enterprise:

1. На сегодняшний день лучшей защитой беспроводной сети является использование режима безопасности WPA Enterprise с алгоритмом шифрования CCMP (AES). Алгоритм AES — это симметричный 128-разрядный метод шифрования блоков данных, который работает на разных уровнях сети. Это самая эффективная система шифрования, доступная в настоящее время для беспроводных сетей. Если все клиенты или другие точки доступа в сети совместимы с протоколом WPA/CCMP, используйте этот алгоритм шифрования (если все клиенты совместимы с протоколом WPA2, используйте только поддержку клиентов WPA2).
2. Вторым по надежности режимом безопасности является WPA Enterprise с совместным использованием алгоритмов шифрования TKIP и CCMP. Он позволяет клиентам WPA устанавливать связь друг с другом без поддержки CCMP, использует протокол TKIP для шифрования многоадресных (см. *Многоадресная передача*) и широковещательных (см. *Широковещательная передача*) кадров и разрешает клиентам выбирать между CCMP и TKIP для шифрования одноадресных (см. *Одноадресная передача*) кадров (от точки доступа к одной станции). Эта конфигурация WPA обеспечивает более высокий уровень взаимодействия за счет некоторого снижения уровня защиты. Клиентские станции с поддержкой CCMP могут использовать его для шифрования своих одноадресных (см. *Одноадресная передача*) кадров. При возникновении проблем взаимодействия при передаче данных от точки доступа к станции с использованием параметра алгоритма шифрования «Both» (Все) необходимо выбрать алгоритм TKIP (см. следующий параметр).
3. Третьим по надежности режимом безопасности является WPA Enterprise с алгоритмом шифрования *TKIP*. На некоторых клиентах могут возникать проблемы взаимодействия при одновременном использовании протоколов CCMP и TKIP. В таких случаях в качестве алгоритма шифрования требуется выбрать TKIP. Это стандартный режим WPA, который является наилучшим с точки зрения взаимодействия с параметрами безопасности клиентского беспроводного программного обеспечения. TKIP — единственный алгоритм шифрования, прошедший сертификацию *Wi-Fi WPA*.

Дополнительные сведения

Для получения информации о настройке данного режима безопасности см. раздел «WPA Enterprise» на стр. 122.

10.1.3 Повышается ли уровень защиты при запрете широковещательного идентификатора SSID?

Вы можете выключить (запретить) широковещательную трансляцию, чтобы станции не смогли автоматически обнаружить вашу точку доступа. Если передача широковещательного идентификатора SSID точки доступа запрещена, сетевое имя не будет отображаться в списке доступных сетей на клиентской станции. В этом случае для подключения к точке доступа в модуле запроса клиента должно быть указано точное сетевое имя.

Запрет широковещательного идентификатора SSID предотвращает случайное подключение клиентов к вашей сети, но не защищает даже от простейших попыток несанкционированного подключения или мониторинга незашифрованного трафика.

Это обеспечивает самый минимальный уровень защиты в так или иначе обнаруживаемой сети (например, гостевой сети), где приоритетом является простота подключения клиентов и отсутствуют конфиденциальные данные.

См. также раздел «Гостевая сеть» на стр. 110.

10.1.4 Как изоляция станции защищает сеть?

Если *изоляция станции* включена, точка доступа блокирует связь между беспроводными клиентами. Через точку доступа может передаваться трафик между беспроводными клиентами и проводными устройствами в сети, но не между беспроводными клиентами.

Также блокируется трафик, передаваемый беспроводными клиентами, подключенными к сети через ссылки *WDS*. Эти клиенты не могут взаимодействовать друг с другом при включенной изоляции станции.

См. Гл. 20: «Распределенная беспроводная система» для получения дополнительной информации о WDS.

10.2 Настройка параметров безопасности

Чтобы настроить режим безопасности, перейдите на вкладку *Security* (*Безопасность*) и внесите изменения в настройки, как указано ниже.

Рис. 10.1 Экран параметров безопасности

| | |
|-----------------------|--|
| Basic Settings | <h3>Modify Internal Network security settings</h3> <p><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</p> <p>Mode: WPA Personal</p> <p>WPA Versions: <input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2</p> <p>Cipher Suites: <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES)</p> <p>Key: reoreore</p> <p>Update</p> |
| User Management | |
| Cluster | |
| Access Points | |
| Sessions | |
| Channel Management | |
| Wireless Neighborhood | |
| Security | |
| Status | |
| Interfaces | |
| | |
| | |
| | |

Приведенная ниже информация о конфигурации описывает процесс настройки режимов безопасности на точке доступа. Помните, что для возможности обмена данными с точкой доступа на каждом беспроводном клиенте должен быть настроен аналогичный режим безопасности, а параметры ключей шифрования должны соответствовать режиму безопасности точки доступа.

На точке доступа с двумя радиомодулями данные параметры безопасности применимы к обоим радиомодулям.



Примечание. Все режимы безопасности, кроме «Plain-text» (Простой текст), используются только в конфигурации внутренней сети. В гостевой сети используется только режим «Plain-text» (Простой текст) (для получения дополнительной информации о гостевых сетях см. Гл. 14: «Настройка гостевого доступа»).

10.2.1 Широковещательный SSID, изоляция станции и режим безопасности

Для настройки системы безопасности на точке доступа выберите режим безопасности и заполните соответствующие поля, как описано в Табл. 10.5.

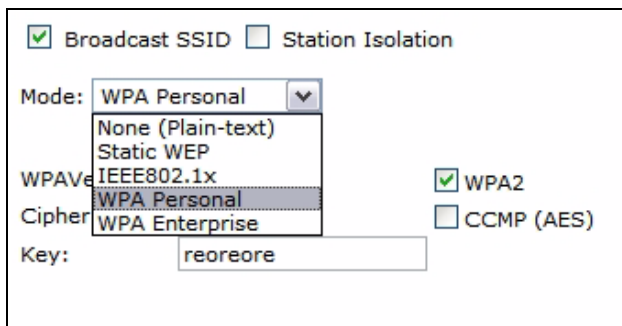


Примечание. В качестве дополнительных мер безопасности вы также можете разрешить или запретить трансляцию идентификатора SSID и включить/выключить изоляцию станции, как описано в Табл. 10.5 на стр. 109.

Табл. 10.5 Параметры безопасности

| Поле | Описание |
|---|--|
| <i>Broadcast SSID</i> (Широковещательный идентификатор SSID) | <p>Чтобы включить широковещательный идентификатор SSID, установите соответствующий флажок. По умолчанию точка доступа транслирует (разрешает передачу) идентификатора набора служб (SSID) в кадрах маячка.</p> <p>Вы можете выключить (запретить) широковещательную трансляцию, чтобы станции не смогли автоматически обнаружить вашу точку доступа. Если передача широковещательного идентификатора SSID точки доступа запрещена, сетевое имя не будет отображаться в списке доступных сетей на клиентской станции. В этом случае для подключения к точке доступа в модуле запроса клиента должно быть указано точное сетевое имя.</p> |
| <i>Station Isolation</i> (Изоляция станции) | <p>Чтобы включить изоляцию станции, установите соответствующий флажок.</p> <ul style="list-style-type: none"> Если изоляция станции <i>отключена</i>, беспроводные клиенты могут устанавливать связь друг с другом в обычном режиме, передавая трафик через точку доступа. Если изоляция станции <i>включена</i>, точка доступа блокирует связь между беспроводными клиентами. Через точку доступа может передаваться трафик между беспроводными клиентами и проводными устройствами в сети, но не между беспроводными клиентами. Также блокируется трафик, передаваемый беспроводными клиентами, подключенными к сети через ссылки WDS. Эти клиенты не могут взаимодействовать друг с другом при включенной изоляции станции. См. Гл. 20: «Распределенная беспроводная система» для получения дополнительной информации о WDS. |
| <i>Security Mode</i> (Режим безопасности) | <p>Выберите <i>режим безопасности</i>. Доступны следующие варианты:</p> <ul style="list-style-type: none"> «None (Plain-text) (Нет (Простой текст))» на стр. 110. «Static WEP (Статическое WEP-шифрование)» на стр. 111. «IEEE 802.1x» на стр. 116. «WPA Personal» на стр. 119. «WPA Enterprise» на стр. 122. <p>Для гостевой сети используется только режим безопасности «None (Plain-text)» (Нет (Простой текст)) (для получения дополнительной информации см. Гл. 14: «Настройка гостевого доступа»).</p> <p>Все режимы безопасности, кроме «None (Plain-text)» (Нет (Простой текст)), используются только в конфигурации внутренней сети.</p> |

10.2.2 Режимы безопасности



10.2.2.1 None (Plain-text) (Нет (Простой текст))

Отсутствие режима безопасности (или режим безопасности «простой текст») означает, что все данные, передаваемые и получаемые беспроводным шлюзом 9160 G2 Wireless Gateway, являются незашифрованными.

При выборе параметра *None (Plain-text) (Нет (Простой текст))* точка доступа не имеет дополнительных настраиваемых параметров. Этот режим безопасности может быть использован при первоначальной настройке сети или для устранения проблем, однако он не рекомендуется к регулярному использованию во внутренней сети по причине недостаточного уровня защиты.

Гостевая сеть

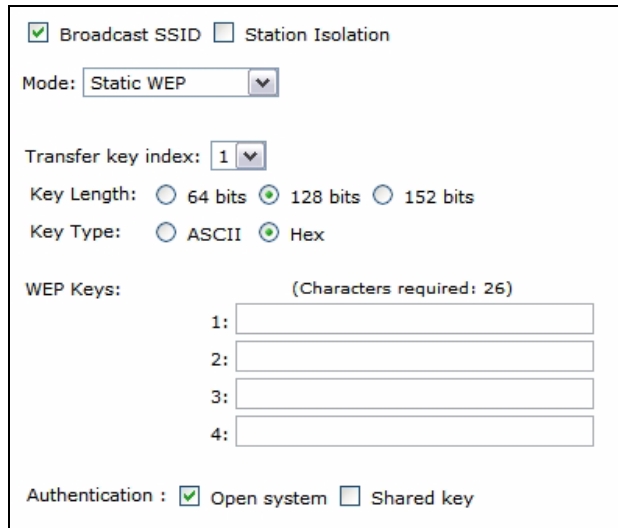
Для работы гостевой сети, которая по определению является легко доступной и небезопасной *LAN*, всегда виртуально или физически отделенной от конфиденциальных данных внутренней LAN, можно установить только режим безопасности «None (Plain-text)» (Нет (Простой текст)). Например, гостевая сеть может использоваться для предоставления доступа к сети Интернет или принтеру для посетителей.

Отсутствие режима безопасности на гостевой точке доступа обеспечивает легкое подключение к сети для гостей без необходимости настройки параметров безопасности на их клиентских устройствах.

Для обеспечения минимального уровня защиты гостевой сети вы можете отключить (запретить) широковещательную трансляцию идентификатора SSID (сетевое имя), чтобы клиентские станции не смогли автоматически обнаружить вашу точку доступа (см. также раздел «Повышается ли уровень защиты при запрете широковещательного идентификатора SSID?» на стр. 107).

Для получения дополнительной информации о гостевых сетях см. Гл. 14: «Настройка гостевого доступа».

10.2.2.2 Static WEP (Статическое WEP-шифрование)



☒ Broadcast SSID ☐ Station Isolation

Mode: Static WEP

Transfer key index: 1

Key Length: ☐ 64 bits ☒ 128 bits ☐ 152 bits

Key Type: ☐ ASCII ☒ Hex

WEP Keys: (Characters required: 26)

1:

2:

3:

4:

Authentication : ☒ Open system ☐ Shared key

Эквивалент конфиденциальности проводных сетей (*WEP*) — это протокол шифрования данных для беспроводных сетей 802.11. Все беспроводные станции и точки доступа в сети настраиваются с помощью статического 64-разрядного общего ключа (40-разрядный секретный ключ + 24-разрядный вектор инициализации (IV)) или 128-разрядного общего ключа (104-разрядный секретный ключ + 24-разрядный вектор инициализации) для шифрования данных. Нельзя комбинировать 64-разрядные и 128-разрядные ключи WEP точек доступа и клиентских станций.

Статическое WEP-шифрование является не самым безопасным режимом, но обеспечивает более высокий уровень защиты, чем режим безопасности «None (Plain-text)» (Нет (Простой текст)), так как предотвращает получение доступа к незашифрованному беспроводному трафику несанкционированными лицами. Для получения дополнительной информации о режимах безопасности см. разделы «IEEE 802.1x» на стр. 116, «WPA Personal» на стр. 119 или «WPA Enterprise» на стр. 122.

Протокол WEP зашифровывает данные, передаваемые по беспроводной сети, с помощью статического ключа (используемый алгоритм шифрования — потоковое шифрование RC4). Точка доступа использует ключ для передачи данных клиентским станциям. Каждая клиентская станция должна использовать аналогичный ключ для декодирования данных, которые она получает от точки доступа.

Клиентские станции могут использовать другие ключи для передачи данных точке доступа. Все они также могут использовать один и тот же ключ, но это снижает уровень защиты, так как означает, что одна станция может декодировать данные, отправленные другой. При выборе режима безопасности *Static WEP (Статическое WEP-шифрование)* необходимо предоставить информацию о параметрах точки доступа, как показано на рисунке ниже и описано в Табл. 10.6 на стр. 112.

Табл. 10.6 Параметры безопасности режима «Static WEP» (Статическое WEP-шифрование)

| Поле | Описание |
|--|---|
| <i>Transfer Key Index (Индекс передаточного ключа)</i> | Выберите индекс ключа из раскрывающегося меню. Доступны индексы от 1 до 4. Индекс по умолчанию: 1. Индекс передаточного ключа указывает, какой ключ WEP будет использовать точка доступа для шифрования передаваемых данных. |
| <i>Key Length (Длина ключа)</i> | Укажите длину ключа, выбрав один из переключателей: <ul style="list-style-type: none">• 64 бита• 128 бит |
| <i>Key Type (Тип ключа)</i> | Укажите тип ключа, выбрав один из переключателей: <ul style="list-style-type: none">• ASCII• Hex (Шестнадцатеричное значение) |
| <i>Characters Required (Количество символов)</i> | Указывает количество обязательных символов в ключе WEP. Количество обязательных символов автоматически обновляется при выборе длины и типа ключа. |
| <i>WEP Keys (Ключи WEP)</i> | Можно указать не более четырех ключей WEP. Введите строку символов ключа в каждое текстовое поле. Если вы выбрали тип «ASCII», введите любую комбинацию целых чисел и букв: 0-9, a-z и A-Z. Если вы выбрали тип «HEX», введите шестнадцатеричные цифры (любую комбинацию 0-9 и a-f или A-F). Количество символов в каждом ключе должно совпадать со значением, указанным в поле «Characters Required» (Количество символов). Это ключи WEP RC4, которые являются общими для станций, использующих точку доступа. Каждая клиентская станция должна быть настроена на использование аналогичных ключей WEP с теми же значениями, которые указаны в данных настройках точки доступа (см. раздел «Правила использования статического WEP-шифрования» на стр. 113). |

Табл. 10.6 Параметры безопасности режима «Static WEP» (Статическое WEP-шифрование) (Продолжение)

| Поле | Описание |
|-------------------------|---|
| Алгоритм аутентификации | <p>Алгоритм аутентификации определяет метод, который используется, чтобы указать, разрешена ли ассоциация клиентской станции с точкой доступа в режиме безопасности «Static WEP» (Статическое WEP-шифрование). Укажите алгоритм аутентификации, который вы хотите использовать, выбрав один из следующих пунктов в раскрывающемся меню:</p> <ul style="list-style-type: none"> • Open System (Открытая система); • Shared Key (Общий ключ); • Both (Все). <p>Open System (Открытая система) — это метод аутентификации, позволяющий любой клиентской станции устанавливать связь с точкой доступа, вне зависимости от того, имеет эта станция правильный ключ WEP или нет. Данный алгоритм также используется в режимах «простой текст», IEEE 802.1x, и WPA. При выборе алгоритма аутентификации «Open System» (Открытая система) любой клиент может устанавливать связь с точкой доступа.</p> <p>Обратите внимание, что <i>установка связи</i> клиентской станции с точкой доступа не подразумевает обязательный обмен трафиком между ними. Для получения доступа к данным точки доступа и их декодирования, а также для передачи доступных для чтения данных, клиентская станция должна иметь правильный ключ WEP.</p> <p>Shared Key (Общий ключ) — это метод аутентификации, при котором для установки связи с точкой доступа клиентская станция должна иметь правильный ключ WEP. При выборе алгоритма аутентификации «Shared Key» (Общий ключ) станция с неправильным ключом WEP не сможет установить связь с точкой доступа.</p> <p>Both (Все) является значением по умолчанию. При выборе значения алгоритма аутентификации «Both» (Все) должны выполняться следующие условия:</p> <ul style="list-style-type: none"> • Клиентские станции, настроенные на использование протокола WEP в режиме общего ключа, должны иметь действительный ключ WEP для установки связи с точкой доступа. • Клиентские станции, настроенные на использование протокола WEP в режиме открытой системы (с отключенным общим ключом), смогут установить связь с точкой доступа, даже если у них нет правильного ключа WEP. |

Правила использования статического WEP-шифрования

- Режим безопасности беспроводной сети (WLAN) всех клиентских станций должен быть установлен в значение WEP, и для декодирования данных, полученных от точки доступа, клиенты должны иметь один из ключей WEP, указанных на точке доступа.

- Для декодирования данных, полученных от клиентских станций, точка доступа должна иметь все ключи, используемые клиентами.
- Ключи и их значения должны совпадать на всех узлах (точке доступа и клиентах). Например, если точка доступа определяет ключ abc123 как ключ WEP 3, клиентские станции тоже должны определять эту строку как ключ WEP 3.
- Некоторые программы беспроводных клиентов (такие как Funk Odyssey) позволяют настроить несколько ключей WEP и определить значение «transfer key index» (индекс передаточного ключа) для клиентской станции, а затем настроить параметры станции для шифрования передаваемых ими данных с помощью разных ключей. Это запрещает соседним точкам доступа декодировать передаваемые ими данные.

Пример использования статического WEP-шифрования

В качестве простого примера можно привести настройку трех ключей WEP на точке доступа. В нашем примере значение «Transfer Key Index» (Индекс передаточного ключа) для точки доступа равно 3. Это означает, что ключ WEP «3» является ключом, который будет использовать точка доступа для шифрования отправляемых данных.

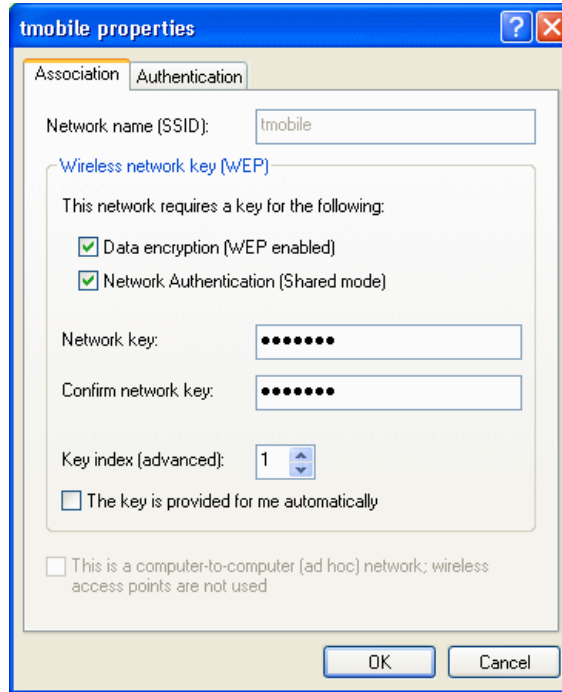
Рис. 10.2 Настройка передаточного ключа на точке доступа

The image shows a configuration window for WEP security. At the top, there are two checkboxes: 'Broadcast SSID' (checked) and 'Station Isolation' (unchecked). Below them is a 'Mode:' dropdown menu set to 'Static WEP'. Underneath is a 'Transfer key index:' dropdown menu set to '3'. Then, there are three radio buttons for 'Key Length': '64 bits' (selected), '128 bits', and '152 bits'. Below that are two radio buttons for 'Key Type': 'ASCII' (selected) and 'Hex'. The 'WEP Keys:' section has a note '(Characters required: 5)' and four input fields. The first three fields are labeled '1:', '2:', and '3:', and contain the text 'abcde', 'fghij', and 'klmno' respectively. The fourth field is labeled '4:' and is empty. At the bottom, there is an 'Authentication:' section with two checkboxes: 'Open system' (checked) and 'Shared key' (unchecked).

Затем необходимо установить режим безопасности WEP на всех клиентских станциях и сохранить комбинации ключей и значений, указанных на точке доступа, на каждой клиентской станции.

В данном примере мы сохраним ключ WEP 1 на клиенте Windows.

Рис. 10.3 Сохранение ключа WEP на беспроводном клиенте



Если имеется вторая клиентская станция, на ней тоже нужно сохранить один из ключей WEP, указанных на точке доступа. Можно сохранить ключ, выделенный для первой станции. В качестве более безопасного решения на второй станции можно сохранить другой ключ WEP (например, ключ 2), чтобы одна станция не могла декодировать передаваемые другой станцией данные.

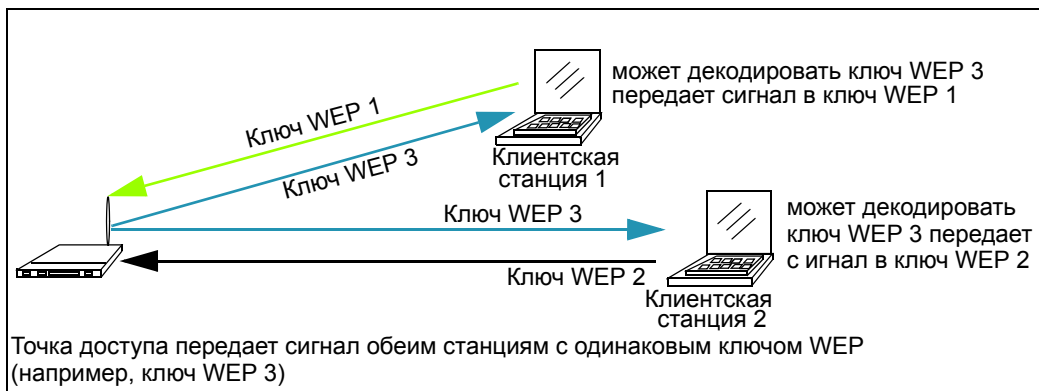
Статическое WEP-шифрование с индексами передаточных ключей на клиентских станциях

Некоторые программы беспроводных клиентов (такие как Funk Odyssey) позволяют настроить несколько ключей WEP и определить значение «transfer key index» (индекс передаточного ключа) для клиентской станции, а затем указать разные ключи для передачи данных от станции точке доступа. Стандартное ПО Windows беспроводных клиентов не позволяет выполнять такие настройки.

В нашем примере с помощью клиентского ПО Funk Odyssey каждому клиенту можно назначить ключ WEP 3, чтобы они могли декодировать данные, передаваемые точкой доступа, а также назначить клиенту 1 ключ WEP 1 и установить его в качестве передаточного ключа. Затем на клиенте 2 можно сохранить ключ WEP 2 и установить его в качестве индекса передаточного ключа.

Рис. 10.2.2.3 демонстрирует работу точки доступа и двух клиентских станций, использующих несколько ключей WEP и индекс передаточного ключа.

Рис. 10.4 Пример использования нескольких ключей WEP и индекса передаточного ключа на клиентских станциях



10.2.2.3 IEEE 802.1x

IEEE 802.1x — это стандарт, определяющий протокол аутентификации и доступ к инфраструктуре для управления ключами с использованием портов. Сообщения расширяемого протокола аутентификации (**EAP**), отправляемые по беспроводной сети **IEEE 802.11** по протоколу передачи EAP-сообщений в стандарте 802.1x (EAP Encapsulation Over LANs, EAPOL). В режиме безопасности IEEE 802.1x используются динамически генерируемые ключи, которые периодически обновляются. Поточное шифрование RC4 используется для шифрования тела кадра и периодической проверки резервирования (CRC) каждого кадра 802.11.

Этот режим требует использования **RADIUS**-сервера для аутентификации пользователей. Если разрешено использование внутреннего RADIUS-сервера, настройте учетные записи пользователей на точке доступа с помощью вкладки *Cluster (Кластер) > User Management (Управление пользователями)*. В противном случае настройте учетные записи пользователей на внешнем RADIUS-сервере.

Для работы точки доступа необходимо наличие RADIUS-сервера, поддерживающего протокол **EAP**, например сервера аутентификации Microsoft Internet Authentication Server или внутреннего сервера аутентификации 9160 G2 Wireless Gateway. Для работы с клиентами Windows сервер аутентификации должен поддерживать защищенный расширяемый протокол аутентификации (PEAP) и **MSCHAP V2**.

При настройке режима IEEE 802.1x вы можете выбрать, какой RADIUS-сервер будет использоваться — встроенный или внешний. Встроенный RADIUS-сервер беспроводного шлюза 9160 G2 Wireless Gateway поддерживает защищенный расширяемый протокол аутентификации (Protected *EAP*, PEAP) и протокол MSCHAP V2.

При использовании собственного RADIUS-сервера вы можете выбрать любые методы аутентификации, поддерживаемые режимом безопасности IEEE 802.1x, включая сертификаты, Kerberos и аутентификацию с использованием открытого ключа. Необходимо помнить, что на клиентских станциях должен быть настроен метод аутентификации, аналогичный методу, используемому точкой доступа.

При выборе режима безопасности *IEEE 802.1x* необходимо указать следующую информацию:

The screenshot shows a configuration window titled "Security Mode". At the top, there is a dropdown menu set to "IEEE 802.1x". Below this, there is a section for "Authentication Server" with a dropdown menu set to "Built-in". Underneath, the "Radius IP" is configured as "127.0.0.1" using four separate input fields. The "Radius Key" is represented by a masked text field with ten dots. At the bottom, there is a checkbox labeled "Enable radius accounting" which is currently unchecked.

The screenshot shows a configuration window for wireless security. At the top, there are two checkboxes: "Broadcast SSID" (checked) and "Station Isolation" (unchecked). Below these is a "Mode:" dropdown menu set to "IEEE802.1x". A section titled "Use internal radius server" is highlighted with a grey background. Inside this section, the "Radius IP" is set to "10.128.14.14" and the "Radius Key" is a masked field with ten dots. At the bottom of this section is a checkbox labeled "Enable radius accounting" which is unchecked.

Табл. 10.7 Параметры безопасности режима IEEE 802.1х


| Поле | Описание |
|--|--|
| <i>Use internal radius server</i> (Использовать внутренний RADIUS-сервер) | <p>Выберите один из следующих пунктов в раскрывающемся меню:</p> <ul style="list-style-type: none">• Чтобы использовать сервер аутентификации, предоставляемый беспроводным шлюзом 9160 G2 Wireless Gateway, установите флажок Use internal radius server (Использовать внутренний RADIUS-сервер). При выборе этого параметра не нужно указывать IP-адрес и ключ RADIUS-сервера — эти значения подставляются автоматически. Если разрешено использование внутреннего RADIUS-сервера, настройте учетные записи пользователей на точке доступа с помощью вкладки <i>Cluster (Класстер) > User Management (Управление пользователями)</i>. Для получения дополнительной информации см. раздел Гл. 7: «Управление учетными записями пользователей».• Чтобы использовать внешний сервер аутентификации, снимите флажок Use internal radius server (Использовать внутренний RADIUS-сервер). Если этот параметр не выбран, необходимо указать IP-адрес и ключ RADIUS-сервера, который вы будете использовать. <p>Примечание. RADIUS-сервер определяется по IP-адресу и номерам портов UDP для каждой предоставляемой им службы. В текущей версии беспроводного шлюза 9160 G2 Wireless Gateway порты протокола пользовательских датаграмм (UDP) RADIUS-сервера, используемые точкой доступа, являются ненастраиваемыми. В беспроводном шлюзе 9160 G2 Wireless Gateway порт UDP 1812 RADIUS-сервера жестко запрограммирован для использования в целях аутентификации, а порт 1813 — для ведения учета.</p> |
| <i>Radius IP</i> (IP-адрес RADIUS-сервера) | <p>Укажите IP-адрес RADIUS-сервера в текстовом поле.</p> <p>Значение <i>Radius IP</i> (IP-адрес RADIUS-сервера) — IP-адрес RADIUS-сервера.</p> <p>IP-адрес внутреннего сервера аутентификации беспроводного шлюза 9160 G2 Wireless Gateway — 127.0.0.1.</p> <p> При наличии в сети внешнего RADIUS-сервера рекомендуется использовать его вместо встроенного RADIUS-сервера на точке доступа. Внешний RADIUS-сервер обеспечит более высокий уровень безопасности, чем локальный сервер аутентификации.</p> <p>Для получения информации о настройке учетных записей пользователей см. Гл. 7: «Управление учетными записями пользователей».</p> |
| <i>Radius Key</i> (Ключ RADIUS-сервера) | <p>Укажите ключ RADIUS-сервера в текстовом поле.</p> <p>Значение <i>Radius Key</i> (Ключ RADIUS-сервера) — общий секретный ключ RADIUS-сервера. Вводимый текст будет отображаться в виде звездочек (*), скрывающих ключ RADIUS от посторонних.</p> <p>Секретный ключ внутреннего сервера аутентификации 9160 G2 Wireless Gateway — secret.</p> <p>Это значение никогда не передается по сети.</p> |

Табл. 10.7 Параметры безопасности режима IEEE 802.1x (Продолжение)

| Поле | Описание |
|---|--|
| <i>Enable radius accounting</i> (Включить учет RADIUS) | Установите флажок «Enable radius accounting» (Включить учет RADIUS) для отслеживания и измерения ресурсов, используемых определенным пользователем, например системного времени, количества переданных и полученных данных и т. д. |

10.2.2.4 WPA Personal

Режим безопасности *WPA Personal* — это стандарт Wi-Fi Alliance IEEE *802.11i*, который включает в себя режим гаммирования/протокол CBC-MAC-улучшенный алгоритм шифрования (*CCMP-AES*) и протокол шифрования с использованием временных ключей (*TKIP*).

Версия Personal стандарта WPA использует предварительный ключ (вместо IEEE *802.1x* и *EAP*, используемых в режиме безопасности WPA Enterprise). Ключ PSK используется только для первоначальной проверки учетных данных. Данный режим безопасности имеет обратную совместимость для беспроводных клиентов, которые поддерживают оригинальный *WPA*.

При выборе режима безопасности *WPA Personal* настройте параметры, как описано в Табл. 10.8 на стр. 120.

Security Mode

WPA/WPA2 Personal (PSK)

Supported Client Stations

Both

Cipher Suites

TKIP

Key

☒ Broadcast SSID ☐ Station Isolation

Mode:

WPA Personal

WPA Versions: ☒ WPA ☒ WPA2

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

Key:

reoreore

Табл. 10.8 Параметры безопасности WPA Personal

| Поле | Описание |
|------------------------------|--|
| WPA Versions (Версии WPA) | <p>Выберите тип клиентских станций, поддержка которых будет необходима:</p> <ul style="list-style-type: none">WPAWPA2Both (Все) <p>WPA. Если все клиентские станции в сети поддерживают оригинальный стандарт WPA, но ни одна не поддерживает более новый стандарт WPA2, выберите значение «WPA».</p> <p>WPA2. Если все клиентские станции в сети поддерживают WPA2, рекомендуется использовать стандарт WPA2, обеспечивающий наилучший уровень защиты по сравнению со стандартом IEEE 802.11i.</p> <p>Both (Все). Если используются различные клиенты, часть которых поддерживает стандарт WPA2, а часть — только оригинальный стандарт WPA, выберите поддержку обоих стандартов. Таким образом клиентские станции с поддержкой WPA и WPA2 смогут взаимодействовать и выполнять процесс аутентификации, в то время как станции, поддерживающие WPA2, смогут использовать этот более надежный стандарт. Эта конфигурация WPA обеспечивает более высокий уровень взаимодействия за счет некоторого снижения уровня защиты.</p> |

Табл. 10.8 Параметры безопасности WPA Personal (Продолжение)

| Поле | Описание |
|---|---|
| <i>Cipher Suites</i> (Наборы шифров) | <p>Выберите набор шифров, который вы хотите использовать:</p> <ul style="list-style-type: none"> • TKIP • CCMP (AES) • Both (Все) <p>Temporal Key Integrity Protocol (протокол шифрования с использованием временных ключей, TKIP) является значением по умолчанию.</p> <p>Протокол TKIP обеспечивает более надежное шифрование данных по сравнению с ключами WEP. Процесс TKIP чаще меняет используемый ключ шифрования и реже использует аналогичные ключи для шифрования данных (что является слабым местом WEP-шифрования). Протокол TKIP использует 128-разрядный «временной ключ», общий для клиентов и точек доступа. Временной ключ комбинируется с MAC-адресом клиента и 16-октетным вектором инициализации, а затем используется для шифрования данных. Таким образом, каждая клиентская станция использует разные ключи для шифрования данных. Аналогично стандарту WEP, для шифрования протокол TKIP использует RC4. Но TKIP меняет временные ключи через каждые 10 000 пакетов и распространяет их, что существенно повышает уровень безопасности сети.</p> <p>Режим гаммирования/протокол CBC-MAC (CCMP) — это метод шифрования для IEEE 802.11i, использующий улучшенный алгоритм шифрования (Advanced Encryption Algorithm, AES). В нем используется CCM в сочетании с режимом сцепления шифрованных блоков/режимом гаммирования (CBC-CTR) и режимом сцепления шифрованных блоков/кодом аутентификации сообщений (CBC-MAC) для шифрования данных и сохранения целостности сообщений.</p> <p>При выборе обоих режимов (TKIP и CCMP(AES)) парное шифрование обеспечивается алгоритмом AES, а групповое шифрование — протоколом TKIP. Парное шифрование используется для одноадресного трафика, а групповое — для многоадресного/широковещательного трафика. Как клиенты TKIP, так и клиенты AES могут устанавливать связь с точкой доступа. Клиенты WPA должны иметь один из следующих параметров для установки связи с точкой доступа:</p> <ul style="list-style-type: none"> • действительный ключ TKIP; • действительный ключ CCMP (AES). <p>Клиенты, не настроенные на использование WPA Personal, не смогут установить связь с точкой доступа.</p> |
| <i>Key (Ключ)</i> | <p>Pre-shared Key (Предварительный ключ) — это общий секретный ключ для режима WPA Personal. Введите строку длиной от 8 до 63 символов.</p> |

10.2.2.5 WPA Enterprise

Режим безопасности *WPA Enterprise* с использованием службы идентификации удаленных пользователей (**RADIUS**) является реализацией стандарта Wi-Fi Alliance **IEEE 802.11h**, который включает в себя усовершенствованный стандарт шифрования (**AES**), режим гаммирования/протокол CBC-MAC (**CCMP**) и протокол шифрования с использованием временных ключей (**TKIP**). В режиме Enterprise необходимо использовать RADIUS-сервер для аутентификации пользователей и настроить учетные записи пользователей на вкладке *Cluster (Классет), User Management (Управление пользователями)*.

Данный режим безопасности имеет обратную совместимость для беспроводных клиентов, которые поддерживают оригинальный **WPA**.

При настройке режима WPA Enterprise вы можете выбрать, какой RADIUS-сервер будет использоваться — встроенный или внешний. Встроенный RADIUS-сервер беспроводного шлюза 9160 G2 Wireless Gateway поддерживает защищенный расширяемый протокол аутентификации (Protected **EAP**, PEAP) и протокол MSCHAP V2.

При выборе режима безопасности «WPA Enterprise» настройте параметры, как описано в Табл. 10.9 на стр. 123.

The screenshot displays the configuration interface for WPA Enterprise security mode. At the top, the 'Security Mode' is set to 'WPA/WPA2 Enterprise (RADIUS)'. Below this, several settings are visible: 'Supported Client Stations' is set to 'WPA'; 'Cipher Suites' is set to 'TKIP'; 'Authentication Server' is set to 'Built-in'. The 'Radius IP' is configured as '127.0.0.1', and the 'Radius Key' is shown as a masked field. There are checkboxes for 'Enable pre-authentication', 'Enable radius accounting', and 'Allow non-WPA IEEE 802.1x clients', with the last one being checked.

| Parameter | Value |
|-----------------------------------|-------------------------------------|
| Security Mode | WPA/WPA2 Enterprise (RADIUS) |
| Supported Client Stations | WPA |
| Enable pre-authentication | <input type="checkbox"/> |
| Cipher Suites | TKIP |
| Authentication Server | Built-in |
| Radius IP | 127.0.0.1 |
| Radius Key | [Masked] |
| Enable radius accounting | <input type="checkbox"/> |
| Allow non-WPA IEEE 802.1x clients | <input checked="" type="checkbox"/> |

☒ Broadcast SSID ☐ Station Isolation

Mode:

WPA Enterprise

WPA Versions: ☒ WPA ☒ WPA2

☐ Enable pre-authentication

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

☐ Use internal radius server

Radius IP:

10.128.14.14

Radius Key:

••••••••••

☐ Enable radius accounting

Табл. 10.9 Параметры безопасности WPA Enterprise

| Поле | Описание |
|------------------------------|--|
| WPA Versions (Версии WPA) | <p>Выберите тип клиентских станций, поддержка которых будет необходима:</p> <ul style="list-style-type: none">• WPA• WPA2• Both (Все) <p>WPA. Если все клиентские станции в сети поддерживают оригинальный стандарт WPA, но ни одна не поддерживает более новый стандарт WPA2, выберите значение «WPA».</p> <p>WPA2. Если все клиентские станции в сети поддерживают WPA2, рекомендуется использовать стандарт WPA2, обеспечивающий наилучший уровень защиты по сравнению со стандартом IEEE 802.11i.</p> <p>Both (Все). Если используются различные клиенты, часть которых поддерживает стандарт WPA2, а часть — только оригинальный стандарт WPA, выберите поддержку обоих стандартов. Таким образом клиентские станции с поддержкой WPA и WPA2 смогут взаимодействовать и выполнять процесс аутентификации, в то время как станции, поддерживающие WPA2, смогут использовать этот более надежный стандарт. Эта конфигурация WPA обеспечивает более высокий уровень взаимодействия за счет некоторого снижения уровня защиты.</p> |

Табл. 10.9 Параметры безопасности WPA Enterprise (Продолжение)

| Поле | Описание |
|--|---|
| <i>Enable pre-authentication (Включить предварительную аутентификацию)</i> | <p>Если вы выбрали значение «WPA2» или «Both» (Все) для поля «WPA Versions» (Версии WPA), вы можете включить предварительную аутентификацию клиентов WPA2.</p> <p>Нажмите «Enable pre-authentication» (Включить предварительную аутентификацию), чтобы беспроводные клиенты WPA2 отправляли пакеты предварительной аутентификации. Данные предварительной аутентификации будут перенаправлены от точки доступа, которую использует клиент, целевой точке доступа. Включение этой функции поможет ускорить процесс аутентификации для клиентов роуминга, подключенных к нескольким точкам доступа.</p> <p>Этот параметр нельзя использовать при выборе значения «WPA» для поля «WPA Versions» (Версии WPA), потому что оригинальный стандарт WPA не поддерживает эту функцию.</p> |

Табл. 10.9 Параметры безопасности WPA Enterprise (Продолжение)

| Поле | Описание |
|---|--|
| <i>Cipher Suites</i> (Наборы шифров) | <p>Выберите шифр, который вы хотите использовать:</p> <ul style="list-style-type: none"> • TKIP • CCMP (AES) • Both (Все) <p>Temporal Key Integrity Protocol (протокол шифрования с использованием временных ключей, TKIP) является значением по умолчанию.</p> <p>Протокол TKIP обеспечивает более надежное шифрование данных по сравнению с ключами WEP. Процесс TKIP чаще меняет используемый ключ шифрования и реже использует аналогичные ключи для шифрования данных (что является слабым местом WEP-шифрования). Протокол TKIP использует 128-разрядный «временной ключ», общий для клиентов и точек доступа. Временной ключ комбинируется с MAC-адресом клиента и 16-октетным вектором инициализации, а затем используется для шифрования данных. Таким образом, каждая клиентская станция использует разные ключи для шифрования данных. Аналогично стандарту WEP, для шифрования протокол TKIP использует RC4. Но TKIP меняет временные ключи через каждые 10 000 пакетов и распространяет их, что существенно повышает уровень безопасности сети.</p> <p>Режим гаммирования/протокол CBC-MAC (CCMP) — это метод шифрования для IEEE 802.11i, использующий улучшенный алгоритм шифрования (Advanced Encryption Algorithm, AES). В нем используется CCM в сочетании с режимом сцепления шифрованных блоков/режимом гаммирования (CBC-CTR) и режимом сцепления шифрованных блоков/кодом аутентификации сообщений (CBC-MAC) для шифрования данных и сохранения целостности сообщений.</p> <p>При выборе обоих протоколов TKIP и CCMP клиенты TKIP и AES могут устанавливать связь с точкой доступа. Клиентские станции, настроенные для использования WPA с RADIUS-сервером, должны иметь один из следующих параметров для установки связи с точкой доступа:</p> <ul style="list-style-type: none"> • действительный IP-адрес RADIUS-сервера для протокола TKIP и действительный общий ключ; • действительный IP-адрес CCMP (AES) и действительный общий ключ. <p>Клиенты, не настроенные на использование WPA с RADIUS-сервером, не смогут установить связь с точкой доступа.</p> <p>По умолчанию выбраны оба значения — TKIP и CCMP. Если выбраны оба значения (TKIP и CCMP), клиентские станции, настроенные для использования WPA с RADIUS-сервером, должны иметь один из следующих параметров:</p> <ul style="list-style-type: none"> • действительный IP-адрес RADIUS-сервера для протокола TKIP и ключ RADIUS; • действительный IP-адрес CCMP (AES) и ключ RADIUS; |

Табл. 10.9 Параметры безопасности WPA Enterprise (Продолжение)


| Поле | Описание |
|--|---|
| <i>Use internal radius server</i> (Использовать внутренний RADIUS-сервер) | <p>Вы можете указать, какой сервер аутентификации вы будете использовать — встроенный сервер беспроводного шлюза 9160 G2 Wireless Gateway или внешний RADIUS-сервер.</p> <ul style="list-style-type: none">• Чтобы использовать сервер аутентификации, предоставляемый беспроводным шлюзом 9160 G2 Wireless Gateway, установите флажок «Use internal radius server» (Использовать внутренний RADIUS-сервер). При выборе этого параметра не нужно указывать IP-адрес и ключ RADIUS-сервера — эти значения подставляются автоматически. Если разрешено использование внутреннего RADIUS-сервера, настройте учетные записи пользователей на точке доступа с помощью вкладки <i>Cluster</i> (Кластер) > <i>User Management</i> (Управление пользователями). Для получения дополнительной информации см. раздел Гл. 7: «Управление учетными записями пользователей».• Чтобы использовать внешний сервер аутентификации, снимите флажок Use internal radius server (Использовать внутренний RADIUS-сервер). Если этот параметр не выбран, необходимо указать IP-адрес и ключ RADIUS-сервера, который вы будете использовать. <p>Примечание. RADIUS-сервер определяется по IP-адресу и номерам портов UDP для каждой предоставляемой им службы. В текущей версии беспроводного шлюза 9160 G2 Wireless Gateway порты протокола пользовательских датаграмм (UDP) RADIUS-сервера, используемые точкой доступа, являются ненастраиваемыми. В беспроводном шлюзе 9160 G2 Wireless Gateway порт UDP 1812 RADIUS-сервера жестко запрограммирован для использования в целях аутентификации, а порт 1813 — для ведения учета.</p> |
| <i>Radius IP</i> (IP-адрес RADIUS-сервера) | <p>Укажите IP-адрес RADIUS-сервера в текстовом поле. Значение <i>Radius IP</i> (IP-адрес RADIUS-сервера) — IP-адрес RADIUS-сервера.</p> <p>IP-адрес внутреннего сервера аутентификации беспроводного шлюза 9160 G2 Wireless Gateway — 127.0.0.1.</p> <div> При наличии в сети внешнего RADIUS-сервера рекомендуется использовать его вместо встроенного RADIUS-сервера на точке доступа. Внешний RADIUS-сервер обеспечит более высокий уровень безопасности, чем локальный сервер аутентификации.</div> <p>Для получения информации о настройке учетных записей пользователей см. Гл. 7: «Управление учетными записями пользователей».</p> |

Табл. 10.9 Параметры безопасности WPA Enterprise (Продолжение)

| Поле | Описание |
|--|---|
| <i>Radius Key (Ключ RADIUS-сервера)</i> | <p>Укажите ключ RADIUS-сервера в текстовом поле.</p> <p>Значение <i>Radius Key (Ключ RADIUS-сервера)</i> — общий секретный ключ RADIUS-сервера. Вводимый текст будет отображаться в виде звездочек (*), скрывающих ключ RADIUS от посторонних.</p> <p>Секретный ключ внутреннего сервера аутентификации 9160 G2 Wireless Gateway — secret.</p> <p>Это значение никогда не передается по сети.</p> |
| <i>Enable RADIUS Accounting (Включить учет RADIUS)</i> | <p>Нажмите Enable RADIUS Accounting (Включить учет RADIUS), если вы хотите принудительно использовать аутентификацию для клиентских станций WPA с указанием имен пользователей и паролей для каждой станции. См. также Гл. 7: «Управление учетными записями пользователей».</p> |

10.3 Обновление параметров

Для обновления параметров безопасности:

1. Перейдите на вкладку *Security (Безопасность)*.
2. Внесите необходимые изменения в параметры безопасности.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

| | |
|--|-----|
| 11.1 Интерфейсы | 131 |
| 11.1.1 Параметры проводной сети Ethernet | 132 |
| 11.1.2 Параметры беспроводной сети | 132 |
| 11.2 Журналы регистрации событий | 132 |
| 11.2.1 Настройка режима «Persistence» (Непрерывный) | 133 |
| 11.2.2 Уровень критичности событий | 134 |
| 11.2.3 Глубина регистрации событий | 135 |
| 11.2.4 Узел ретрансляции журнала событий для сообщений ядра системы | 135 |
| 11.2.4.1 Общие сведения о регистрации событий | 135 |
| 11.2.4.2 Настройка узла ретрансляции журнала | 136 |
| 11.2.4.3 Включение и отключение узла ретрансляции журнала на экране «Status» (Статус), «Events» (События) | 137 |
| 11.2.5 Журнал регистрации событий | 138 |
| 11.3 Статистика передачи и получения данных | 139 |
| 11.4 Ассоциированные беспроводные клиенты | 140 |
| 11.4.1 Мониторинг целостности соединения | 141 |
| 11.5 Соседние точки доступа | 141 |



Важно! *Проведение всех описываемых операций по техническому обслуживанию и мониторингу оборудования подразумевает просмотр и изменение параметров конкретных точек доступа, а не конфигурации кластера, автоматически объединяющего несколько точек доступа. Поэтому перед настройкой определенной точки доступа необходимо убедиться, что настройка производится на веб-страницах администрирования этой точки доступа. Для получения дополнительной информации см. раздел «Конфигурационная информация определенной точки доступа и управление автономными точками доступа» на стр. 66.*

11.1 Интерфейсы

Для просмотра параметров проводных и беспроводных (*WLAN*) сетей выберите меню *Status (Статус) > Interfaces (Интерфейсы)* на нужной точке доступа.



Примечание. Для точки доступа с двумя радиомодулями отображаются текущие беспроводные параметры первого и второго радиомодулей. Для точки доступа с одним радиомодулем отображаются параметры одного радиомодуля. На рисунке ниже показан экран «Interfaces» (Интерфейсы) для точки доступа с двумя радиомодулями.

Рис. 11.1 Экран сетевых интерфейсов

View settings for network interfaces

Wired Settings

(Edit)

LAN or Internal Interface

MAC Address00:08:A2:01:10:AC

VLAN ID

IP Address10.128.75.98

Subnet Mask255.255.0.0

Guest Interface

MAC Address00:00:00:00:00:00

VLAN ID

Subnet

Wireless Settings

(Edit)

Radio

ModeIEEE 802.11g

Channel5 (2432 MHz)

Internal Interface

MAC Address00:08:A2:01:10:B0

Network Name (SSID)SFGWPA /

Guest Interface

MAC Addressn/a

Network Name (SSID)TEKLOGIX GUEST /

?

This page displays current Ethernet (Wired) and Wireless settings on the access point.

To configure Ethernet Settings, go to the [Ethernet \(Wired\) Settings](#) tab.

To configure Wireless Settings, go to the [Wireless Settings](#) tab.

[More ...](#)

На этом экране отображены текущие параметры беспроводного шлюза 9160 G2 Wireless Gateway. Здесь представлены *параметры проводной сети Ethernet* и *параметры беспроводной сети*.

11.1.1 Параметры проводной сети Ethernet

Интерфейс *Internal (Внутренний)* включает в себя Ethernet MAC Address (*MAC-адрес*), IP Address (*IP-адрес*), Subnet Mask (*Маска подсети*) и **SSID** (имя связанной беспроводной сети).

Интерфейс *Guest (Гостевой)* включает в себя *MAC Address (MAC-адрес)*, *VLAN ID (идентификатор VLAN)* и **SSID** (имя связанной беспроводной сети).

Чтобы внести изменения в эти параметры, нажмите на ссылку **Edit** (Редактировать).

11.1.2 Параметры беспроводной сети

Интерфейс *Radio (Радиомодуль)* включает параметры радиомодуля *Mode (Режим)* и *Channel (Канал)*. Здесь также указаны MAC-адреса (*MAC address*) (в режиме «только для чтения») и имена сетей для внутреннего и гостевого интерфейсов (для получения дополнительной информации см. Гл. 13: «Настройка беспроводного интерфейса» и Гл. 16: «Настройка параметров радиомодуля 802.11»).

Чтобы внести изменения в параметры, нажмите ссылку **Edit** (Редактировать).

11.2 Журналы регистрации событий

Для просмотра системных событий и журнала событий ядра системы для конкретной точки доступа выберите меню *Status (Статус)* > *Events (События)* на веб-странице администрирования этой точки доступа.

Рис. 11.2 События точек доступа

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

View events generated by this access point

Options

Persistence ☐ Enabled ☒ Disabled

Severity

7

Depth 128

Update

☐ Relay Log

Relay Host

Relay Port 514

Update

Events

Clear All

| Time | Type | Service | Description |
|----------------|------|-----------------|--|
| Jun 4 19:14:29 | info | dropbear [3074] | exit after auth (admin): Exited normally |
| Jun 4 19:14:29 | err | dropbear [3074] | chown /dev/tty0 0 0 failed: Read-only file system |
| Jun 4 18:25:30 | info | hostapd | wlan0: STA 00:10:c6:36:6f:1f WPA: group key poll timed out (no reply was received) |
| Jun 4 18:24:00 | info | hostapd | wlan0: STA 00:10:c6:36:6f:1f WPA: group key exchange completed |

На вкладке *Events* (События) можно включить и отключить режим *Persistence* (Непрерывный). На этом экране также можно включить удаленный «узел ретрансляции журнала» для записи всех системных событий и ошибок в журнал ядра. Перед включением этого параметра необходимо настроить удаленный узел ретрансляции. См. «Узел ретрансляции журнала событий для сообщений ядра системы» на стр. 135. Также на вкладке *Events* (События) находится список последних событий точки доступа (см. «Журнал регистрации событий» на стр. 138).



Примечание. Беспроводной шлюз 9160 G2 Wireless Gateway получает информацию о дате и времени по сетевому протоколу синхронизации времени (NTP). Данные поступают в формате UTC (среднее время по Гринвичу). Необходимо конвертировать эти данные в формат местного времени. Для получения информации о настройке сетевого протокола синхронизации времени см. Гл. 25: «Сетевой протокол синхронизации времени».

11.2.1 Настройка режима «Persistence» (Непрерывный)

Режим *Persistence* (Непрерывный) можно включить на вкладке *Events* (События). Непрерывный журнал событий сохраняется в память NVRAM. Непрерывные журналы событий хранятся в памяти NVRAM даже после перезагрузки системы. Прочие типы журналов событий сохраняются только во время работы оборудования. При перезагрузке беспроводного шлюза 9160 G2 все эти журналы событий будут утеряны.

При включении режима *Persistence* (Непрерывный) на вкладке *Events* (События) все журналы событий сохраняются в память NVRAM и остаются доступными даже после перезагрузки системы.



Примечание. Необходимо помнить, что после включения режима «Persistence» (Непрерывный) события будут записываться непрерывно. Так как эта ситуация может привести к износу флэш-памяти точки доступа, необходимо учесть этот риск перед использованием данного режима.

Табл. 11.1 Параметры настройки режима «Persistence» (Непрерывный)

| Поле | Описание |
|--|--|
| <i>Relay Log</i> (Ретрансляция журнала) | Включение или отключение режима <i>Persistence</i> (Непрерывный). |
| <i>Relay Log</i> (Узел ретрансляции) | Выбор уровня <i>Severity</i> (Критичность) — от 0 до 7. Уровень <i>Severity</i> (Критичность) 7 является наименее критичным, а уровень <i>Severity</i> (Критичность) 0 — наиболее критичным. Для получения дополнительной информации об уровнях критичности событий см. «Уровень критичности событий» на стр. 134. |
| <i>Relay Port</i> (Порт ретрансляции) | Задайте значение от 1 до 128. Для получения дополнительной информации о глубине регистрации событий см. раздел «Глубина регистрации событий» на стр. 135. |

11.2.2 Уровень критичности событий

Настройка уровня критичности событий предназначена для отбора или ограничения количества сообщений системы безопасности, отображаемого в журнале регистрации событий. Необходимость просматривать список всех событий возникает очень редко. Поэтому можно исключить сообщения о событиях с более низким уровнем критичности или важности с помощью параметра настройки *Severity* (Критичность). При установке уровня *Severity* (Критичность) 7 в журнале регистрации событий будут отображаться все сообщения о событиях с уровнем критичности от 7 до 0. Если вы хотите исключить некоторые сообщения, установите уровень *Severity* (Критичность) 4. В этом случае в журнале регистрации событий будут отображаться сообщения о событиях с уровнем критичности от 4 до 0. Сообщения и уведомления о событиях с более низким уровнем критичности будут проигнорированы.

Табл. 11.2 Параметры настройки уровня критичности

| Уровень критичности | Описание |
|---------------------|---|
| 0 | <i>Emergency (Экстренная ситуация)</i> : система не может быть использована |
| 1 | <i>Alert (Опасность)</i> : необходимы немедленные действия |
| 2 | <i>Critical (Критическая ситуация)</i> : критическое состояние системы |
| 3 | <i>Error (Ошибка)</i> : ошибка системы |
| 4 | <i>Warning (Предупреждение)</i> : предупреждение системы |
| 5 | <i>Notice (Уведомление)</i> : важное уведомление при нормальном состоянии системы |
| 6 | <i>Informational (Информация)</i> : информационные сообщения |
| 7 | <i>Debug (Отладка)</i> : сообщения уровня отладки системы |

11.2.3 Глубина регистрации событий

Значение поля *Depth (Глубина)* определяет количество записей журнала, которое может быть сохранено в память NVRAM. Можно сохранить не более 128 записей. Если вы используете сообщения журнала событий для мониторинга производительности точки доступа, задайте для поля *Depth (Глубина)* максимальное значение **128**.

11.2.4 Узел ретрансляции журнала событий для сообщений ядра системы

- «Общие сведения о регистрации событий» на стр. 135.
- «Настройка узла ретрансляции журнала» на стр. 136.
- «Включение и отключение узла ретрансляции журнала на экране «Status» (Статус), «Events» (События)» на стр. 137.

11.2.4.1 Общие сведения о регистрации событий

Журнал событий ядра представляет собой полный список сообщений о системных событиях, отображаемый в системном журнале, и сообщений ядра, таких как сообщения об ошибках (пропадание кадров и т.д.).

Сообщения журнала ядра для точки доступа невозможно просматривать непосредственно из веб-интерфейса администрирования. Сначала нужно настроить удаленный сервер с запущенным процессом syslog, действующий как «узел ретрансляции журнала» процесса syslog в вашей сети. Затем необходимо настроить отправку сообщений syslog от беспроводного шлюза 9160 G2 Wireless Gateway на удаленный сервер.

Использование удаленного сервера для сбора сообщений syslog точек доступа дает ряд преимуществ. Вы можете выполнять следующие действия:

- выполнять сбор сообщений syslog нескольких точек доступа;
- сохранять в журнале больше событий по сравнению с историей событий, хранимых в одной точке доступа;
- активировать заданные сценарием операции управления и оповещения.

11.2.4.2 Настройка узла ретрансляции журнала

Чтобы использовать функцию ретрансляции журнала ядра, необходимо настроить удаленный сервер для получения сообщений syslog. Процесс настройки зависит от типа оборудования, используемого в качестве удаленного узла регистрации. Ниже приведен пример настройки удаленного сервера Linux с помощью служебного процесса syslog.

Пример использования Linux syslogd

Выполните следующие действия для активации служебной программы syslog на сервере Linux. Убедитесь, что все операции выполняются от имени пользователя root.

1. Войдите от имени пользователя root на оборудование, которое вы хотите использовать в качестве узла ретрансляции журнала.

Для выполнения следующих операций необходимо иметь права пользователя root. Если вы не вошли в систему как пользователь root, введите su в командной строке для выполнения действия от имени пользователя root («суперпользователя»).

2. Откройте для редактирования /etc/init.d/syslogd и добавьте «-r» в переменную SYSLOGD в верхней части файла. Редактируемая строка должна выглядеть так:
SYSLOGD= «-r»

На страницах справочника можно найти дополнительную информацию о командах syslogd. (Введите man syslogd в командную строку.)

3. Если необходимо отправлять все сообщения в файл, откройте для редактирования /etc/syslog.conf.

Например, чтобы отправлять все сообщения в файл журнала с именем «AP_syslog», можно добавить следующую строку:

```
*.* -/tmp/AP_syslog
```

На страницах справочника можно найти дополнительную информацию о командах syslog.conf. (Введите `man syslog.conf` в командную строку.)

4. Выполните перезапуск сервера syslog с помощью ввода следующей команды:
`/etc/init.d/syslogd restart`



Примечание. По умолчанию процесс syslog использует порт 514. Порт по умолчанию менять не рекомендуется. Однако при необходимости изменить порт журнала убедитесь, что номер порта, назначенного для syslog, не используется другим процессом.

11.2.4.3 Включение и отключение узла ретрансляции журнала на экране «Status» (Статус), «Events» (События)

Чтобы включить и настроить ретрансляцию журнала на экране *Status (Статус)* > *Events (События)*, выполните описанные ниже действия по настройке параметров *Log Relay (Ретрансляция журнала)* и нажмите **Update** (Обновить).

Relay Log ☒

Relay Host

Relay Port

Update

Табл. 11.3 Параметры узла ретрансляции журнала

| Поле | Описание |
|--|--|
| <i>Relay Log</i> (Ретрансляция журнала) | Включение или отключение узла ретрансляции журнала: При установке флажка Relay Log (Ретрансляция журнала) происходит включение узла ретрансляции журнала событий, а поля <i>Relay Host</i> (Узел ретрансляции) и <i>Relay Port</i> (Порт ретрансляции) становятся редактируемыми. |
| <i>Relay Log</i> (Узел ретрансляции) | Определение параметра IP-адрес или имени DNS узла ретрансляции. Примечание. При использовании центра управления беспроводными сетями <i>Devicescape Wireless Operations Center</i> сервер репозитория должен получать сообщения syslog от всех точек доступа. Поэтому в качестве значения «Relay Host» (Узел ретрансляции) необходимо использовать IP-адрес сервера репозитория данного центра управления. |
| <i>Relay Port</i> (Порт ретрансляции) | Определение номера порта процесса syslog на узле ретрансляции. Порт по умолчанию — 514 . |

Обновление параметров

Чтобы применить изменения, нажмите **Update** (Обновить).

Если вы *включили* использование узла ретрансляции журнала событий, после нажатия **Update** (Обновить) будет активирована удаленная регистрация событий. Точка доступа будет отправлять сообщения о событиях ядра в режиме реального времени, и они будут доступны для просмотра на мониторе удаленного сервера регистрации событий, в указанном файле журнала ядра или в другом хранилище, в зависимости от настроек узла ретрансляции журнала событий.

Если вы *отключили* использование узла ретрансляции журнала событий, после нажатия **Update** (Обновить) удаленная регистрация событий будет деактивирована.

11.2.5 Журнал регистрации событий

В журнале регистрации событий хранятся сообщения о системных событиях точки доступа, такие как ассоциирование станций во время аутентификации и другие события. Журнал регистрации событий всегда отображается в режиме реального времени на веб-странице администрирования *Status* (Статус), *Events* (События) просматриваемой точки доступа.

11.3 Статистика передачи и получения данных

Для просмотра статистики переданных и полученных данных для конкретной точки доступа выберите меню *Status (Статус) > Transmit/Receive (Передача/получение данных)* на веб-странице администрирования этой точки доступа.



Примечание. На Рис. 11.3 показан экран «Transmit/Receive» (Передача/получение данных) точки доступа с двумя радиомодулями. Веб-страница администрирования точки доступа с одним радиомодулем будет выглядеть несколько иначе.

Рис. 11.3 Экран статистики передачи и получения данных

| | | | | |
|---------------------------|--|--|--|--|
| Basic Settings | View transmit and receive statistics for this access point | | | |
| User Management | | | | |
| Cluster | | | | |
| Access Points | | | | |
| Sessions | | | | |
| Channel Management | | | | |
| Wireless Neighborhood | | | | |
| Security | | | | |
| Status | | | | |
| Interfaces | | | | |
| Events | | | | |
| Transmit/Receive | | | | |
| Client Associations | | | | |
| Neighboring Access Points | | | | |
| Manage | | | | |
| Ethernet Settings | | | | |
| 802.11 Settings | | | | |
| 802.11 Advanced Settings | | | | |
| VWN | | | | |

| Type | Ethernet | | Radio |
|-------------|-------------------|-------------------|-----------------------|
| Name | Guest | Internal | Guest |
| IP Address | 10.128.75.4 | | |
| MAC Address | 00:08:A2:01:4B:52 | 00:00:00:00:00:00 | 00:08:A2:01:4B:56 n/a |
| VLAN ID | | | |
| Name (SSID) | SFG | | TEKLOGIX GUEST |

| Transmit | | | | |
|---------------|----------|----------|--------|--|
| Type | Ethernet | | Radio | |
| Name | Guest | Internal | Guest | |
| Total packets | 11329 | 0 | 4622 | |
| Total bytes | 3482589 | 0 | 649463 | |
| Errors | 0 | 0 | 2 | |

| Receive | | | | |
|---------------|----------|----------|-------|--|
| Type | Ethernet | | Radio | |
| Name | Guest | Internal | Guest | |
| Total packets | 833047 | 0 | 37 | |
| Total bytes | 89628621 | 0 | 3190 | |
| Errors | 0 | 0 | 0 | |

На данном экране представлена базовая информация о текущей точке доступа и в режиме реального времени отображается статистика передачи и получения данных для данной точки доступа (см. Табл. 11.4 на стр. 140). Статистика включает общие показатели данных, переданных и полученных с момента последнего запуска точки доступа. При перезапуске точки доступа будут показаны общие показатели данных, переданных и полученных с момента перезапуска.

Табл. 11.4 Статистика передачи и получения данных

| Поле | Описание |
|--|---|
| <i>IP Address</i> (<i>IP-адрес</i>) | <i>IP-адрес</i> для точки доступа. |
| <i>MAC Address</i> (<i>MAC-адрес</i>) | Адрес управления доступом к среде передачи данных (<i>MAC</i>) для указанного интерфейса. MAC-адрес является постоянным уникальным аппаратным адресом любого устройства, представляющего интерфейс для сети. MAC-адрес присваивается производителем. Беспроводной шлюз 9160 G2 Wireless Gateway имеет уникальный MAC-адрес для каждого интерфейса. Каждый интерфейс каждого из радиомодулей точки доступа с двумя радиомодулями имеет свой MAC-адрес. |
| <i>VLAN ID</i> (<i>Идентификатор VLAN</i>) | Идентификатор виртуальной <i>LAN (VLAN)</i> . VLAN — программно реализованная логическая группа сетевых устройств, взаимодействующих так, как будто они подключены к единой физической сети, хотя они могут быть к ней не подключены. VLAN могут использоваться для создания внутренних и гостевых сетей на одной точке доступа. |
| <i>Name (SSID)</i> (<i>Имя (SSID)</i>) | Имя беспроводной сети. Так называемый <i>SSID</i> — буквенно-цифровой ключ, который является уникальным идентификатором беспроводной локальной сети. Настройка SSID выполняется на вкладке «Basic Settings» (Базовые параметры). (См. «Настройка сетевых параметров» на стр. 53.) |
| Информация о переданных и полученных данных | |
| <i>Total Packets</i> (<i>Всего пакетов</i>) | Общее количество пакетов, переданных (таблица «Transmit» (Передача)) или полученных (таблица «Received» (Получено)) точкой доступа. |
| <i>Total Bytes</i> (<i>Всего байт</i>) | Общее количество байт, переданных (таблица «Transmit» (Передача)) или полученных (таблица «Received» (Получено)) точкой доступа. |
| <i>Errors (Ошибки)</i> | Общее количество ошибок, связанных с передачей и получением данных точкой доступа. |

11.4 Ассоциированные беспроводные клиенты

Для просмотра клиентских станций, связанных с определенной точкой доступа выберите меню *Status (Статус) > Client Associations (Ассоциации клиентов)* на веб-странице администрирования этой точки доступа.

Будут отображены ассоциированные станции, а также информация о пакетном трафике, переданном и полученном каждой станцией (см. Рис. 11.4 на стр. 141).

Рис. 11.4 Ассоциированные клиентские станции

| | | | | | | | | |
|---------------------------|---|-------------------|-----|-----|--------------|--------|------------|--------|
| Basic Settings | View list of currently associated client stations | | | | | | | |
| User Management | | | | | | | | |
| Cluster | | | | | | | | |
| Access Points | wlan0 | 00:0c:f1:3e:99:ae | Yes | Yes | From Station | | To Station | |
| Sessions | | | | | Packets | Bytes | Packets | Bytes |
| Channel Management | wlan0 | 00:90:4b:93:f4:35 | Yes | Yes | 1732 | 261063 | 1517 | 510274 |
| Wireless Neighborhood | | | | | 687 | 123005 | 572 | 155409 |
| Security | | | | | | | | |
| Status | | | | | | | | |
| Interfaces | | | | | | | | |
| Events | | | | | | | | |
| Transmit/Receive | | | | | | | | |
| Client Associations | | | | | | | | |
| Neighboring Access Points | | | | | | | | |

11.4.1 Мониторинг целостности соединения

Беспроводной шлюз 9160 G2 Wireless Gateway предоставляет возможность *мониторинга целостности соединения*, обеспечивающего постоянную проверку соединения каждого ассоциированного клиента (даже при отсутствии обмена данными). При отсутствии трафика точка доступа отправляет пакеты данных клиентам каждые несколько секунд. Таким образом точка доступа определяет клиентов, находящихся вне диапазона, даже тогда, когда не происходит обмен трафиком. Клиентское соединение исключается из списка ассоциированных клиентов в течение 300 секунд после выхода клиента из диапазона, даже при сохранении подключения.

11.5 Соседние точки доступа

На экране статуса «соседних точек доступа» в режиме реального времени отображается статистика всех точек доступа, находящихся в диапазоне точки доступа, веб-страницу администрирования которой вы просматриваете. Для просмотра информации о других точках доступа в беспроводной сети выберите меню *Status (Статус) > Neighboring Access Points (Соседние точки доступа)* (см. Рис. 11.5 на стр. 142).

Рис. 11.5 Статус соседних точек доступа

| View neighboring access points | | | | | | | | | | | | | |
|--|-------------|------|-------|---------|-----|------|---------|------|--------|---------|-------------------------|----------------------------------|--|
| AP Detection <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="button" value="Update"/> | | | | | | | | | | | | | |
| MAC | Beacon Int. | Type | SSID | Privacy | WPA | Band | Channel | Rate | Signal | Beacons | Last Beacon | Rates | |
| 00:08:a2:01:13:20 | 100 | AP | | On | Off | 2.4 | 11 | 1 | | 2 | Fri Jan 2 06:33:01 1970 | 1,2,5,5,6,9,11,12,18,24,36,48,54 | |
| 00:08:a2:01:22:34 | 100 | AP | | On | On | 2.4 | 3 | 1 | | 3 | Fri Jan 2 06:31:23 1970 | 1,2,5,5,6,9,11,12,18,24,36,48,54 | |
| 00:08:a2:01:12:fc | 100 | AP | | On | Off | 2.4 | 6 | 1 | | 1 | Fri Jan 2 06:26:45 1970 | 1,2,5,5,6,9,11,12,18,24,36,48,54 | |
| 00:08:a2:01:22:30 | 100 | AP | | On | On | 2.4 | 6 | 1 | | 1 | Fri Jan 2 06:26:07 1970 | 1,2,5,5,6,9,11,12,18,24,36,48,54 | |
| 00:08:a2:02:73:e4 | 100 | AP | steve | On | On | 2.4 | 6 | 1 | | 6616 | Fri Jan 2 06:34:40 1970 | 1,2,5,5,6,9,11,12,18,24,36,48,54 | |

Данные, предоставляемые о соседних точках доступа, описаны в Табл. 11.5.

Табл. 11.5 Статистика соседних точек доступа

| Поле | Описание |
|--------------------------------------|--|
| <i>MAC (MAC-адрес)</i> | <p>Показывает MAC-адрес соседней точки доступа.</p> <p>MAC-адрес — это аппаратный адрес, являющийся уникальным идентификатором каждого узла сети.</p> |
| <i>Radio (Радиомодуль)</i> | <p>Точки доступа с двумя радиомодулями</p> <p>Если точка доступа, осуществляющая определение соседней точки доступа, имеет два радиомодуля, отображается поле «Radio» (Радиомодуль).</p> <p>Поле «Radio» (Радиомодуль) показывает, на каком радиомодуле была обнаружена соседняя точка доступа:</p> <ul style="list-style-type: none">• wlan0 (первый радиомодуль)• wlan1 (второй радиомодуль) <p>Точки доступа с одним радиомодулем</p> <p>Это поле не отображается на экранах <i>Neighboring Access Points (Соседние точки доступа)</i> точек доступа с одним радиомодулем.</p> |
| <i>Beacon Int. (Интервал маячка)</i> | <p>Показывает интервал маячка (см. Маячок), используемый данной точкой доступа.</p> <p>Точка доступа передает кадры маячка через равные промежутки времени, объявляя о существовании беспроводной сети. По умолчанию передается один кадр маячка каждые 100 миллисекунд (или 10 в секунду).</p> <p>Интервал маячка устанавливается на вкладке <i>Manage (Управление) > 802.11 Advanced Settings (Расширенные параметры 802.11)</i> (см. Гл. 16: «Настройка параметров радиомодуля 802.11»).</p> |

Табл. 11.5 Статистика соседних точек доступа (Продолжение)

| Поле | Описание |
|-------------------------------------|---|
| <i>Capability (Емкость)</i> | Шестнадцатеричное число, которое после конвертации в двоичное определяет все функции и возможности IEEE 802,11 , а также их состояние («вкл.» или «выкл.») для данной точки доступа. |
| <i>Type (Тип)</i> | Указывает тип устройства: <ul style="list-style-type: none">• «AP» (точка доступа) указывает на то, что соседнее устройство является точкой доступа, поддерживающей стандарт IEEE 802.11 Инфраструктура беспроводной сети в режиме Режим инфраструктуры.• «Ad hoc» (прямое подключение) указывает на то, что соседняя станция работает в режиме Режим прямого подключения. Станции, работающие в режиме прямого подключения, взаимодействуют друг с другом непосредственно, не используя традиционную точку доступа. Режим прямого подключения является средой IEEE 802.11 Инфраструктура беспроводной сети, также известной как «одноранговый» режим или независимый основной набор служб (IBSS). |
| <i>SSID</i> | <p>Идентификатор набора служб (SSID) для точки доступа.</p> <p>SSID — это буквенно-цифровая строка, состоящая не более чем из 32 символов, которая является уникальным идентификатором беспроводной локальной сети. Она также называется <i>Network Name (Сетевое имя)</i>.</p> <p>Настройка SSID выполняется на вкладке «Basic Settings» (Базовые параметры) (см. Гл. 5: «Настройка базовых параметров») или в меню <i>Manage (Управление) > Wireless Settings (Параметры беспроводной сети)</i> (см. Гл. 13: «Настройка беспроводного интерфейса»).</p> <p>Гостевая и внутренняя сети, работающие на той же точке доступа, должны иметь разные сетевые имена.</p> |
| <i>Privacy (Конфиденциальность)</i> | <p>Определяет наличие системы безопасности на соседнем устройстве.</p> <ul style="list-style-type: none">• Off (Выкл.) указывает на то, что для режима безопасности соседнего устройства задано значение «None» (Нет) (режим безопасности отключен).• On (Вкл.) указывает на то, что на соседнем устройстве включен режим безопасности. <p>Настройка режима безопасности осуществляется на вкладке <i>Security (Безопасность)</i> точки доступа. Для получения дополнительной информации о параметрах системы безопасности см. Гл. 10: «Настройка режимов безопасности».</p> |
| <i>WPA</i> | Указывает на состояние режима безопасности WPA точки доступа (On (Вкл.) или Off (Выкл.)). |

Табл. 11.5 Статистика соседних точек доступа (Продолжение)

| Поле | Описание |
|---------------------------------|---|
| <i>Band (Диапазон)</i> | <p>Указывает на то, что на данной точке доступа используется режим IEEE 802.11. (Например, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.)</p> <p>Отображаемое число указывает на используемый режим в соответствии со следующей схемой:</p> <ul style="list-style-type: none">• 2.4 — режим IEEE 802.11b или IEEE 802.11g;• 5 — режим IEEE 802.11a. |
| <i>PHY (Физический уровень)</i> | <p>Указывает на то, что на данной точке доступа используется режим IEEE 802.11. (Например, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.)</p> <p>Отображаемое число указывает на используемый режим в соответствии со следующей схемой:</p> <ul style="list-style-type: none">• 4 — режим IEEE 802.11b;• 7 — режим IEEE 802.11g;• 8 — режим IEEE 802.11a;• 256 — режим Atheros Turbo. |
| <i>Channel (Канал)</i> | <p>Показывает текущий канал вещания точки доступа.</p> <p>Канал определяет часть спектра радиоволн, которую радиомодуль использует для передачи и получения данных.</p> <p>Настройка канала осуществляется на странице <i>Radio Settings (Параметры радиомодуля)</i> (см. Гл. 16: «Настройка параметров радиомодуля 802.11»).</p> |
| <i>Rate (Скорость)</i> | <p>Показывает скорость (в мегабитах в секунду) передачи данных точки доступа.</p> <p>Текущая скорость всегда будет одной из поддерживаемых скоростей, указанных в разделе <i>Rates (Скорости)</i>.</p> |
| <i>Signal (Сигнал)</i> | <p>Указывает силу радиосигнала, исходящего из точки доступа, в децибелах (дБ).</p> |

Табл. 11.5 Статистика соседних точек доступа (Продолжение)

| Поле | Описание |
|-------------------------|---|
| <i>ERP</i> | <p>Протокол <i>Extended Rate Protocol (ERP)</i> используется станциями IEEE 802.11g.</p> <p>Это поле указывает, как клиентская станция IEEE 802.11g, использующая данную точку доступа, должна отправлять данные, когда станции или точки доступа IEEE 802.11b (не использующие протокол ERP) и станция IEEE 802.11g (использующая протокол ERP) присутствуют на одном канале.</p> <p>Если станция IEEE 802.11g определяет, что один или несколько узлов сети IEEE 802.11b используют тот же канал, что и эта сеть, на ней включается защита типа <i>request-to-send</i> (запрос передачи данных, RTS) и <i>clear-to-send</i> (разрешение на передачу данных, CTS).</p> <p>Число, отображаемое на текущем пользовательском интерфейсе, является шестнадцатеричным числом, которое при конвертации в бинарное показывает настройки флажка ERP.</p> <p>Для определения текущего параметра ERP для данной точки доступа используйте следующую схему.</p> <ul style="list-style-type: none">• 0x0 — «нет». Не найдены станции IEEE 802.11b (не использующие протокол ERP).• 0x1 — присутствует одно устройство IEEE 802.11b (не использующее протокол ERP). Данная точка доступа имеет одну станцию, работающую только в режиме IEEE 802.11b (нельзя использовать только один этот флажок).• 0x2 — станции IEEE 802.11g должны использовать защиту RTS/CTS. На канале есть другая точка доступа с клиентскими станциями, работающими только в режиме IEEE 802.11b.• 0x3 — присутствует устройство, не использующее протокол ERP, и станции IEEE 802.11g должны использовать защиту RTS/CTS.• 0x4 — станции IEEE 802.11g должны использовать преамбулу «последовательность Баркера».• 0x5 — станции IEEE 802.11g должны использовать протокол, предусмотренный в 0x1, и преамбулу «последовательность Баркера».• 0x6 — станции IEEE 802.11g должны использовать протокол, предусмотренный в 0x2, и преамбулу «последовательность Баркера».• 0x7 — станции IEEE 802.11g должны использовать протокол, предусмотренный в 0x3, и преамбулу «последовательность Баркера». |
| <i>Beacons (Маячки)</i> | <p>Показывает общее количество маячков, переданных точкой доступа с момента ее последнего запуска.</p> |

Табл. 11.5 Статистика соседних точек доступа (Продолжение)

| Поле | Описание |
|--|---|
| <i>Last Beacon</i> (Последний маячок) | Показывает дату и время последнего маячка, переданного точкой доступа. |
| <i>Rates</i> (Скорости) | <p>Показывает диапазоны поддерживаемой и базовой (заявленной) скорости для соседней точки доступа. Скорости указываются в мегабитах в секунду (Мбит/с).</p> <p>Список содержит все поддерживаемые скорости (Supported Rates), при этом базовые скорости (Basic Rates) выделены полужирным шрифтом.</p> <p>Настройка диапазонов скорости осуществляется на странице <i>Radio Settings</i> (Параметры радиомодуля) (см. Гл. 16: «Настройка параметров радиомодуля 802.11»). Показатели скорости, отображаемые для точки доступа, всегда будут совпадать с показателями, указанными для данной точки доступа на ее странице <i>Radio Settings</i> (Параметры радиомодуля).</p> |

ИНТЕРФЕЙС ETHERNET (ПРОВОДНОЙ)

12

| | |
|---|-----|
| 12.1 Переход к параметрам Ethernet/проводной сети. | 149 |
| 12.1.1 Имя хоста DNS. | 151 |
| 12.1.2 Гостевой доступ | 151 |
| 12.1.2.1 Настройка внутренней сети LAN и гостевой сети. | 151 |
| 12.1.2.2 Включение и отключение гостевого доступа. | 152 |
| 12.1.2.3 Настройка виртуальной гостевой сети | 152 |
| 12.1.3 Виртуальные беспроводные сети. | 153 |
| 12.1.4 Параметры внутреннего интерфейса. | 154 |
| 12.1.5 Параметры гостевого интерфейса | 157 |
| 12.1.6 Обновление параметров. | 158 |

На экране **Ethernet (Wired) Settings** (Параметры Ethernet/проводной сети) находятся параметры настройки **Ethernet** локальной сети (**LAN**).



*Примечание. Параметры Ethernet не являются общими для всего кластера. Эти параметры настраиваются отдельно для каждой точки доступа с помощью интерфейса администрирования. Чтобы перейти в интерфейс администрирования точки доступа, находящейся в текущем кластере, нажмите на ссылку **IP Address** (IP-адрес) в разделе **Cluster** (Кластер) > **Access Points** (Точки доступа) на текущей точке доступа. Дополнительную информацию о том, какие параметры являются общими для всего кластера, см. в разделе «Какие параметры являются/не являются общими в конфигурации кластера?» на стр. 61.*

12.1 Переход к параметрам Ethernet/проводной сети

Чтобы настроить адрес проводной сети и сопутствующие параметры на беспроводном шлюзе 9160 G2 Wireless Gateway, перейдите на вкладку *Manage* (Управление) > *Ethernet Settings* (Параметры Ethernet) и внесите изменения в настройки, как указано ниже.

Рис. 12.1 Обзор параметров Ethernet

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Modify Ethernet (Wired) settings

DNS Hostname

PTX9160-Wireless-AP

Guest Access

Enabled

Disabled

For Guest Access

VLAN on Ethernet Port

Virtual Wireless Networks (Using VLANs on Ethernet Port 1)

Enabled

Disabled

Internal Interface Settings

MAC Address

00:08:A2:01:4B:52

VLAN ID

2

Management VLAN ID

2

Untagged VLAN

Enabled

Disabled

Untagged VLAN ID

1

Connection Type

DHCP

Static IP Address

192168110

Subnet Mask

2552552550

Default Gateway

1921681254

DNS Settings via DHCP

On

Off

DNS Nameservers

DNS Domain

example.com

Guest Interface Settings

MAC Address

00:00:00:00:00:00

VLAN ID

Subnet

n/a

Update

12.1.1 Имя хоста DNS

Табл. 12.1 Настройка имени DNS

| Поле | Описание |
|--|--|
| <i>DNS Hostname</i> (Имя хоста DNS) | <p>В этом текстовом поле указывается имя DNS для точки доступа.</p> <p>Это имя хоста, которое можно уточнить у поставщика услуг Интернета или у системного администратора. Также можно указать имя самостоятельно.</p> <p>Системные имена подчиняются следующим правилам:</p> <ul style="list-style-type: none">• Длина имени должна быть не более 20 символов.• Можно использовать только буквы, цифры и тире.• Имя должно начинаться с буквы и заканчиваться либо буквой, либо цифрой. |

12.1.2 Гостевой доступ

На одном и том же беспроводном шлюзе 9160 G2 Wireless Gateway можно организовать изолированную сеть для гостевого доступа и защищенную внутреннюю сеть LAN.

12.1.2.1 Настройка внутренней сети LAN и гостевой сети

Локальная сеть (LAN) — это коммуникационная сеть, охватывающая ограниченную зону, например один этаж здания. LAN соединяет множество компьютеров и других сетевых устройств, таких как системы хранения данных и принтеры.

Ethernet — наиболее распространенная технология реализации LAN.

Wi-Fi (IEEE) — еще одна очень популярная технология LAN.

Беспроводной шлюз 9160 G2 Wireless Gateway позволяет настроить две разных LAN на одной и той же точке доступа: защищенную *внутреннюю* LAN и общедоступную *гостевую* сеть, в которой не применяются никакие механизмы безопасности и почти никогда не предоставляется доступ к внутренним ресурсам. Для настройки этих двух сетей необходимо задать параметры беспроводной сети и параметры Ethernet (проводной сети).

Сведения о настройке параметров Ethernet (проводной сети) приведены в следующих разделах.

Информацию о настройке параметров беспроводной сети см. в Гл. 13: «Настройка беспроводного интерфейса». Обзор настроек гостевого интерфейса см. в Гл. 14: «Настройка гостевого доступа».

12.1.2.2 Включение и отключение гостевого доступа

Беспроводной шлюз 9160 G2 Wireless Gateway оснащен встроенной функцией гостевого доступа, которая по умолчанию **отключена**. Если требуется предоставить гостевой доступ на точке доступа, включите гостевой доступ на вкладке *Ethernet (Wired) Settings (Параметры Ethernet/проводной сети)*.

Табл. 12.2 Включение и отключение гостевого доступа

| Поле | Описание |
|---------------------------------------|---|
| <i>Guest Access (Гостевой доступ)</i> | <p>По умолчанию встроенная функция гостевого доступа, реализованная в беспроводном шлюзе 9160 G2 Wireless Gateway, отключена.</p> <ul style="list-style-type: none">• Чтобы включить гостевой доступ, нажмите Enabled (Включено).• Чтобы отключить гостевой доступ, нажмите Disabled (Отключено). |

12.1.2.3 Настройка виртуальной гостевой сети

После включения гостевого доступа на точке доступа необходимо создать две *виртуальные* сети: «внутреннюю» и «гостевую». Для этого подключите порт LAN точки доступа к порту с соответствующим обозначением на коммутаторе, поддерживающем *VLAN*, затем укажите две виртуальные LAN на экране администрирования (для получения дополнительной информации см. Гл. 14: «Настройка гостевого доступа»). Создайте виртуально выделенные LAN, внутреннюю и гостевую, следуя инструкциям в Табл. 12.3.

Табл. 12.3 Настройка виртуальной гостевой сети

| Поле | Описание |
|---------------------------------------|--|
| <i>Guest Access (Гостевой доступ)</i> | <ul style="list-style-type: none">• Выберите Enabled (Включено), чтобы включить гостевой доступ. Если выбран этот вариант, в следующем параметре <i>For Guest access use (Для гостевого доступа)</i> необходимо выбрать VLAN и задать остальные параметры VLAN для этой гостевой сети.• Выберите Disabled (Отключено), чтобы отключить гостевой доступ. |

Табл. 12.3 Настройка виртуальной гостевой сети (Продолжение)

| Поле | Описание |
|---|--|
| <i>For Guest Access (Для гостевого доступа)</i> | <p>Укажите виртуально выделенную гостевую сеть для данной точки доступа:</p> <ul style="list-style-type: none">Поскольку точка доступа использует только одно физическое подключение к внутренней LAN, выберите в раскрывающемся меню пункт VLAN on Ethernet Port 1 (VLAN на порту Ethernet 1). После этого станут активны параметры VLAN, и вы сможете задать идентификатор VLAN. См. раздел «Параметры гостевого интерфейса» на стр. 157. <p>Важно! Во время перенастройки гостевого и внутреннего интерфейсов для работы с VLAN подключение к точке доступа может быть потеряно. Прежде всего необходимо проверить, поддерживает ли коммутатор и сервер DHCP развертывание VLAN по стандарту IEEE 802.1Q. После завершения настройки параметров VLAN на экране <i>Manage (Управление)</i> > <i>Ethernet Settings (Параметры Ethernet)</i> повторно подключите физический кабель Ethernet к порту для передачи тегированных пакетов (VLAN). Затем с помощью веб-страниц администрирования выполните повторное подключение к новому IP-адресу. При необходимости обратитесь к администратору инфраструктуры и уточните параметры конфигураций VLAN и DHCP.</p> |

12.1.3 Виртуальные беспроводные сети

Если в качестве внутренней сети требуется настроить VLAN (независимо от того, настроен ли гостевой доступ), можно включить параметр «Virtual Wireless Networks» (Виртуальные беспроводные сети) на точке доступа.

Эту функцию необходимо включить, если требуется настроить дополнительные виртуальные сети в среде VLAN на вкладке *Manage (Управление)* > *VWN*, как указано в разделе «Настройка VLAN» на стр. 179.

Табл. 12.4 Включение виртуальных беспроводных сетей

| Поле | Описание |
|--|---|
| <i>Virtual Wireless Networks (Виртуальные беспроводные сети) (с использованием VLAN на порту Ethernet 1)</i> | <ul style="list-style-type: none">Выберите <i>Enabled (Включено)</i>, чтобы включить VLAN для внутренней сети и дополнительных сетей. Если выбран этот параметр, вы можете развернуть внутреннюю сеть на основе VLAN независимо от того, настроен ли гостевой доступ. Также вы сможете настроить дополнительные сети на основе VLAN с помощью параметров на вкладке <i>Manage (Управление)</i> > <i>VWN</i>, как указано в разделе «Настройка VLAN» на стр. 179.Выберите <i>Disabled (Отключено)</i>, чтобы отключить VLAN для внутренней сети и для всех дополнительных виртуальных сетей на данной точке доступа. |

12.1.4 Параметры внутреннего интерфейса

Чтобы настроить параметры Ethernet (проводной сети) для внутренней LAN, заполните поля, как указано в Табл. 12.5.

Табл. 12.5 Параметры Ethernet для внутренней LAN

| Поле | Описание |
|---|---|
| <i>MAC Address</i> (MAC-адрес) | Отображает адрес MAC для внутреннего интерфейса и порта Ethernet на данной точке доступа. Значение в этом поле доступно только для чтения, и его нельзя изменить. |
| <i>VLAN ID</i> (Идентификатор VLAN) | <p>Это поле активно, если внутренняя и гостевая сети настроены как «VLAN».</p> <p>Укажите число от 1 до 4094 для внутреннего VLAN.</p> <p>После этого точка доступа будет отправлять запросы DHCP с тегом VLAN. На коммутаторе и сервере DHCP должна поддерживаться передача кадров VLAN IEEE 802.1p. Сервер DHCP должен быть доступен для точки доступа.</p> <p>Обратитесь к администратору и уточните параметры конфигураций VLAN и DHCP.</p> |
| <i>Management VLAN ID</i> (Управляющий идентификатор VLAN) | <p>Это поле активно, если VWN или гостевой доступ настроены как VLAN.</p> <p>Введите значение управляющего идентификатора VLAN. В качестве идентификатора можно указать любое значение от 1 до 4094.</p> <p>Управляющий идентификатор VLAN позволяет указать VLAN для управления точкой доступа. После этого точкой доступа можно будет управлять с помощью пользовательского веб-интерфейса, интерфейса командной строки и запросов SNMP, передавая данные по этому VLAN.</p> <p>Если для параметра «Connection Type» (Тип подключения) выбрано значение «DHCP», точка доступа будет отправлять запросы DHCP с тегом VLAN. На коммутаторе и сервере DHCP должна поддерживаться передача кадров VLAN IEEE 802.1Q. Сервер DHCP должен быть доступен для точки доступа.</p> <p>Ограничений на формат управляющего идентификатора VLAN не существует. В качестве управляющего идентификатора VLAN можно указать то же значение, что и для внутреннего идентификатора VLAN, гостевого идентификатора VLAN, идентификатора VWN VLAN или идентификатора VLAN без тегов.</p> |

Табл. 12.5 Параметры Ethernet для внутренней LAN (Продолжение)

| Поле | Описание |
|--|---|
| <i>Untagged VLAN (VLAN без тегов)</i> | <p>Если VWN или гостевой доступ настроены как VLAN, вы можете включить или отключить VLAN без тегов.</p> <p>Выберите Enabled (Включено), чтобы включить <i>VLAN без тегов</i>.</p> <p>Выберите Disabled (Отключено), чтобы отключить <i>VLAN без тегов</i>.</p> <p>Если включен <i>VLAN без тегов</i>, любые полученные пакеты без тега VLAN будут обрабатываться так, как если бы они были снабжены определенным идентификатором VLAN без тегов.</p> <p>Если <i>VLAN без тегов</i> отключен, любые полученные пакеты без тега VLAN перенаправляются на мостовые соединения WDS и никак иначе не обрабатываются точкой доступа.</p> |
| <i>Untagged VLAN ID (Идентификатор VLAN без тегов)</i> | <p>Это поле активно, если включен параметр <i>Untagged VLAN (VLAN без тегов)</i>.</p> <p>Введите значение <i>идентификатора VLAN без тегов</i>. В качестве идентификатора можно указать любое значение от 1 до 4094.</p> <p>Ограничений на формат идентификатора VLAN без тегов не существует. В качестве идентификатора VLAN без тегов можно указать то же значение, что и для внутреннего идентификатора VLAN, гостевого идентификатора VLAN, идентификатора VWN VLAN или управляющего идентификатора VLAN.</p> |

Табл. 12.5 Параметры Ethernet для внутренней LAN (Продолжение)

| Поле | Описание |
|--|---|
| <i>Connection Type</i> (Тип подключения) | <p>Здесь можно выбрать значение DHCP или Static IP (Статический IP).</p> <p><i>Протокол динамического конфигурирования хоста (DHCP)</i> определяет способ, используемый централизованным сервером для предоставления данных о сетевой конфигурации другим устройствам в сети. Сервер DHCP предлагает клиентским устройствам данные «в аренду». Предоставляемые данные включают в себя IP-адреса и маски сети, а также адреса серверов DNS и шлюза.</p> <p>Значение <i>Static IP (Статический IP)</i> указывает, что все параметры сети настраиваются вручную. В этом случае необходимо указать IP-адрес для беспроводного шлюза 9160 G2 Wireless Gateway, маску подсети, IP-адрес шлюза по умолчанию и IP-адрес как минимум одного сервера имен DNS.</p> <p>Если выбрано значение DHCP, беспроводной шлюз 9160 G2 Wireless Gateway будет получать IP-адрес, маску подсети, DNS и адрес шлюза от серверов DHCP.</p> <p>Если выбрано значение Static IP (Статический IP), необходимо заполнить поля в разделе <i>Static IP Settings (Параметры статического IP)</i>.</p> <p>Важно! Если во внутренней сети отсутствует сервер DHCP и использовать его не планируется, первое, что нужно сделать после включения точки доступа, — изменить значение параметра «Connection Type» (Тип подключения) с «DHCP» на «Static IP» (Статический IP). При изменении значения параметра «Connection Type» (Тип подключения) на «Static IP» (Статический IP), можно либо присвоить точке доступа новый Статический IP-адрес, либо оставить адрес по умолчанию. Рекомендуется присвоить новый адрес, чтобы при последующем добавлении новых устройств 9160 G2 Wireless Gateway в ту же самую сеть IP-адреса этих двух точек доступа остались уникальными.</p> <p>Если требуется восстановить статический IP-адрес, который был задан по умолчанию, можно вернуть заводские настройки точки доступа, как описано в разделе «Сброс конфигурации до заводских настроек по умолчанию» на стр. 358.</p> |
| <i>Static IP Address</i> (Статический IP-адрес) | <p>Эти поля активны, если в качестве типа подключения выбран Static IP (Статический IP).</p> <p>Укажите статический IP-адрес в текстовых полях.</p> |
| <i>Subnet Mask</i> (Маска подсети) | <p>Укажите маску подсети в текстовых полях. Эти данные необходимо запросить у поставщика услуг Интернет или у системного администратора.</p> |

Табл. 12.5 Параметры Ethernet для внутренней LAN (Продолжение)

| Поле | Описание |
|---|--|
| <i>Default Gateway</i> (Шлюз по умолчанию) | Укажите шлюз по умолчанию в текстовых полях. |
| <i>DNS Settings via DHCP</i> (Настройка DNS с помощью DHCP) | Служба доменных имен (DNS) преобразует описательное имя сетевого ресурса в числовой IP-адрес. Если этот параметр включен, IP-адреса для серверов DNS будут присваиваться автоматически через DHCP. Эта настройка доступна, только если для параметра <i>Connection Type</i> (Тип подключения) выбрано значение «DHCP». Если выбрано значение Off (Выкл.), статические IP-адреса необходимо присвоить вручную. |
| <i>DNS Nameservers</i> (Серверы имен DNS) | Служба доменных имен (DNS) преобразует описательное имя сетевого ресурса (например, имя <i>domainname</i> ресурса <i>www.pSIONteklogix.com</i>) в числовой IP-адрес (например, 66.93.138.219). Сервер DNS называется <i>сервером имен</i> . Как правило, существует два сервера имен, основной и дополнительный. |
| <i>DNS Domain</i> (Домен DNS) | Укажите домен для серверов DNS. |

12.1.5 Параметры гостевого интерфейса

Чтобы настроить параметры Ethernet (проводной сети) для гостевого интерфейса, заполните поля, как указано ниже.

Табл. 12.6 Настройка параметров Ethernet для гостевого интерфейса

| Поле | Описание |
|--|--|
| <i>MAC Address</i> (MAC-адрес) | Отображает адрес MAC для гостевого интерфейса и порта Ethernet на данной точке доступа. Значение в этом поле доступно только для чтения, и его нельзя изменить. |
| <i>VLAN ID</i> (Идентификатор VLAN) | Это поле активно , если внутренняя и гостевая сети настроены как «VLAN». Укажите число от 1 до 4094 для гостевого VLAN. |
| <i>Subnet</i> (Подсеть) | Отображает адрес подсети для гостевого интерфейса. Например, 192 . 168 . 1 . 0. |

12.1.6 Обновление параметров

Для обновления параметров Ethernet:

1. Перейдите на экран *Ethernet Settings (Параметры Ethernet)*.
2. Внесите необходимые изменения в параметры Ethernet.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

НАСТРОЙКА БЕСПРОВОДНОГО ИНТЕРФЕЙСА

13

| | |
|--|-----|
| 13.1 Переход к параметрам беспроводной сети | 161 |
| 13.2 Настройка поддержки регулятивного домена 802.11d. | 162 |
| 13.3 Управление регулятивным доменом 802.11h. | 163 |
| 13.4 Настройка радиointерфейса | 164 |
| 13.5 Настройка параметров «внутренней» беспроводной сети | 166 |
| 13.6 Настройка параметров «гостевой» беспроводной сети | 166 |
| 13.7 Обновление параметров беспроводной сети | 167 |

В разделе *Wireless Settings (Параметры беспроводной сети)* содержатся настройки локальной сети (**LAN**), имеющие непосредственное отношение к радиомодулю точки доступа (Режим и **Канал 802.11**) и ее сетевому интерфейсу (**MAC**-адрес для точки доступа и имя беспроводной сети, или **SSID**).

В следующих разделах приведена информация о настройке адресов беспроводной сети и других сопутствующих параметров, включая параметры 802.IQv1, на беспроводном шлюзе 9160 G2 Wireless Gateway.

13.1 Переход к параметрам беспроводной сети

Чтобы задать адрес беспроводной сети для точки доступа, перейдите на вкладку *Manage (Управление) > 802.11 Settings (Параметры 802.11)* на экране *Wireless Settings (Параметры беспроводной сети)* и внесите изменения в настройки, как указано ниже.



Примечание. На рисунке Рис. 13.1 показан экран «Wireless Settings» (Параметры беспроводной сети) для точки доступа с двумя радиомодулями. Веб-страница администрирования точки доступа с одним радиомодулем будет выглядеть несколько иначе.

Рис. 13.1 Настройка параметров беспроводной сети

| | | |
|---------------------------|---|-------------------|
| Basic Settings | Modify wireless settings | |
| User Management | 802.11d Regulatory Domain Support <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled | |
| Cluster | IEEE802.11h support present. | |
| Access Points | Radio Interface | |
| Sessions | Mode | IEEE 802.11g |
| Channel Management | Channel | 6 |
| Wireless Neighborhood | Internal Settings | |
| Security | MAC Address | 00:08:A2:01:4B:56 |
| Status | SSID | SFG |
| Interfaces | Guest Settings | |
| Events | MAC Address | |
| Transmit/Receive | SSID | TEKLOGIX GUEST |
| Client Associations | <input type="button" value="Update"/> | |
| Neighboring Access Points | | |
| Manage | | |
| Ethernet Settings | | |
| 802.11 Settings | | |
| 802.11 Advanced Settings | | |

13.2 Настройка поддержки регулятивного домена 802.11d

Вы можете включить или отключить поддержку регулятивного домена IEEE *802.11d* для широкополосной передачи кода страны точки доступа (см. ниже).

Табл. 13.1 Включение поддержки стандарта 802.11d

| Поле | Описание |
|---|---|
| <i>802.11d Regulatory Domain Support (Поддержка регулятивного домена 802.11d)</i> | <p>При включении поддержки стандарта IEEE 802.11d на точке доступа в маячки точки доступа будет добавляться информация о стране, в которой она находится.</p> <ul style="list-style-type: none">• Чтобы включить поддержку регулятивного домена 802.11d, нажмите Enabled (Включено).• Чтобы отключить поддержку регулятивного домена 802.11d, нажмите Disabled (Отключено). Для точек доступа с двумя радиомодулями во внутреннем интерфейсе отображаются два MAC-адреса, по одному для каждого радиомодуля. <p>Примечание. Стандарт IEEE 802.11d позволяет применять стандартные правила функционирования беспроводных сетей IEEE 802.11 в любой стране без изменения настроек. Благодаря стандарту IEEE 802.11d клиентские станции могут работать в любой стране без изменения настроек. Настройка эталонных точек доступа Devicescape осуществляется производителем с помощью интерфейса командной строки. При этом вводятся коды стран, позволяющие точке доступа работать в определенной стране.</p> |

13.3 Управление регулятивным доменом 802.11h

Табл. 13.2 Стандарт IEEE 802.11h

| Поле | Описание |
|---------------------|---|
| <i>IEEE 802.11h</i> | <p>Значение, отображаемое в интерфейсе администрирования, показывает, включено ли управление регулятивным доменом IEEE 802.11h на точке доступа. Конечный пользователь с правами администратора не может отключить IEEE 802.11h. Следующие сведения приведены только в информационных целях.</p> <p>Стандарт IEEE 802.11h включает две службы, необходимые для использования определенных регулятивных доменов на частоте 5 ГГц. Это служба управления мощностью передачи (TPC) и служба поддержки динамического выбора частоты (DFS).</p> <ul style="list-style-type: none">Служба TPC требует, чтобы в радиочастотных локальных сетях (RLAN), функционирующих в диапазоне 5 ГГц, применялся контроль мощности передачи. Это требование включает в себя соблюдение максимальной выходной мощности передачи и требования к ослаблению для каждого разрешенного канала. В результате снижается уровень помех между локальными сетями и службами спутниковой связи.Служба DFS требует, чтобы в RLAN, функционирующих в диапазоне 5 ГГц, был реализован механизм, предотвращающий работу на одном канале с системами радаров и обеспечивающий унифицированное использование всех доступных каналов. <p>Примечание. Стандарт 802.11h включается автоматически, если точка доступа настроена для работы в любой стране, где стандарт 802.11h является минимальным требованием. В настоящее время поддержка этого стандарта требуется только в странах, относящихся к категории, утвержденной Европейским институтом телекоммуникационных стандартов (ETSI). Поддержка стандарта 802.11h также доступна для Японии.</p> |

Разработчикам точек доступа следует помнить несколько важных моментов, связанных со стандартом IEEE **802.11h**:

- Стандарт 802.11h применяется только к диапазону 802.11a. Он не требуется ни для диапазона 802.11b, ни для диапазона 802.11g.
- При работе в домене с поддержкой стандарта 802.11h для BSS всегда будет включен автоматический выбор канала. Даже если настроить другой канал, эта настройка будет игнорироваться и будет использоваться автоматический выбор канала.
- Если включен стандарт 802.11h, время начальной загрузки увеличивается как минимум на 60 секунд. Это минимальное время, требуемое для сканирования выбранного канала на наличие конфликтов с радарными системами.

- Настройка соединений WDS при включенном стандарте 802.11h может вызывать затруднения. Это связано с тем, что рабочие каналы двух точек доступа, соединенных подключением WDS, могут меняться в зависимости от использования каналов и наличия конфликтов с радарными системами. WDS будет функционировать, только если две точки доступа будут работать на одном и том же канале. Для получения дополнительной информации о WDS см. Гл. 20: «Распределенная беспроводная система».

13.4 Настройка радиоинтерфейса

С помощью радиоинтерфейса можно настроить *Канал* и режим *802,11* радиомодуля, как описано в Табл. 13.3.



Примечание. Для точек доступа с двумя радиомодулями эти параметры необходимо настроить как для первого радиоинтерфейса (Radio Interface One), так и для второго.

Табл. 13.3 Параметры радиоинтерфейса

| Поле | Описание |
|---|---|
| <i>MAC Addresses (MAC-адреса) (отображаются только для точек доступа с двумя радиомодулями)</i> | <p>Этот параметр определяет адреса управления доступом к среде (MAC) для интерфейса.</p> <p>MAC-адреса внутренней и гостевой сети для первого и второго радиоинтерфейса отображаются только для точек доступа с двумя радиомодулями.</p> <p>MAC-адрес является постоянным уникальным аппаратным адресом любого устройства, представляющего интерфейс для сети. MAC-адрес присваивается производителем. Этот адрес нельзя изменить. Значение этого адреса как уникального идентификатора интерфейса отображается только в информационных целях.</p> |

Табл. 13.3 Параметры радиоинтерфейса (Продолжение)

| Поле | Описание |
|------------------------|---|
| <i>Mode (Режим)</i> | <p>Параметр <i>Mode (Режим)</i> определяет стандарт <i>физического уровня (PHY)</i>, используемый радиомодулем.</p> <p>Беспроводной шлюз 9160 G2 Wireless Gateway представлен моделями точки доступа с одним или двумя радиомодулями и одним или двумя диапазонами. Доступные значения параметра <i>Mode (Режим)</i> зависят от модели устройства.</p> <p>Однодиапазонная точка доступа. Для однодиапазонной точки доступа можно выбрать один из следующих режимов:</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g <p>Двухдиапазонная точка доступа. Для двухдиапазонной точки доступа можно выбрать один из следующих режимов, по одному на каждый радиоинтерфейс:</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g• IEEE 802.11a <p>Точка доступа с одним или двумя радиомодулями. Если используется точка доступа с двумя радиомодулями, выберите режим IEEE 802.11 для каждого из двух радиоинтерфейсов. У точки доступа с одним радиомодулем будет только один радиоинтерфейс.</p> |
| <i>Channel (Канал)</i> | <p>Выберите <i>канал</i>. Диапазон доступных каналов и канал, используемый по умолчанию, определяются значением параметра <i>Mode (Режим)</i>, выбранным для радиоинтерфейса.</p> <p>Канал определяет часть радиочастотного спектра, который будет использоваться радиомодулем для передачи и приема сигнала. В каждом режиме доступно несколько каналов, в зависимости от того, насколько этот спектр лицензирован национальными и международными контролирующими органами, такими как Федеральная комиссия по связи США (FCC) или Международный союз телекоммуникаций (ITU-R).</p> <p>По умолчанию используется режим Auto (Авто), и во время запуска устройства автоматически выбирается канал с наименьшей загрузкой.</p> |

13.5 Настройка параметров «внутренней» беспроводной сети

На экране параметров внутренней сети находятся такие параметры, как «*MAC Address*» (MAC-адрес) (доступен только для чтения) и «*Network Name*» (Сетевое имя) (другое название — *SSID*), для внутренней *беспроводной сети* (WLAN), описанные в Табл. 13.4.

Табл. 13.4 Параметры беспроводной сети

| Поле | Описание |
|---|--|
| <i>MAC Address</i> (MAC-адрес) | <p>Отображает один или несколько адресов <i>MAC</i> для внутреннего интерфейса на данной точке доступа. Значение в этом поле доступно только для чтения, и его нельзя изменить.</p> <p>Несмотря на то, что точка доступа в физическом смысле представляет собой одно устройство, в сети она может быть представлена двумя или более узлами, каждый из которых имеет свой уникальный MAC-адрес. Это достигается за счет использования нескольких <i>идентификаторов базового набора служб (BSSID)</i> для одной точки доступа.</p> <p>MAC-адреса, указанные для «внутренней» точки доступа, соответствуют идентификаторам BSSID во «внутреннем» интерфейсе.</p> <p>Для точек доступа с двумя радиомодулями во внутреннем интерфейсе отображается два MAC-адреса, по одному на каждый радиомодуль.</p> |
| <i>Wireless Network Name</i> (Имя беспроводной сети) (<i>SSID</i>) | <p>Введите идентификатор <i>SSID</i> для внутренней WLAN.</p> <p><i>Идентификатор набора служб (SSID)</i> — это буквенно-цифровая строка, состоящая не более чем из 32 символов, которая является уникальным идентификатором беспроводной локальной сети. Она также называется «<i>Network Name</i>» (<i>Сетевое имя</i>). В идентификаторе SSID можно использовать любые символы без ограничений.</p> |

13.6 Настройка параметров «гостевой» беспроводной сети

На экране параметров гостевой сети находятся такие параметры, как «*MAC Address*» (MAC-адрес) (доступен только для чтения) и «*Wireless Network Name*» (Имя беспроводной сети) (*SSID*) для *гостевой сети*, описанные в Табл. 13.5. Если на точке доступа настроено два разных сетевых имени (SSID), становится возможным использование гостевого интерфейса на беспроводном шлюзе 9160 G2 Wireless Gateway. Для получения дополнительной информации см. Гл. 14: «Настройка гостевого доступа».

Табл. 13.5 Параметры гостевой беспроводной сети

| Поле | Описание |
|---|--|
| <i>MAC Address (MAC-адрес)</i> | <p>Отображает MAC-адреса для гостевого интерфейса на данной точке доступа. Значение в этом поле доступно только для чтения, и его нельзя изменить.</p> <p>Несмотря на то, что точка доступа в физическом смысле представляет собой одно устройство, в сети она может быть представлена двумя или более узлами, каждый из которых имеет свой уникальный MAC-адрес. Это достигается за счет использования нескольких <i>идентификаторов базового набора служб (BSSID)</i> для одной точки доступа.</p> <p>MAC-адреса, указанные для «гостевой» точки доступа, соответствуют идентификаторам BSSID в «гостевом» интерфейсе.</p> <p>Для точек доступа с двумя радиомодулями в гостевом интерфейсе отображается два MAC-адреса, по одному на каждый радиомодуль.</p> |
| <i>Wireless Network Name (Имя беспроводной сети) (SSID)</i> | <p>Введите идентификатор <i>SSID</i> для <i>гостевой сети</i>.</p> <p><i>Идентификатор набора служб (SSID)</i> — это буквенно-цифровая строка, состоящая не более чем из 32 символов, которая является уникальным идентификатором беспроводной локальной сети. Она также называется «<i>Network Name</i>» (<i>Сетевое имя</i>). В идентификаторе SSID можно использовать любые символы без ограничений.</p> <p>Для гостевой сети необходимо указать идентификатор SSID, отличный от внутреннего идентификатора SSID и легко распознаваемый в качестве идентификатора «гостевой» сети.</p> |

13.7 Обновление параметров беспроводной сети

Для обновления параметров беспроводной сети:

1. Перейдите на экран *802.11 Settings (Параметры 802.11)*.
2. Внесите необходимые изменения в параметры беспроводной сети.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

НАСТРОЙКА ГОСТЕВОГО ДОСТУПА 14

| | |
|---|-----|
| 14.1 Общие сведения о гостевом интерфейсе | 171 |
| 14.2 Настройка гостевого интерфейса | 172 |
| 14.2.1 Настройка гостевой сети в виртуальной LAN | 172 |
| 14.2.2 Настройка экрана приветствия (каптивный портал). | 173 |
| 14.3 Клиентский доступ в гостевую сеть | 174 |
| 14.4 Пример развертывания. | 175 |

С помощью стандартного *гостевого интерфейса* можно настроить контролируемый гостевой доступ к изолированной сети для беспроводного шлюза 9160 G2 Wireless Gateway. Одну и ту же точку доступа можно настроить для широкополосной передачи и обслуживания двух разных беспроводных сетей: безопасной «внутренней» LAN и общедоступной «гостевой» сети. Гостевые клиенты могут получать доступ в гостевую сеть без имени пользователя или пароля. При входе в систему для гостей отображается *приветственный экран* (другое название — «*каптивный портал*»).

14.1 Общие сведения о гостевом интерфейсе

Вы можете задать уникальные параметры для *гостевых* подключений и изолировать гостевых клиентов от других зон сети с более высоким уровнем конфиденциальности.



Важно! *В гостевой сети не применяются никакие механизмы защиты; единственный разрешенный режим безопасности — Plain Text (Простой текст).*

В то же время вы можете настроить защищенную *внутреннюю* сеть (с помощью той же точки доступа, на которой настраивался гостевой интерфейс). Такая сеть предоставляет полный доступ к внутренней информации и защищена межсетевым экраном, а для безопасного входа требуются учетные данные или сертификат.

Настроить беспроводной шлюз 9160 G2 Wireless Gateway для работы с гостевым интерфейсом можно с помощью одной сети в среде VLAN. Параметры гостевого интерфейса для беспроводного шлюза 9160 G2 Wireless Gateway можно настроить на веб-страницах администрирования. Подробные сведения о настройке этого типа гостевого интерфейса см. в разделе «Настройка гостевой сети в виртуальной LAN» на стр. 172.



Примечания. *При таком способе настройки используются технологии нескольких BSSID и виртуальных LAN (VLAN), встроенные в беспроводной шлюз 9160 G2 Wireless Gateway. Внутренние и гостевые сети реализуются как несколько идентификаторов BSSID на одной и той же точке доступа. При этом каждой сети соответствует уникальное сетевое имя (SSID) в беспроводном интерфейсе и отдельный идентификатор VLAN в проводном интерфейсе.*

*На точках доступа с двумя радиомодулями как к первому, так и ко второму радиомодулю применяются параметры **Guest Management** (Управление гостевым доступом) и **Login** (Вход).*

14.2 Настройка гостевого интерфейса

Чтобы настроить гостевой интерфейс на беспроводном шлюзе 9160 G2 Wireless Gateway, выполните следующие действия.

1. Настройте точку доступа для обслуживания двух *виртуально* разделенных сетей, как указано в разделе ниже, «Настройка гостевой сети в виртуальной LAN».
2. Настройте *приветственный экран* для гостевого каптивного портала, следуя инструкциям в разделе «Настройка экрана приветствия (каптивный портал)» на стр. 173.



*Примечание. Параметры гостевого интерфейса не являются общими для точек доступа, находящихся в одном кластере. Эти параметры настраиваются отдельно для каждой точки доступа с помощью интерфейса администрирования. Чтобы перейти в интерфейс администрирования точки доступа, находящейся в текущем кластере, нажмите на ссылку **IP Address** (IP-адрес) в разделе «Cluster (Кластер)» > «Access Points» (Точки доступа) на текущей точке доступа. Дополнительную информацию о том, какие параметры являются общими для всего кластера, а какие нет, см. в разделе «Какие параметры являются/не являются общими в конфигурации кластера?» на стр. 61.*

14.2.1 Настройка гостевой сети в виртуальной LAN



Примечания. Если требуется настроить гостевую и внутреннюю сеть в виртуальной LAN (VLAN), необходимо убедиться, что коммутатор и сервер DHCP поддерживают использование VLAN.

На предварительном этапе необходимо настроить порт коммутатора для обработки тегированных пакетов VLAN в соответствии со стандартом IEEE 802.1Q.

Параметры гостевого экрана приветствия являются общими для точек доступа, находящихся в одном кластере. При обновлении этих параметров на одной точке доступа конфигурация распространяется на все остальные точки доступа в кластере. Дополнительную информацию о том, какие параметры являются общими для всего кластера, а какие нет, см. в разделе «Какие параметры являются/не являются общими в конфигурации кластера?» на стр. 61.

Чтобы настроить виртуальную и гостевую сеть в виртуальной LAN, выполните следующие действия.

1. Используйте только одно проводное подключение между сетевым портом точки доступа и LAN (убедитесь, что этот порт настроен для обработки тегированных пакетов VLAN).
2. Настройте параметры проводного соединения Ethernet для внутренней и гостевой сетей в среде VLAN, следуя инструкциям в Гл. 12: «Интерфейс Ethernet (проводной)».

Сначала необходимо разрешить гостевой доступ и выбрать параметр *For Internal and Guest access, use two: VLANs (Использовать для внутренней и гостевой сети 2: VLAN)*, как указано в разделе «Настройка виртуальной гостевой сети» на стр. 152.

3. Настройте параметры интерфейса радиомодуля и задайте сетевые имена (идентификаторы SSID) для внутренней и гостевой сети, как указано в Гл. 13: «Настройка беспроводного интерфейса».
4. Настройте гостевую экранную заставку, как указано в разделе «Настройка экрана приветствия (каптивный портал)» на стр. 173.

14.2.2 Настройка экрана приветствия (каптивный портал)

Вы можете настроить или изменить параметры приветственного экрана, который отображается на гостевых клиентах, когда пользователь открывает веб-браузер или пытается выйти в Интернет. Чтобы настроить каптивный портал, выполните следующие действия.

1. Перейдите на вкладку *Manage (Управление) > Guest Login (Гостевой вход)*.

Рис. 14.1 Параметры экрана гостевого входа

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

Modify guest welcome screen settings

Guest User Welcome Screen ☒ Enabled ☐ Disabled

Welcome Screen Text

Thank you for using wireless Guest Access as provided by this 9160 wireless AP. Upon clicking "Accept", you will gain access to our wireless guest network. This network allows

Update

2. Выберите параметр **Enabled** (Включено), чтобы активировать экран приветствия.
3. В поле *Welcome Screen Text* (Текст на экране приветствия) введите текст сообщения, которое будет отображаться для гостей пользователей в каптивном портале.
4. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

14.3 Клиентский доступ в гостевую сеть

После завершения настройки гостевой сети клиенты могут получить доступ к гостевой сети следующим образом.

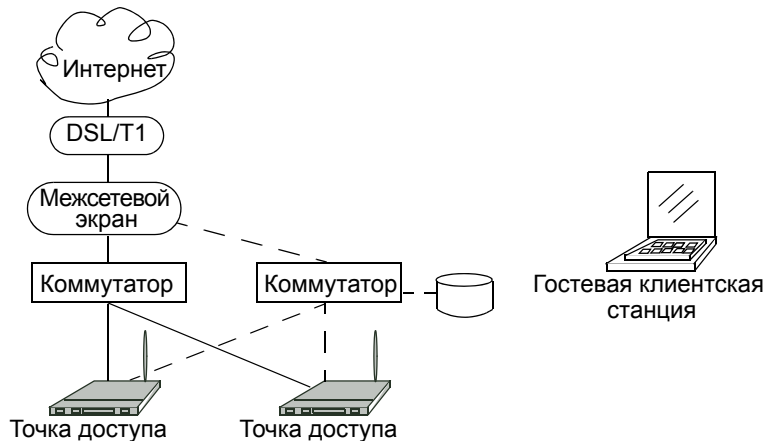
1. Гостевой клиент входит в зону покрытия и выполняет поиск беспроводных сетей.
2. Гостевая сеть объявляет свой гостевой SSID или другое подобное имя, в зависимости от параметров SSID, заданных на веб-страницах администрирования для гостевого интерфейса.
3. Гостевой клиент выбирает гостевой SSID.

4. Гостевой клиент открывает веб-браузер, в котором отображается экран приветствия.
5. На гостевом экране приветствия находится кнопка «Продолжить».
6. После этого гостевой клиент может работать в «гостевой» сети.

14.4 Пример развертывания

На Рис. 14.2 выделенные гостевые подключения обозначены пунктирными линиями. Администрирование всех точек доступа и всех подключений (в том числе гостевых) осуществляется с помощью одних и тех же веб-страниц администрирования беспроводного шлюза 9160 G2 Wireless Gateway.

Рис. 14.2 Выделенные гостевые подключения



| | |
|--|-----|
| 15.1 Переход к параметрам виртуальных беспроводных сетей | 179 |
| 15.2 Настройка VLAN | 179 |
| 15.3 Обновление параметров | 182 |

В следующих разделах приведены инструкции по настройке нескольких беспроводных сетей в виртуальных LAN (*VLAN*).

15.1 Переход к параметрам виртуальных беспроводных сетей

Чтобы настроить несколько сетей в средах VLAN, перейдите на вкладку *Manage* (*Управление*) > *VWN* и внесите изменения в настройки, как указано ниже.

Рис. 15.1 Параметры VWN

| Modify Virtual Wireless Network settings | | | | | |
|--|--------------------------|---------|----------------------------|-------------------------------------|----------|
| Virtual Wireless Networks : Disabled | | | | | |
| VWN | Enabled | VLAN ID | SSID | Broadcast SSID | Security |
| 1 | <input type="checkbox"/> | | Virtual Wireless Network 1 | <input checked="" type="checkbox"/> | None |
| 2 | <input type="checkbox"/> | | Virtual Wireless Network 2 | <input checked="" type="checkbox"/> | None |

15.2 Настройка VLAN



Примечание. Чтобы настроить дополнительные сети в средах VLAN, необходимо сначала разрешить использование виртуальных беспроводных сетей на экране параметров Ethernet. См. раздел «Виртуальные беспроводные сети» на стр. 153.



Важно! При настройке VLAN возможна потеря соединения с точкой доступа. Прежде всего необходимо проверить, поддерживает ли ваш коммутатор и сервер DHCP развертывание VLAN по стандарту IEEE 802.1Q. После завершения настройки VLAN повторно подключите физический кабель Ethernet коммутатора к порту для передачи тегированных пакетов (VLAN). Затем с помощью веб-страниц администрирования выполните повторное подключение к новому IP-адресу. При необходимости обратитесь к администратору инфраструктуры и уточните параметры конфигураций VLAN и DHCP.

Табл. 15.1 Параметры виртуальной беспроводной сети

| Поле | Описание |
|---|--|
| <i>Virtual Wireless Network (Виртуальная беспроводная сеть)</i> | В одной среде можно настроить до 6 сетей VWN. |
| <i>Enabled (Включено)</i> | <p>Вы можете включить или отключить настроенную сеть.</p> <ul style="list-style-type: none">• Чтобы включить определенную сеть, установите флажок <i>Enabled (Включено)</i> рядом с именем соответствующей сети VWN.• Чтобы отключить определенную сеть, снимите флажок <i>Enabled (Включено)</i> рядом с именем соответствующей сети VWN. <p>При отключении сети будет потерян введенный идентификатор VLAN.</p> |
| <i>VLAN ID (Идентификатор VLAN)</i> | <p>Укажите число от 1 до 4094 для внутреннего VLAN.</p> <p>После этого точка доступа будет отправлять запросы DHCP с тегом VLAN. На коммутаторе и сервере DHCP должна поддерживаться передача кадров VLAN IEEE 802.1Q. Сервер DHCP должен быть доступен для точки доступа.</p> <p>Обратитесь к администратору и уточните параметры конфигураций VLAN и DHCP.</p> |
| <i>SSID</i> | <p>Введите имя беспроводной сети в виде строки символов. Это имя будет применяться ко всем точкам доступа в данной сети. По мере добавления новых точек доступа они будут получать этот общий идентификатор SSID.</p> <p>Идентификатор набора служб (Service Set Identifier, SSID) представляет собой строку, состоящую максимум из 32 буквенно-числовых символов.</p> <p>Примечание. Если вы подключены к администрируемой точке доступа с помощью беспроводного клиента, при сбросе SSID соединение с этой точкой доступа будет потеряно. После сохранения новой настройки потребуется повторное подключение к новому SSID.</p> |

Табл. 15.1 Параметры виртуальной беспроводной сети (Продолжение)

| Поле | Описание |
|---|--|
| <i>Broadcast SSID</i> (Широковещательный идентификатор SSID) | <p>Включите параметр <i>Broadcast SSID</i> (Широковещательный идентификатор SSID), установив флажок Broadcast SSID (Широковещательный идентификатор SSID).</p> <p>По умолчанию точка доступа транслирует (разрешает использование) идентификатора набора служб (SSID) в кадрах маячка.</p> <p>Вы можете выключить (запретить) широковещательную трансляцию, чтобы станции не смогли автоматически обнаружить вашу точку доступа. Если передача широковещательного идентификатора SSID точки доступа запрещена, сетевое имя не будет отображаться в списке доступных сетей на клиентской станции. В этом случае для подключения к точке доступа в модуле запроса клиента должно быть указано точное сетевое имя.</p> <p>Примечание. Настраиваемый здесь параметр «Broadcast SSID» (Широковещательный идентификатор SSID) применяется именно к данной виртуальной сети (One (Один) или Two (Два)). В других сетях будут по-прежнему использоваться ранее настроенные режимы безопасности:</p> <ul style="list-style-type: none"> В исходной внутренней сети (настроенной на экране параметров Ethernet) будет использоваться широковещательный идентификатор SSID, заданный в разделе параметров Security (Безопасность). Если в вашей среде настроена гостевая сеть, использование широковещательного идентификатора SSID разрешено всегда. |
| <i>Security</i> (Безопасность) | <p>Выберите режим безопасности для VLAN. Доступны следующие варианты:</p> <ul style="list-style-type: none"> None (Plain-text) (Нет (Простой текст)) Static WEP (Статическое WEP-шифрование) WPA Personal <p>Примечание. Настраиваемый здесь режим безопасности применяется именно к данной виртуальной сети. В других сетях будут по-прежнему использоваться ранее настроенные режимы безопасности:</p> <ul style="list-style-type: none"> В исходной внутренней сети (настроенной на экране параметров Ethernet) будет использоваться режим безопасности, заданный в разделе параметров Security (Безопасность). Если в вашей среде настроена гостевая сеть, всегда выбирайте для режима безопасности вариант None (Нет). |

15.3 Обновление параметров

Для обновления параметров VLAN:

1. Перейдите на вкладку *VWN (Виртуальная беспроводная сеть)*.
2. Внесите необходимые изменения в параметры VLAN.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

НАСТРОЙКА ПАРАМЕТРОВ РАДИОМОДУЛЯ 802.11

16

| | |
|--|-----|
| 16.1 Общие сведения о параметрах радиомодуля | 185 |
| 16.2 Переход к параметрам радиомодуля | 185 |
| 16.3 Настройка параметров радиомодуля | 187 |
| 16.4 Обновление параметров. | 194 |

В следующих разделах приведены инструкции по настройке параметров радиомодуля 802.11 на беспроводном шлюзе 9160 G2 Wireless Gateway.

16.1 Общие сведения о параметрах радиомодуля

Параметры радиомодуля определяют функционирование радиомодуля точки доступа и его взаимодействие с физической средой (то есть, способ излучения и тип электромагнитных волн, излучаемых точкой доступа). Вы можете включить или отключить радиомодуль, задать радиочастоту (RF) широкополосного канала, интервал маячка (промежуток времени между передачей сигналов маячка с точки доступа), мощность передачи, рабочий режим IEEE 802.11 для радиомодуля и т. д. Беспроводной шлюз 9160 G2 Wireless Gateway представляет собой двухдиапазонную точку доступа с одним радиомодулем.

Эта точка доступа поддерживает широкополосную передачу сигнала в следующих режимах:

- Режим IEEE *802.11b*.
- Режим IEEE *802.11g*.
- Режим IEEE *802.11a*.
- Atheros Turbo 5 ГГц.
- Atheros Dynamic Turbo 5 ГГц.
- Atheros Turbo 2,4 ГГц.
- Atheros Dynamic Turbo 2,4 ГГц.
- Расширенный диапазон.



Важно! *Мобильные компьютеры Psion Teklogix не поддерживают режимы Atheros Turbo, поэтому в целях предотвращения передачи ненужных радиосигналов использовать режим Turbo не рекомендуется.*

Режим IEEE с сопутствующими параметрами радиомодуля настраивается в соответствии с инструкциями в разделах «Переход к параметрам радиомодуля» на стр. 185 и «Настройка параметров радиомодуля» на стр. 187.

16.2 Переход к параметрам радиомодуля

Чтобы настроить параметры радиомодуля, перейдите на вкладку *Manage (Управление) > 802.11 Advanced Settings (Расширенные параметры 802.11)*.

На экране *Radio Settings (Параметры радиомодуля)* внесите изменения в настройки, как указано в Табл. 16.1 на стр. 187.

Рис. 16.1 Обзор настройки параметров радиомодуля

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Modify radio settings

Status ☒ On ☐ Off

Mode IEEE 802.11g

Super AG ☐ Enabled ☒ Disabled

Extended Range ☐ Enabled ☒ Disabled

Channel 6

Beacon Interval 100 (Msec, Range: 20 - 2000)

DTIM Period 2 (Range: 1-255)

Fragmentation Threshold 2346 (Range: 256-2346, Even Numbers)

RTS Threshold 2347 (Range: 0-2347)

Maximum Stations 2007 (Range: 0-2007)

Transmit Power 100 Percent

Rate Supported Basic

54 Mbps ☒ ☐

48 Mbps ☒ ☐

36 Mbps ☒ ☐

24 Mbps ☒ ☐

18 Mbps ☒ ☐

12 Mbps ☒ ☐

11 Mbps ☒ ☒

9 Mbps ☒ ☐

6 Mbps ☒ ☐

5.5 Mbps ☒ ☒

2 Mbps ☒ ☒

1 Mbps ☒ ☒

Rate Sets

☐ Broadcast/Multicast Rate Limiting

Rate Limit 50 (packets per second)

Rate Limit Burst 75 (packets per second)

186 Руководство пользователя беспроводного шлюза 9160 G2 Wireless Gateway Psion Teklogix

16.3 Настройка параметров радиомодуля

Табл. 16.1 Параметры радиомодуля

| Поле | Описание |
|---|--|
| <i>Radio (Радиомодуль)</i> | <p>Беспроводной шлюз 9160 G2 Wireless Gateway представлен моделями точки доступа с одним или двумя радиомодулями.</p> <p>Точка доступа с одним радиомодулем. Если используется версия беспроводного шлюза 9160 G2 Wireless Gateway с одним радиомодулем, это поле отсутствует на вкладке Radio (Радиомодуль).</p> <p>Точка доступа с двумя радиомодулями. Если используется версия беспроводного шлюза 9160 G2 Wireless Gateway с двумя радиомодулями, укажите Radio One (Первый радиомодуль) или Radio Two (Второй радиомодуль). Остальные параметры, доступные на этой вкладке для точек доступа с двумя радиомодулями, применяются к радиомодулю, выбранному в этом поле. Не забудьте настроить параметры для обоих радиомодулей.</p> |
| <i>Status (On/Off) (Состояние (Вкл./Выкл.))</i> | <p>Вы можете включить или отключить радиомодуль, выбрав соответствующее значение: On (Вкл.) или Off (Выкл.).</p> |

Табл. 16.1 Параметры радиомодуля (Продолжение)

| Поле | Описание |
|---------------------|--|
| <i>Mode (Режим)</i> | <p>Параметр <i>Mode (Режим)</i> определяет стандарт <i>физического уровня (PHY)</i>, используемый радиомодулем.</p> <p>Беспроводной шлюз 9160 G2 Wireless Gateway представлен моделями точки доступа с одним или двумя диапазонами.</p> <p>Однодиапазонная точка доступа. Для однодиапазонной точки доступа можно выбрать один из следующих режимов:</p> <ul style="list-style-type: none">• <i>IEEE 802.11b</i>• <i>IEEE 802.11g</i> <p>Двухдиапазонная точка доступа. Для двухдиапазонной точки доступа можно выбрать один из следующих режимов:</p> <ul style="list-style-type: none">• <i>IEEE 802.11b</i>• <i>IEEE 802.11g</i>• <i>IEEE 802.11a</i> <p>Примечание. При использовании точки доступа с двумя радиомодулями могут быть доступны различные режимы в зависимости от того, какое значение выбрано в поле «Radio» (Радиомодуль): «Radio One» (Первый радиомодуль) или «Radio Two» (Второй радиомодуль).</p> <p>При выборе режима автоматически выбираются соответствующие диапазоны базовой и поддерживаемой скорости передачи (описание диапазонов скорости передачи приведено далее в этой таблице, см. стр. 192).</p> |
| <i>Super AG</i> | <p>Включение функции Super AG обеспечивает более высокую производительность благодаря увеличению пропускной способности радиомодуля в выбранном режиме радиосвязи (IEEE 802.11b, g, a и т. д.). Обратите внимание, что при включенной функции Super AG на передачу сигналов точки доступа будет расходоваться больший процент полосы пропускания.</p> <ul style="list-style-type: none">• Чтобы включить функцию Super AG, нажмите Enabled (Включено).• Чтобы отключить функцию Super AG, нажмите Disabled (Отключено). |

Табл. 16.1 Параметры радиомодуля (Продолжение)

| Поле | Описание |
|---|--|
| <i>Extended Range</i> (Расширенный диапазон) | <p>Расширенный диапазон Atheros (XR) — это коммерческая реализация метода низкоскоростной передачи трафика на большие расстояния. Этот метод доступен для клиентов и точек доступа с поддержкой XR, а также совместим со стандартом 802.11 в режимах 802.11g и 802.11a. Поддержка Atheros XR, Atheros Turbo 5 ГГц и Atheros Dynamic Turbo 5 ГГц, в режиме 802.11b не реализована.</p> <p>При включении функции Atheros XR расширяется рабочий диапазон клиентов и точек доступа.</p> <ul style="list-style-type: none"> • Чтобы включить расширенный диапазон, нажмите Enabled (Включено). • Чтобы отключить расширенный диапазон, нажмите Disabled (Отключено). <p>Эта функция недоступна, если выбран аппаратный режим IEEE 802.11b, Atheros Turbo 5 ГГц или Atheros Dynamic Turbo 5 ГГц. Расширенный диапазон Atheros XR в этих аппаратных режимах не поддерживается.</p> |
| <i>Channel</i> (Канал) | <p>Канал определяет часть спектра радиоволн, которую радиомодуль использует для передачи и получения данных. Диапазон каналов и канал, используемый по умолчанию, определяются значением параметра «Mode» (Режим), выбранным для радиоинтерфейса.</p> <p>Для большинства режимов по умолчанию используется значение Auto (Авто). Значение Auto (Авто) является рекомендованным для большинства режимов, так как в этом случае включается автоматическое обнаружение лучшего канала, исходя из мощности сигнала, загруженности трафиком и т. д. Тем не менее, вы можете также выбрать любой канал от 1 до 11 включительно.</p> |
| <i>Beacon Interval</i> (Интервал маячка) | <p>Точка доступа передает сигнальные кадры (см. <i>Маячок</i>) через равные промежутки времени, объявляя о существовании беспроводной сети. По умолчанию кадр маячка передается каждые 100 миллисекунд (то есть, в секунду передается 10 таких кадров).</p> <p>Значение параметра <i>Beacon Interval</i> (Интервал маячка) указывается в миллисекундах. Введите значение от 20 до 2000.</p> |

Табл. 16.1 Параметры радиомодуля (Продолжение)

| Поле | Описание |
|---|--|
| <i>DTIM Period (Период DTIM)</i> | <p>В некоторые кадры маячка (см. <i>Маячок</i>) включается такой элемент, как сообщение со схемой данных о доставке трафика (<i>DTIM</i>). Эта схема определяет, для каких клиентских станций, находящихся в данный момент в режиме пониженного энергопотребления, на точке доступа имеются буферизированные данные, ожидающие приема.</p> <p>Указанный в этой настройке период DTIM определяет периодичность, с которой клиенты, обслуживаемые данной точкой доступа, будут проверять наличие буферизированных данных, ожидающих приема.</p> <p>Укажите период DTIM в пределах допустимого диапазона (1-255).</p> <p>Период измеряется в количестве маячков. Например, если задано значение 1, клиенты будут проверять наличие буферизированных на точке доступа данных при получении каждого маячка. Если задано значение 2, клиенты будут выполнять проверку при получении каждого второго маячка. Если задано значение 10, клиенты будут выполнять проверку при получении каждого десятого маячка.</p> |
| <i>Fragmentation Threshold (Порог фрагментации)</i> | <p>Укажите число от 256 до 2346, соответствующее пороговому размеру кадра в байтах.</p> <p>С помощью <i>порога фрагментации</i> можно ограничить размер пакетов (кадров), передаваемых по сети. Если размер пакета превышает заданный порог фрагментации, активируется функция фрагментирования, и пакет передается как несколько кадров 802.11.</p> <p>Если размер пакета меньше или равен указанному пороговому значению, фрагментация не применяется.</p> <p>Если выбрано максимальное значение (2346 байт), фрагментация отключается.</p> <p>Фрагментация создает дополнительную нагрузку на сеть, так как она не только требует дополнительных затрат на разделение и повторную сборку кадров, но и увеличивает объем трафика сообщений в сети. Однако при правильной настройке фрагментации можно применять в целях <i>повышения</i> производительности и надежности сети.</p> <p>Передача кадров меньшего размера (при более низком пороговом значении фрагментации) помогает устранить некоторые проблемы, связанные с помехами, например, от микроволновых печей.</p> <p>По умолчанию фрагментация отключена. Фрагментацию рекомендуется использовать только при подозрении на наличие радиочастотных помех. Дополнительные заголовки, создаваемые для каждого фрагмента, создают дополнительную нагрузку на сеть и могут привести к значительному сокращению пропускной способности.</p> |

Табл. 16.1 Параметры радиомодуля (Продолжение)


| Поле | Описание |
|---|--|
| <i>RTS Threshold</i> (Порог RTS) | <p>Укажите значение «RTS Threshold» (Порог RTS) в пределах от 0 до 2347.</p> <p>Порог RTS определяет размер пакета запроса на передачу (RTS). Этот параметр помогает контролировать поток трафика, проходящий через точку доступа, особенно при большом количестве клиентов.</p> <p>Если указано низкое пороговое значение, пакеты RTS будут отправляться чаще. Это приведет к увеличению потребления полосы пропускания и сокращению пропускной способности пакетов.</p> <p>С другой стороны, передача большего количества пакетов RTS помогает восстановить работоспособность сети в случае помех или конфликтов, которые могут возникать при большой нагрузке на сеть или при возникновении электромагнитных помех.</p> |
| <i>Maximum Stations</i> (Максимальное число станций) | <p>Укажите максимальное число станций, одновременно подключенных к точке доступа.</p> <p>Для этого параметра можно указать значение от 0 до 2007.</p> |
| <i>Transmit Power</i> (Мощность передачи) | <p>Укажите процентное значение мощности передачи для данной точки доступа.</p> <p>По умолчанию точка доступа использует при передаче 100 процентов своей мощности.</p> <p> Рекомендации.</p> <ul style="list-style-type: none"> В большинстве случаев рекомендуется использовать значение по умолчанию (100 процентов мощности). Такой режим мощности более экономичен, так как при этом точка доступа имеет максимальный широкоэмитательный диапазон, что сокращает число необходимых точек доступа. Чтобы увеличить емкость сети, расположите точки доступа ближе друг к другу и установите более низкое значение мощности передачи. Это поможет сократить перекрытие сигналов и помехи между точками доступа. Более низкая мощность передачи также помогает повысить уровень безопасности сети, так как у более слабых сигналов беспроводной сети меньше шансов распространиться за физические границы сети. |

Табл. 16.1 Параметры радиомодуля (Продолжение)

| Поле | Описание |
|---------------------------------------|---|
| <i>Rate Sets (Диапазоны скорости)</i> | <p>Выберите диапазоны скорости передачи, которые должна поддерживать данная точка доступа, и базовые диапазоны скорости, которые будут заявлены точкой доступа.</p> <p>Скорость измеряется в Мбит/с.</p> <ul style="list-style-type: none">• Supported Rate Sets (Поддерживаемые диапазоны скорости) указывают диапазоны скорости, поддерживаемые данной точкой доступа. Вы можете выбрать несколько скоростей (чтобы выбрать скорость или отменить выбор, установите или снимите флажок). Точка доступа автоматически выбирает наиболее эффективную скорость с учетом различных факторов, таких как коэффициент ошибок и расстояние от клиентских станций до точки доступа.• Basic Rate Sets (Базовые диапазоны скорости) указывают скорости, которые точка доступа объявляет в сети, чтобы установить связь с другими точками доступа и клиентскими станциями. Как правило, более эффективны конфигурации, где точка доступа передает в широковещательном режиме набор диапазонов поддерживаемых скоростей. <p>Если необходима поддержка клиентов «b» и «g», измените значение параметра Mode (Режим) радиомодуля на IEEE 802.11g. В веб-интерфейсе будут автоматически выбраны диапазоны скорости по умолчанию, при которых к точке доступа смогут подключаться как клиенты «b», так и клиенты «g».</p> <p>Если необходима поддержка только клиентов «g», измените режим радиомодуля на IEEE 802.11g. В веб-интерфейсе будут автоматически выбраны диапазоны скорости по умолчанию. Затем добавьте диапазоны скорости 24, 12 и 6 в качестве базовых. В этом случае клиенты «b» не смогут установить подключение, так как они не поддерживают эти скорости. В то же время клиенты «g» смогут подключаться к точке доступа, так как они поддерживают эти скорости в соответствии со стандартом.</p> <p>Для получения дополнительной информации см. описание параметра <i>Mode (Режим)</i> далее в этой таблице, на стр. 188.</p> |

Табл. 16.1 Параметры радиомодуля (Продолжение)

| Поле | Описание |
|---|---|
| <i>Включение ограничения скорости для широковещательной/многоадресной передачи</i> | <p>Ограничение скорости широковещательной и многоадресной передачи способствует повышению общей производительности сети, так как при этом ограничивается число пакетов, передаваемых по сети.</p> <p>Некоторые протоколы используют многоадресные и широковещательные пакеты для передачи данных, которые не имеют значения для большинства узлов сети. Например, это могут быть запросы ARP для других компьютеров, сообщения DHCP или BOOTP. В случае с некоторыми протоколами ограничение скорости позволяет ограничить число избыточных пакетов, пересылаемых по сети. Как правило, весь отфильтрованный трафик передается повторно через какое-то время, и такая повторная передача не вызывает проблем.</p> <ul style="list-style-type: none"> • Чтобы включить ограничение скорости для многоадресной и широковещательной передачи, нажмите Enabled (Включено). • Чтобы отключить ограничение скорости для многоадресной и широковещательной передачи, нажмите Disabled (Отключено). <p>По умолчанию параметр <i>Multicast/Broadcast Rate Limiting</i> (Ограничение скорости многоадресной/широковещательной передачи) отключен. Если параметр «Multicast/Broadcast Rate Limiting» (Ограничение скорости многоадресной/широковещательной передачи) отключен, следующие поля будут неактивны.</p> |
| <i>Broadcast/Multicast Rate Limit (Ограничение скорости для широковещательной/многоадресной передачи)</i> | <p>Укажите предельную скорость для многоадресной и широковещательной передачи. Указанное значение должно быть больше 1, но меньше 50 пакетов в секунду. Любой трафик, не превышающий указанный предел, будет считаться нормальным и передаваться в пункт назначения.</p> <p>По умолчанию устанавливается максимальное значение — 50 пакетов в секунду.</p> |
| <i>Broadcast/Multicast Rate Limit Burst (Импульсные передачи при ограничении скорости для широковещательной/многоадресной передачи)</i> | <p>Эта настройка определяет предел скорости импульсных передач трафика, которые можно совершать до тех пор, пока весь трафик не превысит заданное ограничение скорости. Предел импульсной передачи позволяет время от времени импульсно передавать пакеты трафика сверх установленного предела.</p> <p>По умолчанию устанавливается максимальное значение — 75 пакетов в секунду.</p> |

16.4 Обновление параметров

Для обновления параметров радиомодуля:

1. Перейдите на вкладку *802.11 Advanced Settings (Расширенные параметры 802.11)*.
2. Внесите необходимые изменения в параметры радиомодуля.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.



*Примечание. Если используется модель беспроводного шлюза 9160 G2 Wireless Gateway с двумя радиомодулями, обратите внимание, что параметры на этой вкладке необходимо настроить для обоих радиомодулей (первого и второго). Отображаемые параметры применяются либо к первому, либо ко второму радиомодулю, в зависимости от значения, выбранного в поле **Radio (Радиомодуль)** (первое поле на вкладке). Завершив настройку первого радиомодуля, нажмите кнопку **Update** (Обновить), прежде чем перейти к настройке второго радиомодуля. Не забудьте нажать кнопку **Update** (Обновить), чтобы применить вторую группу настроек для второго радиомодуля.*

ФИЛЬТРАЦИЯ MAC-АДРЕСОВ

17

| | |
|--|-----|
| 17.1 Переход к параметрам фильтрации MAC-адресов | 197 |
| 17.2 Использование фильтрации MAC-адресов | 198 |
| 17.3 Обновление параметров | 199 |

Адрес *управления доступом к среде (MAC)* — это аппаратный адрес, являющийся уникальным идентификатором каждого узла сети. Сетевые устройства стандарта IEEE 802 используют распространенный 48-разрядный формат MAC-адреса, который обычно отображается в виде строки из 12 шестнадцатеричных цифр, разделенных двоеточиями, например FE:DC:BA:09:87:65. Каждая беспроводная сетевая плата (*NIC*), используемая беспроводным клиентом, имеет уникальный MAC-адрес.

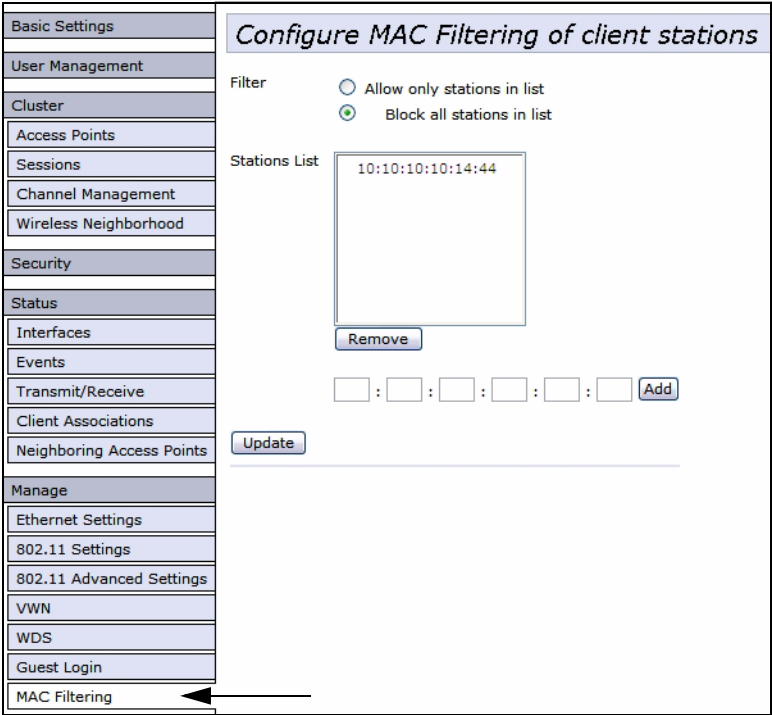
Пользователи могут управлять доступом клиентов к беспроводной сети с помощью настройки *MAC Filtering (Фильтрация MAC-адресов)* и списка утвержденных MAC-адресов. Когда включена настройка «MAC Filtering» (Фильтрация MAC-адресов), доступ к сети могут получать только клиенты с MAC-адресом, находящимся в этом списке.

Использование фильтрации MAC-адресов в беспроводном шлюзе 9160 G2 Wireless Gateway описано в следующих разделах.

17.1 Переход к параметрам фильтрации MAC-адресов

Чтобы включить фильтрацию по MAC-адресу, перейдите на вкладку *Manage (Управление) > MAC Filtering (Фильтрация MAC-адресов)* и внесите изменения в настройки, как указано ниже.

Рис. 17.1 Параметры фильтрации MAC-адресов



17.2 Использование фильтрации MAC-адресов

На этом экране находятся настройки доступа к беспроводному шлюзу 9160 G2 Wireless Gateway. Контроль доступа осуществляется с помощью адресов *управления доступом к среде* (MAC-адресов). В зависимости от выбранных фильтров можно либо *разрешить* доступ только клиентским станциям с MAC-адресом, внесенным в список, либо *запретить* доступ для этих станций.

В гостевом интерфейсе параметры фильтрации *MAC* применяются к обоим *BSS*.

На точках доступа с двумя радиомодулями параметры фильтрации MAC-адресов применяются к обоим радиомодулям.

Табл. 17.1 Параметры фильтрации MAC-адресов

| Поле | Описание |
|--|--|
| <i>Filter</i> (Фильтр) | Чтобы настроить <i>фильтр</i> MAC-адресов, выберите один из переключателей: <ul style="list-style-type: none">• Allow only stations in the list (Разрешить доступ только станциям из списка)• Block all stations in list (Заблокировать все станции в списке) |
| <i>Stations List</i> (Список станций) | Чтобы добавить MAC-адрес в список станций, введите 48-разрядный MAC-адрес в нижние текстовые поля и нажмите Add (Добавить). MAC-адрес появится в списке станций. Чтобы удалить MAC-адрес из списка станций, выберите 48-разрядный MAC-адрес и нажмите Remove (Удалить). В зависимости от выбранных настроек фильтра станциям, внесенным в список, будет разрешено или запрещено подключаться к точке доступа. |

17.3 Обновление параметров

Для обновления параметров MAC:

1. Перейдите на вкладку *MAC Filtering* (Фильтрация MAC-адресов).
2. Внесите необходимые изменения в параметры MAC.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

| | |
|--|-----|
| 18.1 Общие сведения о балансировке нагрузки | 203 |
| 18.1.1 Выявление нарушений баланса. Точки доступа с чрезмерной и недостаточной нагрузкой. | 203 |
| 18.1.2 Настройка ограничений для использования и клиентских соединений | 204 |
| 18.1.3 Балансировка нагрузки и QoS | 204 |
| 18.2 Переход к параметрам балансировки нагрузки | 204 |
| 18.3 Настройка балансировки нагрузки | 205 |
| 18.4 Обновление параметров | 207 |

Беспроводной шлюз 9160 G2 Wireless Gateway позволяет равномерно распределять нагрузку от подключений беспроводных клиентов по всем имеющимся точкам доступа. Балансировка нагрузки позволяет предотвратить ситуации, когда одна точка доступа в сети вынуждена обрабатывать чрезмерный объем беспроводного трафика, что приводит к снижению ее производительности.

В следующих разделах приведена информация о том, как настроить балансировку нагрузки в беспроводной сети.

18.1 Общие сведения о балансировке нагрузки

Как и большинство параметров настройки беспроводного шлюза 9160 G2 Wireless Gateway, параметры балансировки нагрузки являются общими для всех точек доступа, объединенных в кластер.



Примечание. В некоторых случаях может потребоваться установить отдельные ограничения для одной определенной точки доступа, которая постоянно работает в режиме перегрузки. Также можно применить уникальные параметры к точке доступа, работающей в автономном режиме (см. разделы «Общие сведения о кластеризации» на стр. 60 и «Переход к управлению точками доступа» на стр. 59).

18.1.1 Выявление нарушений баланса. Точки доступа с чрезмерной и недостаточной нагрузкой

Как правило, сравнение статистики по данным клиентских соединений и данным приема/передачи для нескольких точек доступа позволяет выявить точки доступа, которые постоянно обрабатывают непропорционально большие объемы беспроводного трафика. Это может быть связано с особенностями среды или другими факторами, из-за которых самый сильный сигнал для большинства клиентов в сети передается одной точкой доступа. По умолчанию большинство клиентских запросов поступает на эту точку доступа, в то время как остальные точки доступа большую часть времени находятся в режиме бездействия.

Нарушения баланса распределения беспроводного трафика по точкам доступа четко прослеживаются в статистике Client Association data and Transmit/Receive (Данные клиентских соединений и прием/передача), где перегруженные точки доступа имеют более высокий показатель использования, а точки доступа с недостаточной нагрузкой — более высокий показатель бездействия. Точка доступа, вынужденная обрабатывать больший объем трафика, чем тот, на который она рассчитана, может демонстрировать более низкую скорость передачи данных, обусловленную перегрузкой.

18.1.2 Настройка ограничений для использования и клиентских соединений

Для корректировки нерационального использования точек доступа можно включить режим балансировки нагрузки и установить ограничения на процент использования и число клиентских соединений, разрешенное для той или иной точки доступа.

18.1.3 Балансировка нагрузки и QoS

Балансировка нагрузки также играет важную роль в обеспечении требуемого *качества обслуживания (QoS)* в системах *передачи голоса по IP (VoIP)* и других чувствительных ко времени приложений, конкурирующих между собой за полосу пропускания и своевременный доступ к радиочастотному спектру беспроводной сети. Дополнительную информацию о влиянии конфигурации сети на уровень QoS см. в Гл. 19: «Качество обслуживания (QoS)».

18.2 Переход к параметрам балансировки нагрузки

В интерфейсе администрирования перейдите на вкладку *Manage (Управление) > Load Balancing (Балансировка нагрузки)* и внесите изменения в настройки, как указано в следующем разделе.

Рис. 18.1 Параметры балансировки нагрузки

| | |
|---------------------------|--|
| Basic Settings | Modify load balancing settings Load Balancing <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Utilization for No New Associations <input type="text" value="0"/> (Percent, 0 disables) Utilization for Disassociation <input type="text" value="0"/> (Percent, 0 disables) Station Threshold for Disassociation <input type="text" value="0"/> Range 1 - 2007, 0 disables. <input type="button" value="Update"/> |
| User Management | |
| Cluster | |
| Access Points | |
| Sessions | |
| Channel Management | |
| Wireless Neighborhood | |
| Security | |
| Status | |
| Interfaces | |
| Events | |
| Transmit/Receive | |
| Client Associations | |
| Neighboring Access Points | |
| Manage | |
| Ethernet Settings | |
| 802.11 Settings | |
| 802.11 Advanced Settings | |
| VWN | |
| WDS | |
| Guest Login | |
| MAC Filtering | |
| Load Balancing | |

18.3 Настройка балансировки нагрузки

Чтобы настроить балансировку нагрузки, *включите параметр Load Balancing* (Балансировка нагрузки), затем установите ограничения и выберите действия, которые будут выполняться при достижении определенного показателя использования на данной точке доступа.



Примечания. *Даже когда клиенты будут отключены от этой точки доступа, качество обслуживания клиентских станций не снизится, если в том же диапазоне будет находиться другая точка доступа, к которой клиенты смогут подключиться для возобновления доступа в сеть. Клиенты должны автоматически осуществлять повторные попытки подключения к исходной точке доступа и проверять наличие других точек доступа в той же подсети. Клиенты, отключенные от одной точки доступа, должны мгновенно и беспрепятственно переключаться на другую точку доступа в той же подсети.*


Параметры балансировки нагрузки применяются ко всему объему трафика на точках доступа. Если разрешен гостевой доступ, эти параметры применяются одновременно к внутренней и к гостевой сети.

На точках доступа с двумя радиомодулями параметры балансировки нагрузки применяются к обоим радиомодулям, но нагрузка для каждого модуля подсчитывается отдельно и включает в себя статистику как для внутренней, так и для гостевой сети (если разрешен гостевой доступ).

Табл. 18.1 Параметры балансировки нагрузки

| Поле | Описание |
|--|---|
| <i>Load Balancing</i> (Балансировка нагрузки) | Чтобы включить балансировку нагрузки для текущей точки доступа, нажмите Enable (Включить). Чтобы отключить балансировку нагрузки для текущей точки доступа, нажмите Disable (Отключить). |
| <i>Utilization for No New Associations</i> (Использование с запретом новых подключений) | Ограничения использования связаны с показателями потребления полосы пропускания. Укажите процентное ограничение потребления полосы пропускания для текущей точки доступа. По достижении указанного значения точка доступа перестанет принимать от клиентов новые запросы на подключение. Если настроенное для точки доступа ограничение будет превышено, к этой точке доступа больше не сможет подключиться ни один новый клиент. Если в этом поле указано значение 0 , точка доступа будет принимать все запросы на подключение независимо от установленных ограничений использования. |
| <i>Utilization for Disassociation</i> (Использование с отсоединением клиентов) | Ограничения использования связаны с показателями потребления полосы пропускания. Укажите процентное ограничение потребления полосы пропускания для текущей точки доступа. По достижении указанного значения точка доступа будет отключать текущих клиентов. Если настроенное для точки доступа ограничение будет превышено, от этой точки будет отключен один из текущих клиентов. Если в этом поле указано значение 0 , точка доступа никогда не будет отключать текущих клиентов независимо от установленных ограничений использования. |

Табл. 18.1 Параметры балансировки нагрузки (Продолжение)

| Поле | Описание |
|--|--|
| <i>Stations Threshold for Disassociation</i> (Порог отключения станций) | <p>Укажите число клиентских станций, которое будет использоваться в качестве порогового значения для отключения станций от точки доступа. Пока число одновременно подключенных к точке доступа клиентских станций не превышает указанное значение, от точки доступа не будет отключена ни одна станция, независимо от значения параметра <i>Utilization for Disassociation</i> (Использование с отсоединением клиентов).</p> <p>Теоретически к одной точке доступа может быть одновременно подключено не более 2007 клиентских станций.</p> <p> Рекомендуемое значение для этого параметра — от 30 до 50 клиентских станций. Такое число одновременно подключенных станций обеспечивает посильную нагрузку для точки доступа при условии, что полоса пропускания совместно используется всеми клиентами.</p> |

18.4 Обновление параметров

Для обновления параметров балансировки нагрузки:

1. Перейдите на вкладку *Load Balancing* (Балансировка нагрузки).
2. Внесите необходимые изменения в параметры балансировки нагрузки.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

КАЧЕСТВО ОБСЛУЖИВАНИЯ (QoS) 19

| | |
|--|-----|
| 19.1 Общие сведения о QoS | 211 |
| 19.1.1 QoS и балансировка нагрузки | 211 |
| 19.1.2 Поддержка стандартов 802.11e и WMM. | 212 |
| 19.1.3 Очереди QoS и параметры для координирования потоков трафика. | 212 |
| 19.1.3.1 Очереди QoS и типы обслуживания пакетов (ToS) | 213 |
| 19.1.3.2 EDCF — управление кадрами данных и арбитражными межкадровыми интервалами | 215 |
| 19.1.3.3 Произвольная задержка и минимальные/максимальные окна коллизии | 216 |
| 19.1.3.4 Импульсная передача пакетов для повышения производительности | 217 |
| 19.1.3.5 Интервал потенциальной передачи (TXOP) для клиентских станций | 217 |
| 19.1.4 802.1p и теги DSCP | 217 |
| 19.1.4.1 Приоритет VLAN | 219 |
| 19.1.4.2 Приоритет DSCP | 220 |
| 19.2 Настройка очередей QoS. | 221 |
| 19.2.1 Настройка параметров EDCA для точки доступа. | 222 |
| 19.2.2 Включение/отключение поддержки Wi-Fi Multimedia | 225 |
| 19.2.3 Настройка параметров EDCA для станции | 225 |
| 19.3 Обновление параметров | 228 |

Параметры качества обслуживания (Quality of Service, **QoS**) можно использовать для создания нескольких очередей, обеспечивая повышение пропускной способности и производительности при передаче дифференцированного беспроводного трафика, такого как *передача голоса по IP* (VoIP) и другие типы аудио, видео и потоковых мультимедийных данных, а также при передаче обычных данных по IP через беспроводной шлюз 9160 G2 Wireless Gateway.

В следующих разделах приведены инструкции по настройке параметров очередей качества обслуживания на беспроводном шлюзе 9160 G2 Wireless Gateway.

19.1 Общие сведения о QoS

Основным фактором, влияющим на уровень QoS, является перегрузка сети, связанная с увеличением числа клиентов, пытающихся получить доступ к радиоволнам, а также с большими объемами трафика, конкурирующими за полосу пропускания в периоды пиковой дневной активности. Наиболее ярко снижение качества обслуживания в перегруженной сети проявляется в работе чувствительных ко времени приложений, таких как приложения для трансляции видео, *передачи голоса по IP* (VoIP) и потоковой передачи мультимедийных данных.

В отличие от обычных файлов данных, которые меньше страдают от нестабильного уровня QoS, видеоданные, данные VoIP и потоковые трансляции мультимедийных данных должны передаваться в определенном порядке при постоянной скорости и с минимальными задержками между передачей пакетов (см. **Пакет**). Снижение качества обслуживания приводит к искажению звука или видеоизображения.

19.1.1 QoS и балансировка нагрузки

Правильная комбинация балансировки нагрузки (см. Гл. 18: «Балансировка нагрузки») и методов QoS позволяет обеспечивать высокое качество обслуживания для чувствительных ко времени приложений даже в загруженной сети.

Балансировка нагрузки — это способ более эффективного распределения объемов трафика по точкам доступа. QoS — это способ выделения полосы пропускания и доступа в сеть на основе приоритетов передачи, присваиваемых различным типам беспроводного трафика в пределах одной точки доступа.

19.1.2 Поддержка стандартов 802.11e и WMM

QoS включает различные технологии управления потоками данных, передаваемых по общим сетевым каналам. В настоящее время рабочая группа **IEEE 802.11e** занимается разработкой стандарта QoS, который будет регулировать качество передачи и доступность обслуживания в беспроводных сетях. QoS позволяет повысить эффективность сети следующими способами: минимизация перегрузки сети, ограничение искажений (см. *Искажения*), задержек (см. *Запаздывание*) и потерь пакетов (см. *Потеря пакетов*), поддержка выделенной полосы пропускания для чувствительных ко времени и критически важных приложений, а также предоставление доступа к каналу на основе приоритетов беспроводного трафика.

Аналогично всем стандартам, разработанным рабочей группой IEEE **802.11**, цель заключается в определении стандартного способа реализации функций QoS и обеспечении совместимости между компонентами различных компаний.

Беспроводной шлюз 9160 G2 Wireless Gateway предоставляет функции QoS, основанные на спецификации *беспроводных мультимедиа (WMM)* и группе стандартов *беспроводных мультимедиа (WMM)*, которые представляют собой реализацию дополнительного набора функций **802.11e**.

Стандарты WMM могут поддерживаться как на точках доступа, так и на беспроводных клиентах (ноутбуках и электронных бытовых приборах).

19.1.3 Очереди QoS и параметры для координирования потоков трафика

Настройка параметров QoS на беспроводном шлюзе 9160 G2 Wireless Gateway заключается в указании свойств существующих очередей для различных типов беспроводного трафика. Вы можете настроить различное минимальное и максимальное время ожидания для передачи пакетов в каждой очереди с учетом требований к типу передаваемых мультимедийных данных. В очередях автоматически применяется минимальная задержка передачи для голосовых данных, видео и мультимедийных данных, а также для данных критически важных приложений. Для обычных данных, передаваемых по IP, используются параметры по принципу «лучшее из возможного».

Например, чувствительным ко времени голосовым данным, видеоданным и мультимедийным данным присваивается более высокий приоритет передачи (с меньшим временем ожидания доступа к каналу). В то же время другие приложения и обычные данные, передаваемые по IP, которые не отличаются чувствительностью ко времени, но часто предъявляют высокие требования к интенсивности передачи, вынужденно испытывают более продолжительные задержки.

Функции QoS в беспроводном шлюзе 9160 G2 Wireless Gateway реализуются на основе стандарта IEEE Wireless Multimedia (WMM). Для присвоения пакетам тегов и создания нескольких очередей используется класс очередности на базе Linux. Созданные очереди обладают встроенными возможностями приоритизации и маршрутизации, которые применяются в зависимости от типа передаваемых данных. Настраивать параметры очередей можно с помощью интерфейса администрирования.

19.1.3.1 Очереди QoS и типы обслуживания пакетов (ToS)

Реализованные в беспроводном шлюзе 9160 G2 Wireless Gateway функции QoS используют данные *WMM* в заголовке пакета *IP*, имеющие отношение к типу обслуживания (*ToS*). В заголовок каждого пересылаемого по сети IP-пакета включается поле ToS, указывающее способы приоритизации данных и их передачи по сети. Поле ToS содержит значение от 3 до 7 бит, в котором каждый бит представляет отдельный аспект или степень приоритета для этих данных, а также другие метаданные (малая задержка, высокая пропускная способность, высокая надежность, низкие издержки и т. д.).

Например, в поле ToS у пакета данных FTP с большой долей вероятности будет указана максимальная пропускная способность, так как для FTP наибольшее значение имеет возможность оперативно передавать сравнительно большие объемы данных. Функция интерактивной обратной связи в данном случае может быть полезной, но менее важной. Для пакетов данных VoIP указывается минимальная задержка, так как она является определяющим фактором для качественной передачи этого типа данных.

Точка доступа проверяет значения полей ToS в заголовках всех проходящих через нее пакетов. Основываясь на значении поля ToS, точка доступа присваивает пакету приоритет передачи и включает пакет в одну из очередей. Эти действия выполняются автоматически, независимо от того, настроены параметры QoS вручную или нет.

С каждой очередью связывается отдельный тип данных. Ниже приведен список очередей и связанных с ними приоритетов и параметров передачи.

- Data 0 (Голосовые данные). Очередь с самым высоким приоритетом, минимальная задержка. В эту очередь автоматически отправляются чувствительные ко времени данные типа VoIP.
- Data 1 (Видео). Очередь с высоким приоритетом, минимальная задержка. В эту очередь автоматически отправляются чувствительные ко времени данные, такие как видео или потоковые мультимедийные данные.

- Data 2 (Лучшее из возможного). Очередь со средним приоритетом, средней пропускной способностью и задержкой. В эту очередь отправляется большинство обычных данных, передаваемых по IP.
- Data 3 (Фоновый режим). Очередь с наименьшим приоритетом и высокой пропускной способностью. В эту очередь отправляются большие объемы данных, не чувствительные ко времени, но требующие максимальной пропускной способности (например, данные FTP).

Пакеты, поставленные в очередь с более высоким приоритетом, передаются раньше, чем пакеты, находящиеся в очереди с более низким приоритетом. Интерактивные данные из очередей с метками «Data 0» и «Data 1» всегда пересылаются первыми, затем передаются данные среднего приоритета из очереди «Data 2», и в последнюю очередь передаются фоновые (массовые) данные из очереди «Data 3». Каждая из очередей с более низким приоритетом (классом трафика) использует полосу пропускания, оставшуюся от передачи более высоких классов трафика. В крайнем случае, если на точку доступа будут постоянно поступать интерактивные данные, трафик с низким приоритетом не будет передан никогда.

С помощью параметров QoS, доступных в интерфейсе администрирования, можно настроить свойства *улучшенного распределенного доступа к каналу* (Enhanced Distributed Channel Access, EDCA), определяющие способ обработки каждой очереди, которая передается с точки доступа клиенту или с клиента на точку доступа.



Примечание. Передача беспроводного трафика осуществляется по следующим маршрутам:

- По нисходящему каналу с точки доступа на клиентскую станцию.
- По восходящему каналу с клиентской станции на точку доступа.
- По восходящему каналу с точки доступа в сеть.
- По нисходящему каналу из сети на точку доступа.

Если включена поддержка стандарта WMM, параметры QoS, настроенные на беспроводном шлюзе 9160 G2 Wireless Gateway, применяются к первым двум маршрутам: нисходящему трафику, передаваемому с точки доступа на клиентскую станцию (параметры EDCA точки доступа) и восходящему трафику, передаваемому со станции на точку доступа (параметры EDCA станции).

Если поддержка стандарта WMM отключена, вы все равно можете задать параметры для нисходящего потока трафика, передаваемого с точки доступа на клиентскую станцию (параметры EDCA точки доступа).

Остальные фазы потока трафика (в сеть и из сети) не контролируются параметрами QoS на точке доступа.

19.1.3.2 EDCF — управление кадрами данных и арбитражными межкадровыми интервалами

В беспроводных сетях стандарта 802.11 данные передаются в виде *кадров*. **Кадр** включает в себя определенную часть данных и описательные метаданные, объединенные в пакет для передачи по беспроводной сети.



Примечание. Кадр — это почти то же самое, что и пакет. Различие заключается в том, что пакеты обрабатываются на сетевом уровне (уровень 3 в модели OSI), а кадры — на канальном уровне (уровень 2 в модели OSI).

Каждый кадр включает в себя исходный и целевой MAC-адрес, управляющее поле с версией протокола, тип кадра, порядковый номер кадра, тело кадра (фактически передаваемые данные) и порядок проверки кадров на наличие ошибок.

В стандарте 802.11 определены различные типы *кадров* для управления и контроля над беспроводной инфраструктурой, а также для передачи данных. В соответствии со стандартом 802.11 различают следующие типы кадров: (1) *кадры управления*, (2) *кадры контроля* и (3) *кадры данных*. Кадрам управления и контроля (используемым для управления и контроля доступности беспроводной инфраструктуры) автоматически присваивается более высокий приоритет передачи.

В стандарте 802.11e используются *межкадровые интервалы*, определяющие, какие кадры получают доступ к имеющимся каналам, и координирующие время ожидания передачи для различных типов данных.

Кадрам управления и контроля присваивается минимальное время ожидания передачи. Эти кадры имеют *короткий межкадровый интервал* (SIF). Эти интервалы ожидания представляют собой ненастраиваемые встроенные функции 802.11, реализованные для поддержки инфраструктуры.

Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает *функцию улучшенной координации распределения (EDCF)*, определенную в стандарте **802.11e**. Функция EDCF, которая является усовершенствованием стандарта **DCF** и основывается на протоколе **CSMA/CA**, определяет межкадровое пространство (IFS) между *кадрами данных*. Кадры данных ожидают передачи в течение указанного промежутка времени, так называемого *арбитражного межкадрового интервала* (AIFS).

Это настраиваемый параметр.



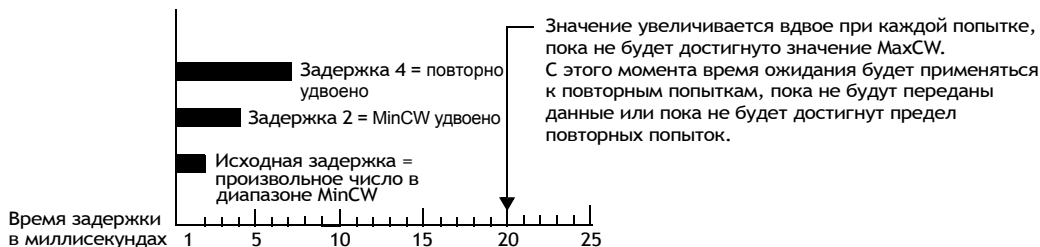
Примечание. Пересылка кадров данных с интервалом AIFS позволяет передавать кадры управления и контроля с более высоким приоритетом и интервалами SIF в первую очередь.

Наличие интервалов AIFS гарантирует, что несколько точек доступа не будут пытаться передать данные в одно и то же время, а будут ожидать, пока освободится канал.

19.1.3.3 Произвольная задержка и минимальные/максимальные окна коллизии

Если точка доступа обнаруживает, что канал уже используется (занят), включается таймер *произвольной задержки* DCF, который определяет время ожидания перед повторной попыткой обращения к данному каналу. Каждая точка доступа проводит некоторое время в режиме ожидания между повторными попытками. Время ожидания (изначально это произвольное значение в диапазоне, указанном в настройке *Minimum Contention Window* (Минимальное окно коллизии)) увеличивается в геометрической прогрессии до тех пор, пока не достигнет заданного предела (*Maximum Contention Window* (Максимальное окно коллизии)). Произвольная задержка позволяет избежать большинства коллизий, которые могли бы произойти, если бы несколько точек доступа одновременно получили доступ к каналу и осуществили попытку передачи данных. Чем больше в сети активных пользователей, тем более эффективно таймер задержки предотвращает коллизии и повторные передачи.

Рис. 19.1 Таймер произвольной задержки DCF



Таймер произвольной задержки, используемый точкой доступа, является настраиваемым параметром. Для определения произвольной задержки используются свойства «Minimum Contention Window» (MinCW) (Минимальное окно коллизии) и «Maximum Contention Window» (MaxCW) (Максимальное окно коллизии).

- Значение, указанное в настройке *Minimum Contention Window* (Минимальное окно коллизии) определяет верхний предел исходного времени произвольной задержки. На таймере произвольной задержки изначально выставляется любое число больше 0, но меньше значения, указанного в настройке «Minimum Contention Window» (Минимальное окно коллизии).

- Если первая произвольная задержка заканчивается до успешной передачи кадра данных, точка доступа увеличивает счетчик повторных попыток и удваивает значение окна произвольной задержки. Значение, указанное в настройке *Maximum Contention Window (Максимальное окно коллизии)*, является верхним пределом этой удвоенной произвольной задержки. Удвоение происходит до тех пор, пока не будет передан кадр данных, либо пока не будет достигнут размер максимального окна коллизии.

19.1.3.4 Импульсная передача пакетов для повышения производительности

В беспроводном шлюзе 9160 G2 Wireless Gateway реализована основанная на стандарте 802.11e технология *импульсной передачи пакетов*, которая повышает пропускную способность при передаче данных и увеличивает скорость передачи по беспроводной сети. Импульсная передача пакетов позволяет передавать множество пакетов, не создавая дополнительную нагрузку за счет избыточных данных заголовков. В результате увеличивается скорость передачи данных и пропускная способность сети. Допустимый размер импульсных пакетов (максимальная длина импульса) является настраиваемым параметром.

19.1.3.5 Интервал потенциальной передачи (TXOP) для клиентских станций

Интервал потенциальной передачи (TXOP) — это промежуток времени, в течение которого клиентская станция стандарта Wi-Fi Multimedia (WMM) имеет возможность инициировать передачу данных по беспроводному каналу (WM).

19.1.4 802.1p и теги DSCP

Стандарт IEEE **802.1p** является расширением стандарта IEEE 802 и регулирует обеспечение QoS. Основная задача стандарта 802.1p — приоритизация сетевого трафика на канальном уровне/уровне MAC. 802.1p предоставляет возможность отфильтровывать многоадресный трафик, чтобы он не выходил за пределы коммутируемых сетей уровня 2. В качестве схемы приоритизации используются кадры тегов. Для обеспечения соответствия этому стандарту коммутаторы уровня 2 должны иметь возможность группировать входящие пакеты LAN в отдельные классы данных.

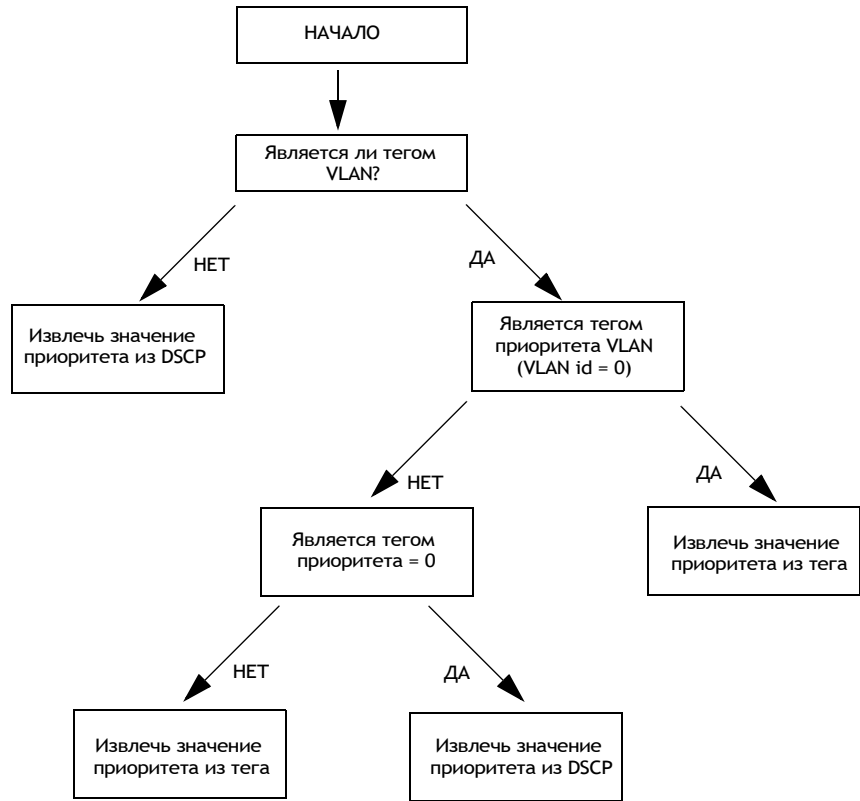
Заголовок 802.1p включает в себя трехбитное поле для приоритизации, которое позволяет объединять пакеты в различные классы трафика. Существует восемь уровней приоритета. Наивысший приоритет — семь — может присваиваться критически важным данным (например, голосовым). Пакеты с более высоким приоритетом всегда передаются в первую очередь. Пакеты с более низким приоритетом не передаются и остаются в очереди до тех пор, пока не будут успешно переданы пакеты с более высоким приоритетом. Наименьший приоритет — ноль — по умолчанию используется в качестве «лучшего из возможных параметров», если не задано никакое другое значение.



Примечание. Важно отметить, что стандарт 802.1p работает, только если включены функции QoS и WMM. Поддержка стандарта WMM должна быть включена как на точке доступа, так и на клиенте, который подключается к ней.

На блок-схеме (Рис. 19.2) показан механизм извлечения тегов и приоритизации трафика в сети.

Рис. 19.2 Приоритизация сетевого трафика



19.1.4.1 Приоритет VLAN

В таблице Табл. 19.1 показаны теги приоритета и связанные с ними значения, извлеченные из тега VLAN.

Табл. 19.1 Приоритеты тегов VLAN

| Тег идентификатора VLAN | Приоритет |
|--------------------------------|----------------------|
| 0 - значение DHCP по умолчанию | Лучшее из возможного |
| 1 | Фоновые данные |
| 2 | Фоновые данные |

Табл. 19.1 Приоритеты тегов VLAN (Продолжение)

| Тег идентификатора VLAN | Приоритет |
|-------------------------|----------------------|
| 3 | Лучшее из возможного |
| 4 | Видео |
| 5 | Видео |
| 6 | Голосовые данные |
| 7 | Голосовые данные |

19.1.4.2 Приоритет DSCP

В таблице Табл. 19.2 показаны значения DSCP, связанные с ними идентификаторы и уровни приоритета.

Табл. 19.2 Приоритеты тегов DSCP

| Тег идентификатора | Приоритет | Значение DSCP |
|--------------------------------|----------------------|---------------|
| 0 - значение DHCP по умолчанию | Лучшее из возможного | 0 |
| 1 | Фоновые данные | 16 |
| 2 | Фоновые данные | 8 |
| 3 | Лучшее из возможного | 24 |
| 4 | Видео | 32 |
| 5 | Видео | 40 |
| 6 | Голосовые данные | 48 |
| 7 | Голосовые данные | 56 |

19.2 Настройка очередей QoS

Чтобы настроить очереди для QoS, перейдите на вкладку *Services (Службы)* > *QoS* и внесите изменения в настройки, как указано ниже.

Рис. 19.3 Параметры качества обслуживания (QoS)

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Modify QoS queue parameters

Queue

AIFS

cwMin

cwMax

Max. Burst

Data 0 (Voice)

1

3

7

1.5

Data 1 (Video)

1

7

15

3.0

Data 2 (Best Effort)

3

15

63

0

Data 3 (Background)

7

15

1023

0

AP EDCA parameters

Wi-Fi Multimedia (WMM)

☒ Enabled

☐ Disabled

Queue

AIFS

cwMin

cwMax

TXOP Limit

Data 0 (Voice)

2

3

7

47

Data 1 (Video)

2

7

15

94

Data 2 (Best Effort)

3

15

1023

0

Data 3 (Background)

7

15

1023

0

Station EDCA parameters

Update

Настройка параметров качества обслуживания (*QoS*) на беспроводном шлюзе 9160 G2 Wireless Gateway заключается в указании параметров существующих очередей для различных типов беспроводного трафика и оптимальном выборе минимального и максимального времени ожидания передачи (с помощью *окон коллизии*). Описанные в этом разделе параметры регулируют поведение точки доступа при передаче данных и не влияют на клиентские станции.



Примечание. В гостевом интерфейсе параметры очередей QoS применяются ко всему объему трафика на точках доступа (к обоим BSS).

Если используется точка доступа с двумя радиомодулями, эти параметры применяются к обоим радиомодулям, но трафик для каждого радиомодуля ставится в очередь отдельно (исключение составляет гостевой трафик, как указано ниже).

Внутренний и гостевой трафик на каждом радиомодуле всегда ставится в очередь совместно. Это относится как к точкам доступа с одним радиомодулем, так и к точкам доступа с двумя радиомодулями.

Функции QoS на точке доступа используют данные в заголовке IP-пакета, имеющие отношение к типу обслуживания (**ToS**). Точка доступа проверяет значения полей ToS в заголовках всех проходящих через нее пакетов. Основываясь на значении поля ToS, точка доступа присваивает пакету приоритет передачи и включает пакет в одну из очередей. С каждой очередью связывается отдельный тип данных. Вы можете настроить параметры, определяющие способ обработки каждой очереди при ее передаче с точки доступа.

Настройка качества обслуживания включает в себя следующие этапы:

- «Настройка параметров EDCA для точки доступа» на стр. 222.
- «Включение/отключение поддержки Wi-Fi Multimedia» на стр. 225.
- «Обновление параметров» на стр. 228.

19.2.1 Настройка параметров EDCA для точки доступа

Параметры улучшенного распределенного доступа к каналу для точки доступа (Enhanced Distributed Channel Access, EDCA) регулируют поток трафика, передаваемого с точки доступа на клиентскую станцию.

Табл. 19.3 Параметры EDCA для точки доступа

| Поле | Описание |
|--|--|
| <i>Queue (Очередь)</i> | <p>Для различных типов данных, передаваемых с точки доступа на клиентскую станцию, предусмотрены следующие очереди:</p> <p>Data 0 (Голосовые данные)</p> <p>Очередь с высоким приоритетом, минимальная задержка. В эту очередь автоматически отправляются чувствительные ко времени данные, такие как VoIP или потоковые мультимедийные данные.</p> <p>Data 1 (Видео)</p> <p>Очередь с высоким приоритетом, минимальная задержка. В эту очередь автоматически отправляются чувствительные ко времени видеоданные.</p> <p>Data 2 (Лучшее из возможного)</p> <p>Очередь со средним приоритетом, средней пропускной способностью и задержкой. В эту очередь отправляется большинство обычных данных, передаваемых по IP.</p> <p>Data 3 (Фоновый режим)</p> <p>Очередь с наименьшим приоритетом и высокой пропускной способностью. В эту очередь отправляются большие объемы данных, не чувствительные ко времени, но требующие максимальной пропускной способности (например, данные FTP).</p> <p>Для получения дополнительной информации см. раздел «Очереди QoS и параметры для координирования потоков трафика» на стр. 212.</p> |
| <i>AIFS (Inter-Frame Space) (Межкадровый интервал)</i> | <p>Параметр <i>Arbitration Inter-Frame Spacing (Арбитражный межкадровый интервал)</i> (AIFS) определяет время ожидания (в миллисекундах) для кадров данных.</p> <p>Допустимые значения AIFS: от 1 до 255 .</p> <p>Для получения дополнительной информации см. описание управления кадрами данных и межкадровыми интервалами с помощью DCF.</p> <p>Для получения дополнительной информации см. раздел «EDCF — управление кадрами данных и арбитражными межкадровыми интервалами» на стр. 215.</p> |

Табл. 19.3 Параметры EDCA для точки доступа (Продолжение)

| Поле | Описание |
|--|---|
| <i>cwMin</i> (<i>Minimum Contention Window</i>) (Минимальное окно коллизии) | <p>Этот параметр предоставляет входное значение для алгоритма, с помощью которого вычисляется время исходной произвольной задержки («окно») перед повторной попыткой передачи данных.</p> <p>Значение, указанное в настройке <i>Minimum Contention Window</i> (Минимальное окно коллизии), определяет верхний предел исходного времени произвольной задержки (в миллисекундах).</p> <p>Первое произвольно генерируемое значение — число больше 0 и меньше числа, указанного в этом поле.</p> <p>Если время первой произвольной задержки истекает до передачи кадра данных, увеличивается счетчик повторной передачи, а значение произвольной задержки (окна) удваивается. Удвоение продолжается до тех пор, пока величина значения произвольной задержки не достигнет числа, указанного в настройке «Maximum Contention Window» (Максимальное окно коллизии).</p> <p>Допустимые значения параметра «cwmin»: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023.</p> <p>Для получения дополнительной информации см. раздел «Произвольная задержка и минимальные/максимальные окна коллизии» на стр. 216.</p> |
| <i>cwMax</i> (<i>Maximum Contention Window</i>) (Максимальное окно коллизии) | <p>Значение, указанное в настройке <i>Maximum Contention Window</i> (Максимальное окно коллизии), является верхним пределом удвоенного значения произвольной задержки (в миллисекундах). Удвоение происходит до тех пор, пока не будет передан кадр данных, либо пока не будет достигнут размер максимального окна коллизии.</p> <p>После достижения величины максимального окна коллизии повторные попытки продолжают до тех пор, пока не будет достигнуто их максимальное число.</p> <p>Допустимые значения параметра «cwmax»: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023.</p> <p>Для получения дополнительной информации см. раздел «Произвольная задержка и минимальные/максимальные окна коллизии» на стр. 216.</p> |

Табл. 19.3 Параметры EDCA для точки доступа (Продолжение)

| Поле | Описание |
|--|--|
| <i>Max. Burst Length</i> (Макс. длина импульса) | <p>Параметр EDCA только для точек доступа (значение, указанное в настройке «Max. Burst Length» (Макс. длина импульса) применяется только к данным, передаваемым с точки доступа на клиентскую станцию).</p> <p>Это значение определяет максимальную длину импульсного пакета (в миллисекундах) при импульсной передаче пакетов по беспроводной сети. <i>Импульсный пакет</i> представляет собой группу из нескольких кадров, передаваемых без данных заголовка. Такой способ передачи позволяет избежать дополнительной нагрузки на сеть и обеспечивает более высокую пропускную способность и производительность.</p> <p>Допустимые значения максимальной длины импульсного пакета: от 0,0 до 999,9.</p> <p>Для получения дополнительной информации см. раздел «Импульсная передача пакетов для повышения производительности» на стр. 217.</p> |

19.2.2 Включение/отключение поддержки Wi-Fi Multimedia

По умолчанию на точке доступа включена поддержка стандарта Wi-Fi MultiMedia (WMM). Если поддержка стандарта WMM включена, функции QoS будут осуществлять приоритизацию и координацию доступа к беспроводному каналу. Если включена поддержка стандарта WMM, параметры QoS, настроенные на беспроводном шлюзе 9160 G2 Wireless Gateway, регулируют *нисходящий* трафик, передаваемый с точки доступа на клиентскую станцию (параметры EDCA точки доступа) и *восходящий* трафик, передаваемый со станции на точку доступа (параметры EDCA станции).

При отключении поддержки WMM функции QoS перестанут контролировать параметры EDCA станции при *восходящей* передаче трафика со станции на точку доступа. Если поддержка WMM отключена, вы все равно можете настроить параметры для нисходящей передачи трафика с точки доступа на клиентскую станцию (параметры EDCA точки доступа).

- Чтобы отключить расширения WMM, нажмите **Disabled** (Отключено).
- Чтобы включить расширения WMM, нажмите **Enabled** (Включено).

19.2.3 Настройка параметров EDCA для станции

Параметры улучшенного распределенного доступа к каналу (Enhanced Distributed Channel Access, EDCA) регулируют поток трафика, передаваемого с клиентской станции на точку доступа.

Табл. 19.4 Параметры EDCA для станции

| Поле | Описание |
|--|--|
| <i>Queue (Очередь)</i> | <p>Для различных типов данных, передаваемых с клиентской станции на точку доступа, предусмотрены следующие очереди:</p> <p>Data 0 (Голосовые данные)</p> <p>Очередь с самым высоким приоритетом, минимальная задержка. В эту очередь автоматически отправляются чувствительные ко времени данные, такие как VoIP или потоковые мультимедийные данные.</p> <p>Data 1 (Видео)</p> <p>Очередь с самым высоким приоритетом, минимальная задержка. В эту очередь автоматически отправляются чувствительные ко времени видеоданные.</p> <p>Data 2 (Лучшее из возможного)</p> <p>Очередь со средним приоритетом, средней пропускной способностью и задержкой. В эту очередь отправляется большинство обычных данных, передаваемых по IP.</p> <p>Data 3 (Фоновый режим)</p> <p>Очередь с наименьшим приоритетом и высокой пропускной способностью. В эту очередь отправляются большие объемы данных, не чувствительные ко времени, но требующие максимальной пропускной способности (например, данные FTP).</p> <p>Для получения дополнительной информации см. раздел «Очереди QoS и параметры для координирования потоков трафика» на стр. 212.</p> |
| <i>AIFS (Inter-Frame Space) (Межкадровый интервал)</i> | <p>Параметр <i>Arbitration Inter-Frame Spacing (Арбитражный межкадровый интервал) (AIFS)</i> определяет время ожидания (в миллисекундах) для кадров данных.</p> <p>Для получения дополнительной информации см. описание управления кадрами данных и межкадровыми интервалами с помощью DCF.</p> <p>Для получения дополнительной информации см. раздел «EDCF — управление кадрами данных и арбитражными межкадровыми интервалами» на стр. 215.</p> |

Табл. 19.4 Параметры EDCA для станции (Продолжение)

| Поле | Описание |
|--|--|
| <i>cwMin</i> (<i>Minimum Contention Window</i>) (Минимальное окно коллизии) | <p>Этот параметр предоставляет входное значение для алгоритма, с помощью которого вычисляется время исходной произвольной задержки («окно») перед повторной попыткой передачи данных.</p> <p>Значение, указанное в настройке <i>Minimum Contention Window</i> (Минимальное окно коллизии), определяет верхний предел исходного времени произвольной задержки (в миллисекундах).</p> <p>Первое произвольно генерируемое значение — число больше 0 и меньше числа, указанного в этом поле.</p> <p>Если время первой произвольной задержки истекает до передачи кадра данных, увеличивается счетчик повторной передачи, а значение произвольной задержки (окна) удваивается. Удвоение продолжается до тех пор, пока величина значения произвольной задержки не достигнет числа, указанного в настройке «<i>Maximum Contention Window</i>» (Максимальное окно коллизии).</p> <p>Для получения дополнительной информации см. раздел «Произвольная задержка и минимальные/максимальные окна коллизии» на стр. 216.</p> |
| <i>cwMax</i> (<i>Maximum Contention Window</i>) (Максимальное окно коллизии) | <p>Значение, указанное в настройке <i>Maximum Contention Window</i> (Максимальное окно коллизии), является верхним пределом удвоенного значения произвольной задержки (в миллисекундах). Удвоение происходит до тех пор, пока не будет передан кадр данных, либо пока не будет достигнут размер максимального окна коллизии.</p> <p>После достижения величины максимального окна коллизии повторные попытки продолжают до тех пор, пока не будет достигнуто их максимальное число.</p> <p>Для получения дополнительной информации см. раздел «Произвольная задержка и минимальные/максимальные окна коллизии» на стр. 216.</p> |
| <i>TXOP Limit</i> (Предел TXOP) | <p>Параметр EDCA только для станций (параметр «TXOP Limit» (Предел TXOP) применяется только к данным, передаваемым с клиентской станции на точку доступа).</p> <p><i>Интервал потенциальной передачи</i> (TXOP) — это промежуток времени, в течение которого клиентская станция стандарта WME имеет возможность инициировать передачу данных по беспроводному каналу (WM).</p> <p>Это значение (в миллисекундах) определяет <i>интервал потенциальной передачи</i> (TXOP) для клиентских станций, то есть промежуток времени, в течение которого клиентская станция WMM имеет возможность инициировать передачу данных по беспроводной сети.</p> |

19.3 Обновление параметров

Для обновления параметров QoS:

1. Перейдите на вкладку *QoS*.
2. Внесите необходимые изменения в параметры QoS.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

| | |
|---|-----|
| 20.1 Общие сведения о распределенной беспроводной системе | 231 |
| 20.1.1 Использование WDS для коммутации отдаленных проводных LAN | 231 |
| 20.1.2 Расширение сети за пределы зоны проводного покрытия с помощью WDS | 232 |
| 20.1.3 Создание резервных подключений с помощью WDS | 233 |
| 20.2 Рекомендации по обеспечению безопасности соединений WDS | 233 |
| 20.2.1 Общие сведения о статическом WEP-шифровании данных. | 234 |
| 20.2.2 Общие сведения о шифровании данных ключом WPA (PSK). | 234 |
| 20.3 Настройка параметров WDS. | 235 |
| 20.3.1 Пример настройки соединения WDS | 239 |
| 20.4 Обновление параметров | 240 |

Беспроводной шлюз 9160 G2 Wireless Gateway позволяет соединить несколько точек доступа посредством распределенной беспроводной системы (**WDS**). С помощью WDS точки доступа могут связываться друг с другом по беспроводной сети. Эта функциональность играет важнейшую роль в управлении несколькими беспроводными сетями и обеспечении постоянного доступа к сети для клиентов, находящихся в роуминге. Кроме того, эта система упрощает сетевую инфраструктуру, сокращая количество требуемых кабельных соединений.

В следующих разделах приведены инструкции по настройке параметров WDS на беспроводном шлюзе 9160 G2 Wireless Gateway.

20.1 Общие сведения о распределенной беспроводной системе

Распределенная беспроводная система (WDS) — это технология беспроводной связи для соединения точек доступа (обозначаемых термином «базовый набор сервисов» (BSS)) и формирования так называемого «расширенного набора сервисов» (ESS).

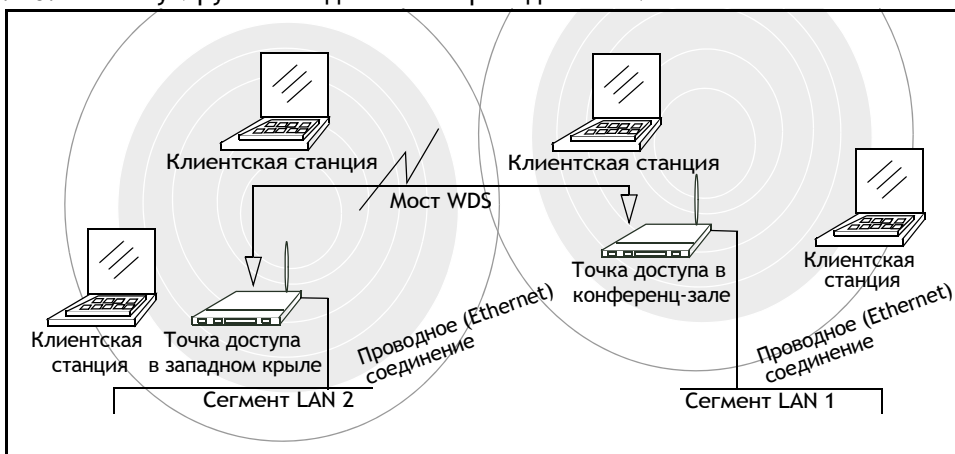


Примечание. BSS, как правило, соответствует одной точке доступа (и развертывается как беспроводная «сеть» с одной точкой доступа). Исключения составляют случаи, когда возможность использования нескольких идентификаторов BSSID позволяет представить одну точку доступа в виде двух и более узлов сети. В таких случаях точка доступа имеет несколько уникальных идентификаторов BSSID.

20.1.1 Использование WDS для коммутации отдаленных проводных LAN

В сети **ESS** с множеством точек доступа каждая точка доступа обслуживает часть зоны, которая слишком велика для одной точки доступа. С помощью WDS можно соединить отдаленные сети Ethernet и создать единую **LAN**. Допустим, что одна точка доступа, подключенная к сети по кабелю Ethernet, обслуживает несколько клиентских станций в конференц-зале (сегмент LAN 1), а другая точка доступа, также с проводным подключением Ethernet, обслуживает станции в кабинетах западного крыла (сегмент LAN 2). Точку доступа в конференц-зале и точку доступа в западном крыле можно соединить с помощью канала WDS, создав единую сеть для клиентов в обеих зонах (см. Рис. 20.1 на стр. 232).

Рис. 20.1 Коммутируемые отдаленные проводные LAN

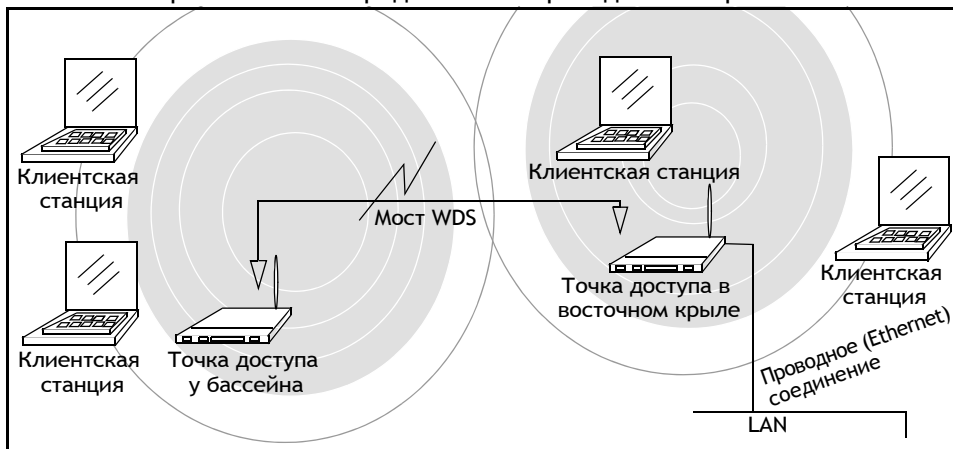


20.1.2 Расширение сети за пределы зоны проводного покрытия с помощью WDS

ESS позволяет расширить охват сети и распространить покрытие на зоны, где прокладка кабелей затруднительна, требует больших расходов или просто неэффективна.

Допустим, что имеется точка доступа, подключенная к сети по кабелю Ethernet, которая обслуживает множество клиентских станций в одной зоне (в данном примере это восточное крыло), но не может взаимодействовать с другими станциями, находящимися вне зоны доступа. Также предположим, что прокладка кабелей Ethernet в этой отдаленной зоне вызывает слишком большие сложности и требует слишком больших расходов. Эту проблему можно решить, разместив вторую точку доступа ближе ко второй группе станций (в данном примере — у бассейна, см. Рис. 20.1.3 на стр. 233) и соединить эти две точки доступа с помощью канала WDS. Это позволит *расширить* границы сети за счет беспроводной связи и создать дополнительный транзитный участок для доступа к отдаленным станциям (см. Рис. 20.1.3 на стр. 233).

Рис. 20.2 Расширение сети за пределы зоны проводного покрытия



20.1.3 Создание резервных подключений с помощью WDS

Еще одна область применения мостовых соединений WDS — создание резервных подключений. С помощью WDS и *протокола связующего дерева (STP)*, поддержка которого включается на беспроводном шлюзе 9160 G2 Wireless Gateway автоматически, можно настраивать резервные каналы связи между точками доступа во всей сети. Например, две точки доступа могут быть соединены как основным каналом Ethernet, так и дополнительным (резервным) беспроводным каналом WDS. В случае потери подключения Ethernet протокол STP перенастраивает схему сети и эффективно восстанавливает связь с вышедшим из строя сегментом сети, активируя резервный беспроводной канал.

20.2 Рекомендации по обеспечению безопасности соединений WDS

Важно, чтобы канал WDS был защищен. Для каналов WDS можно применять любые типы защиты, независимо от параметров безопасности, применяемых к точкам доступа на этом канале. Например, уровень безопасности на первой точке доступа может быть установлен в значение **None** (Нет), а для второй точки доступа может быть включен механизм защиты **WEP**. Несмотря на такое различие в параметрах безопасности, для соединения WDS можно выбрать как вариант «None» (Нет), так и вариант «WEP». Единственным исключением из этого правила является режим WPA (PSK). Механизм безопасности WPA (PSK) применяется к соединению WDS только в случае, когда и на первой, и на второй точке доступа включена система защиты «WPA Personal» или «WPA Enterprise».

20.2.1 Общие сведения о статическом WEP-шифровании данных

Статический эквивалент конфиденциальности проводных сетей (*WEP*) — это протокол шифрования данных для беспроводных сетей 802.11. Для обеих точек доступа на канале WDS должны быть настроены одинаковые параметры безопасности. При использовании статического WEP шифрование данных может осуществляться с помощью статического 64-разрядного общего ключа (40-разрядный секретный ключ + 24-разрядный вектор инициализации (IV)), или с помощью 128-разрядного общего ключа (104-разрядный секретный ключ + 24-разрядный вектор инициализации).

Вы можете разрешить использование статического *WEP* на канале (мостовом соединении) WDS. Когда включен механизм шифрования WEP, все данные, которыми точки доступа обмениваются по каналу WDS, шифруются с помощью фиксированного ключа WEP, предоставленного пользователем.

Статическое WEP-шифрование не обеспечивает эффективную защиту данных на том уровне, на каком она обеспечивается другими режимами безопасности, доступными для клиентских станций. Использование статического WEP-шифрования в *LAN*, предназначенной для передачи защищенного беспроводного трафика, создает угрозу безопасности для вашей сети. В связи с этим рекомендуется использовать шифрование WPA (PSK) на всех каналах WDS во внутренней сети. Используйте каналы WDS со статическим WEP-шифрованием для соединения точек доступа во внутренней сети, только если вы абсолютно уверены в отсутствии рисков безопасности. Для получения дополнительной информации о шифровании WPA (PSK) см. раздел «Общие сведения о шифровании данных ключом WPA (PSK)» далее.

Дополнительные сведения об эффективности различных режимов безопасности см. в Гл. 10: «Настройка режимов безопасности». В этом разделе также рассматривается использование режима безопасности без шифрования для обмена данными между точками доступа и станциями в гостевой сети, имеющей более низкий уровень конфиденциальности.

20.2.2 Общие сведения о шифровании данных ключом WPA (PSK)

Ключ защищенного доступа к Wi-Fi (предварительный ключ), или WPA (PSK) — более надежный механизм защиты по сравнению со статическим WEP-шифрованием. Известное ранее под названием «WPA-Home» шифрование WPA (PSK) заключается в использовании предварительного ключа, который по сути является общим паролем для обмена данными между точками доступа, соединенными мостом. WPA (PSK) обеспечивает более высокий уровень безопасности для беспроводных сетей 802.11, устраняя необходимость в дорогостоящей и сложнореализуемой инфраструктуре аутентификации RADIUS.

Поскольку механизм шифрования WPA (PSK) основывается на использовании общего ключа, для обеих точек доступа на канале WDS должен быть задан один и тот же ключ. В противном случае точки доступа не смогут связываться друг с другом и обмениваться данными.



Примечание. В целях безопасности рекомендуется регулярно менять общие ключи на канале WDS.

Дополнительные сведения об эффективности различных режимов безопасности см. в Гл. 10: «Настройка режимов безопасности».

20.3 Настройка параметров WDS

Чтобы настроить параметры обмена данными для текущей точки доступа, перейдите на вкладку *Manage (Управление) > WDS* и внесите изменения в настройки, как указано ниже.



Примечание. На Рис. 20.3 показан экран параметров WDS для точки доступа с двумя радиомодулями. Веб-страница администрирования точки доступа с одним радиомодулем будет выглядеть несколько иначе.

Рис. 20.3 Параметры распределенной беспроводной системы

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

Configure WDS bridges to other access points

Local Address00:08:A2:01:4B:56

Remote Address

EncryptionNone (Plain-text)

Remote Address

EncryptionNone (Plain-text)

Remote Address

EncryptionNone (Plain-text)

Remote Address

EncryptionNone (Plain-text)

Update

Ниже приведены важные примечания и рекомендации относительно конфигурации **WDS**. Прежде чем перейти к настройке параметров WDS, внимательно ознакомьтесь с этими примечаниями.



Примечание. При использовании WDS необходимо настроить параметры WDS на обеих точках доступа, участвующих в соединении WDS.

Между любой парой точек доступа можно установить только одно соединение WDS. Это означает, что удаленный MAC-адрес указывается в настройках WDS конкретной точки доступа только один раз.

Обе точки доступа, участвующие в соединении WDS, должны работать на одном и том же радиоканале и в одном и том же режиме IEEE 802.11 (для получения сведений о настройке режима радиосвязи и канала см. Гл. 16: «Настройка параметров радиомодуля 802.11»).

Настройка соединений WDS при использовании 802.11h может вызывать затруднения. См. раздел «Управление регулятивным доменом 802.11h» на стр. 163.

Чтобы настроить WDS на данной точке доступа, опишите каждую точку доступа, которая будет принимать запросы на переключение и передавать данные на текущую точку доступа. Для каждой целевой точки доступа необходимо предоставить сведения, как показано в Табл. 20.1.

Табл. 20.1 Параметры целевых точек доступа

| Поле | Описание |
|--|--|
| <i>Local Address</i> (Локальный адрес) | <p>Этот параметр определяет адреса управления доступом к среде (MAC) для данной точки доступа.</p> <p>MAC-адрес является постоянным уникальным аппаратным адресом любого устройства, представляющего интерфейс для сети. MAC-адрес присваивается производителем. Этот адрес нельзя изменить. Значение этого адреса как уникального идентификатора точки доступа или интерфейса приведено только в информационных целях.</p> <p>Точка доступа с одним радиомодулем.</p> <p>Для точек доступа с одним радиомодулем в верхней части экрана параметров WDS отображается только один MAC-адрес. Адрес, отображаемый для точки доступа с одним радиомодулем, является MAC-адресом радиомодуля этой точки доступа. По этому адресу точка доступа распознается другими внешними сетями.</p> <p>Точка доступа с двумя радиомодулями.</p> <p>Параметр <i>Local Address</i> (Локальный адрес), заданный для каждого канала WDS на точке доступа с двумя радиомодулями, представляет собой MAC-адрес внутреннего интерфейса выбранного радиомодуля (первого радиомодуля на WLAN0 или второго радиомодуля на WLAN1).</p> |
| <i>Remote Address</i> (Удаленный адрес) | <p>Укажите MAC-адрес целевой точки доступа. Это точка доступа, на которую будут пересылаться данные и с которой эти данные будут приниматься — другими словами, это точка доступа, к которой будет вести соединение WDS.</p> <p>Нажмите на стрелку справа от поля <i>Remote Address</i> (Удаленный адрес), чтобы просмотреть список всех доступных MAC-адресов и связанных с ними идентификаторов SSID, доступных в сети. Выберите нужный MAC-адрес из списка.</p> <p>Примечание. Идентификатор SSID отображается в списке в качестве подсказки, упрощающей выбор правильного MAC-адреса для целевой точки доступа. Этот идентификатор SSID отличается от SSID, который указывается для соединения WDS. Эти два идентификатора должны иметь разные значения и имена.</p> |

Табл. 20.1 Параметры целевых точек доступа (Продолжение)

| Поле | Описание |
|-----------------------------------|---|
| <i>Encryption</i> (Шифрование) | <p>Если вы считаете, что соединение WDS не создаст угрозы для безопасности, вы можете полностью отказаться от шифрования. Однако в целях безопасности можно выбрать статическое WEP-шифрование либо WPA (PSK).</p> <p>Примечание. Набор доступных типов шифрования зависит от параметров, заданных на вкладке «Security» (Безопасность). Параметр WPA (PSK) доступен на экране WDS, только если для параметра «Mode» (Режим) на вкладке «Security» (Безопасность) выбрано значение WPA Personal или WPA Enterprise.</p> <p>None (Plain Text) (Нет (Простой текст))</p> <p>Если в качестве типа шифрования выбрано значение None (Нет), данные, которыми будут обмениваться точки доступа по каналу WDS, не будут подвергаться шифрованию, а будут передаваться в виде простого текста.</p> <p>WEP</p> <p>Если необходимо, выберите тип шифрования «эквивалент конфиденциальности проводных сетей» (WEP) для канала WDS. Эквивалент конфиденциальности проводных сетей (WEP) — это протокол шифрования данных в беспроводных сетях 802.11. Для обеих точек доступа на канале WDS должны быть настроены одинаковые параметры безопасности. При использовании статического WEP шифрование данных может осуществляться с помощью статического 64-разрядного общего ключа (40-разрядный секретный ключ + 24-разрядный вектор инициализации (IV)), или с помощью 128-разрядного общего ключа (104-разрядный секретный ключ + 24-разрядный вектор инициализации). Для получения дополнительной информации о безопасности WEP см. раздел «Static WEP (Статическое WEP-шифрование)» на стр. 111.</p> <p>WPA (PSK)</p> <p>Если необходимо, выберите тип шифрования WPA (PSK) для канала WDS. Предварительный ключ защищенного доступа к Wi-Fi, или WPA (PSK) — более надежный механизм шифрования по сравнению с WEP. При использовании шифрования WPA (PSK) для каждой точки доступа в сети должен быть задан один и тот же уникальный ключ. В противном случае точки доступа не смогут обмениваться данными друг с другом.</p> <p>Параметр «WPA (PSK)» доступен на экране WDS, только если для параметра «Mode» (Режим) на вкладке <i>Security</i> (Безопасность) выбрано значение WPA Personal или WPA Enterprise. Для получения дополнительной информации о вкладке «Security» (Безопасность) см. раздел «Общие сведения о проблемах безопасности в беспроводных сетях» на стр. 99.</p> <p>Для получения дополнительной информации о режиме безопасности WEP (PSK) см. раздел «WPA Personal» на стр. 119.</p> |

20.3.1 Пример настройки соединения WDS

При использовании WDS необходимо настроить параметры *WDS* на *обеих* точках доступа, соединенных каналом WDS. Например, если требуется создать соединение WDS между парой точек доступа «**MyAP1**» и «**MyAP2**», необходимо выполнить следующие действия.

1. Откройте веб-страницу администрирования для точки доступа **MyAP1**. Для этого введите IP-адрес точки доступа **MyAP1** в адресной строке веб-браузера в следующем формате:
<http://IPAddressOfAccessPoint>
где *IPAddressOfAccessPoint* — адрес точки доступа **MyAP1**.
2. На веб-странице администрирования **MyAP1** перейдите на вкладку *WDS*.
MAC-адрес текущей точки доступа **MyAP1** отобразится в поле «Local Address» (Локальный адрес) в верхней части экрана.
3. Настройте интерфейс WDS для обмена данными с точкой доступа **MyAP2**.
Сначала введите MAC-адрес точки доступа **MyAP2** в поле «Remote Address» (Удаленный адрес), затем заполните поля свойств сети (гостевой или внутренней), задайте значения параметров безопасности и т. д. Сохраните параметры, нажав на кнопку **Update** (Обновить).
4. Перейдите к разделу параметров радиомодуля на веб-странице администрирования (*Manage (Управление) > 802.11 Advanced Settings (Расширенные параметры 802.11)*) и проверьте заданные значения или настройте режим и канал радиосвязи для широкополосных передач точки доступа **MyAP1**.
Помните, что обе точки доступа, участвующие в соединении, **MyAP1** и **MyAP2**, должны работать в одном и том же режиме и передавать данные по одному и тому же каналу.
Допустим, что выбран режим IEEE 802.11b и широкополосный канал 6. Значения «Mode» (Режим) и «Channel» (Канал) можно выбрать в раскрывающихся меню на вкладке «Radio» (Радиомодуль).
5. Повторите вышеперечисленные действия для точки доступа **MyAP2**.
 - Откройте веб-страницу администрирования для точки доступа **MyAP2**, указав IP-адрес **MyAP2** в адресной строке браузера.

- На веб-странице администрирования MyAP2 перейдите на вкладку *WDS*. MAC-адрес точки доступа MyAP2 отобразится в поле «Local Address» (Локальный адрес).
- Настройте интерфейс WDS для обмена данными с точкой доступа MyAP1, начиная с MAC-адреса точки доступа MyAP1.
- Перейдите в раздел параметров радиомодуля MyAP2 и убедитесь, что для этой точки доступа выбран такой же режим и широкополосный канал, как и для точки доступа MyAP1. В данном примере выбран режим 802.11b и канал 6.
- Не забудьте сохранить параметры, нажав кнопку **Update** (Обновить).

20.4 Обновление параметров

Для обновления параметров WDS:

1. Перейдите на вкладку *WDS*.
2. Внесите необходимые изменения в параметры WDS.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

| | |
|---|-----|
| 21.1 Общие сведения о параметрах SNMP | 243 |
| 21.2 Переход к параметрам SNMP | 244 |
| 21.3 Настройка параметров SNMP | 245 |
| 21.3.1 Настройка SNMP-ловушек. | 248 |
| 21.3.2 Обновление параметров SNMP | 249 |

Следующие разделы содержат сведения о настройке SNMP и сопутствующих параметров Enterprise-Manager API на беспроводном шлюзе 9160 G2 Wireless Gateway.

21.1 Общие сведения о параметрах SNMP

Простой протокол сетевого управления (Simple Network Management Protocol, SNMP) определяет стандарт записи, хранения и предоставления общего доступа к данным о сетевых устройствах. Протокол SNMP обеспечивает возможности для управления сетью, устранения неисправностей и технического обслуживания.

Ключевыми компонентами любой сети под управлением протокола SNMP являются управляемые устройства, агенты SNMP и система управления. Агенты сохраняют данные о соответствующих сетевых устройствах в информационных базах управления (Management Information Base, MIB) и возвращают эти данные диспетчеру SNMP по запросу. Управляемые устройства могут быть сетевыми узлами, например базовыми станциями точек доступа, маршрутизаторами, коммутаторами, мостами, концентраторами, серверами или принтерами.

Беспроводной шлюз 9160 G2 Wireless Gateway может использоваться в качестве устройства под управлением протокола SNMP, обеспечивающего полную интеграцию с системами управления сетью, такими как HP OpenView или Devicescape Wireless Operations Center.

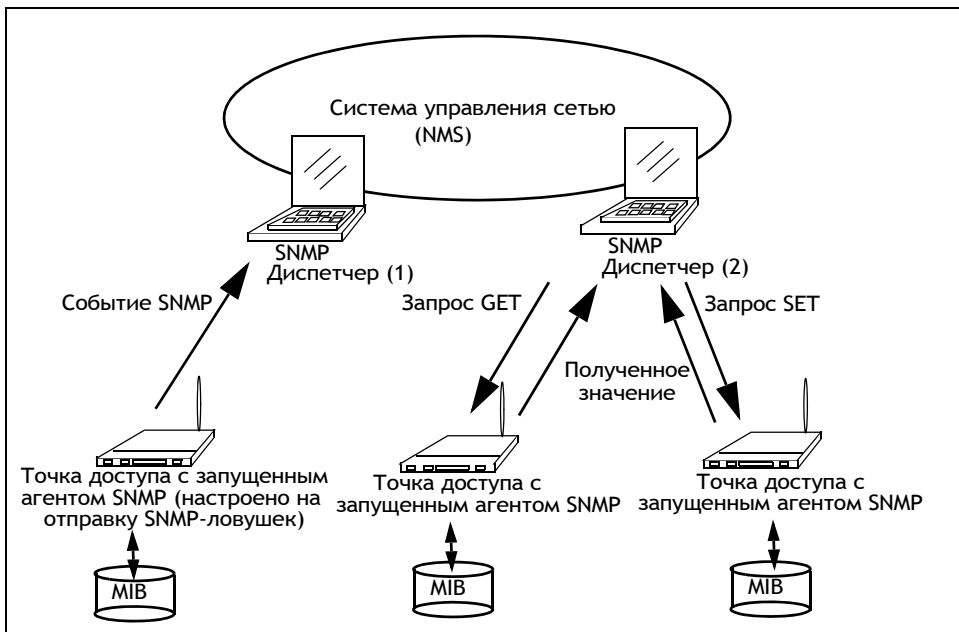
Информационные базы управления (MIB) представляют собой коллекции объектов или файлов, хранящиеся в виртуальной базе данных, доступной по сети. Протокол SNMP получает данные из информационных баз управления с помощью специальных команд и запросов.

Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает следующие стандартные информационные базы управления SNMP:

- Bridge MIB 802.1d (RFC 1493).
- MIB SNMPv2 (RFC 3418).
- MIB стандарта IEEE 802.11 (база).
- MIB группы интерфейсов (RFC 2233).
- Две частные базы MIB (беспроводная база MIB и системная база MIB) на основе MIB разрабатываемого стандарта IEEE 802.11k. Они предоставляют информацию о списке клиентских связей беспроводного шлюза 9160 G2 Wireless Gateway и таблице обнаружения точек доступа соответственно. Частная системная MIB обеспечивает функции технического обслуживания, такие как перезагрузка системы или обновление прошивки.

Беспроводной шлюз 9160 G2 Wireless Gateway также поддерживает SNMP-ловушки. Рис. 21.1 иллюстрирует функционирование протокола SNMP в сети.

Рис. 21.1 Функционирование протокола SNMP в сети



21.2 Переход к параметрам SNMP

Для настройки параметров SNMP перейдите в раздел *Services (Службы) > SNMP* и внесите изменения в настройки, как указано ниже.

Рис. 21.2 Обзор параметров SNMP

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Modify SNMP Settings

SNMP ☒ Enabled ☐ Disabled

Read-only community name (for permitted GETs)

Port number the SNMP agent will listen to

Allow SNMP SET requests ☒ Enabled ☐ Disabled

Read-write community name (for permitted SETs)

Restrict the source of SNMP requests to only the designated hosts or subnets ☐ Enabled ☒ Disabled

Hostname or subnet of Network Management System

Значение

Полученное

Trap Destinations

Community name for traps

Enabled ☒ Hostname

☒

☐

Update

21.3 Настройка параметров SNMP

Включение/выключение управления агентами SNMP, настройка коллективного пароля, доступ к базам MIB и настройка назначений для SNMP-ловушек настраиваются на беспроводном шлюзе 9160 G2 Wireless Gateway, как описано ниже.

Табл. 21.1 Параметры SNMP

| Поле | Описание |
|--|---|
| <i>SNMP Enabled/Disabled (Включение/отключение SNMP)</i> | <p>Вы можете включить протокол SNMP в сети или выключить его. По умолчанию протокол SNMP отключен.</p> <ul style="list-style-type: none">• Чтобы включить протокол SNMP, нажмите Enabled (Включено).• Чтобы отключить протокол SNMP, нажмите Disabled (Отключено). <p>Примечание. Если протокол SNMP отключен, все остальные поля на экране SNMP будут неактивны.</p> |
| <i>Read-only community name for permitted GETs (Коллективное имя для разрешенных запросов GET, только чтение)</i> | <p>Введите коллективное имя, предназначенное только для чтения.</p> <p>В соответствии со стандартом SNMPv2c, это коллективное имя служит в качестве простого механизма аутентификации, ограничивающего число подключенных к сети компьютеров, которые могут запрашивать данные у агента SNMP. Это имя функционирует как пароль, и запрос считается подлинным, если его отправитель знает этот пароль.</p> <p>В качестве коллективного имени можно указать любое сочетание буквенно-числовых символов.</p> |
| <i>Port number the SNMP agent will listen to (Номер порта, прослушиваемого агентом SNMP)</i> | <p>По умолчанию агент SNMP прослушивает на наличие запросов только порт 161. Однако это значение можно изменить, указав номер другого порта для прослушивания.</p> <p>Введите номер порта, который будет прослушиваться агентом SNMP на наличие запросов.</p> |
| <i>Allow SNMP SET Requests (Разрешить запросы SNMP SET)</i> | <p>Вы можете разрешить или запретить запросы SNMP SET.</p> <p>Если запросы SET разрешены, подключенные к сети компьютеры могут выполнять запросы SET для настроенного агента на точке доступа.</p> <p>Примечание. Запросы SET ограничиваются частной системной базой MIB.</p> <ul style="list-style-type: none">• Чтобы включить запросы SNMP SET, нажмите Enabled (Включено).• Чтобы отключить запросы SNMP SET, нажмите Disabled (Отключено). |
| <i>Read-write community name for permitted SETs (Коллективное имя для разрешенных запросов SET, чтение и запись)</i> | <p>Если запросы SNMP SET разрешены, можно указать коллективное имя, предназначенное для чтения и записи.</p> <p>Это коллективное имя выполняет функции, сходные с паролем. Запросы будут приниматься только от компьютеров, идентифицированных по этому коллективному имени.</p> <p>В качестве коллективного имени можно указать любое сочетание буквенно-числовых символов.</p> |

Табл. 21.1 Параметры SNMP (Продолжение)

| Поле | Описание |
|--|---|
| <i>Restrict the source of SNMP requests to only the designated hosts or subnets (Ограничить источник запросов SNMP отдельными хостами или подсетями)</i> | <p>Вы можете ограничить источник разрешенных запросов SNMP.</p> <ul style="list-style-type: none">• Чтобы ограничить источник разрешенных запросов SNMP, нажмите Enabled (Включено).• Чтобы разрешить любому источнику отправлять запросы SNMP, нажмите Disabled (Отключено). |
| <i>Hostname or subnet of Network Management System (Имя хоста или подсеть для системы управления сетью)</i> | <p>Укажите имя хоста DNS или подсеть для компьютеров, которые могут отправлять запросы GET и SET на управляемые устройства.</p> <p>По аналогии с коллективными именами эти значения обеспечивают дополнительный уровень безопасности для параметров SNMP. Агент SNMP будет принимать запросы только от компьютеров с указанными именами или компьютеров, находящихся в указанной подсети.</p> <p>Чтобы указать подсеть, введите один или несколько диапазонов адресов подсети в форме <i>AddressRange/MaskLength</i>, где <i>AddressRange</i> — это IP-адрес, а <i>MaskLength</i> — число бит в маске. Поддерживаются оба формата: <i>NetAddress/NetMask</i> и <i>NetAddress/MaskLength</i>. Также здесь можно указать отдельные хосты, например IP-адрес или имя хоста. Например, если указан диапазон 192.168.1.0/24, это означает, что будет использоваться подсеть с адресом 192.168.1.0 и маской подсети 255.255.255.0.</p> <p>Этот диапазон адресов используется для указания подсети выделенной системы NMS. Выполнение запросов GET и SET на управляемых устройствах будет разрешено только для компьютеров, находящихся в указанном диапазоне IP-адресов. Исходя из вышеприведенного примера, выполнять команды SNMP на устройствах смогут компьютеры с IP-адресами в пределах от 192.168.1.1 до 192.168.1.254. Адрес с суффиксом .0 в диапазоне подсети всегда резервируется в качестве адреса подсети, в то время как адрес с обозначением .255 в диапазоне всегда резервируется в качестве адреса широковещательной передачи.</p> <p>Еще один пример: если указать диапазон 10.10.1.128/25, выполнять запросы SNMP на управляемых устройствах смогут компьютеры с IP-адресами в пределах от 10.10.1.129 до 10.10.1.254. В данном примере 10.10.1.128 является адресом сети, а 10.10.1.255 — адресом широковещательной передачи. Будет выделено 126 адресов.</p> |

21.3.1 Настройка SNMP-ловушек

SNMP-ловушки обеспечивают асинхронную передачу сообщений от устройств под управлением протокола SNMP (например, беспроводных шлюзов 9160 G2 Wireless Gateway) на выделенные главные устройства. Если система управления сетью (NMS) используется для мониторинга большого количества подключенных к сети устройств, периодически опрашивать каждое устройство в сети непрактично. Включение SNMP-ловушек на точке доступа позволяет отдельным устройствам отправлять сообщения об определенных событиях в сети непосредственно диспетчерам SNMP или другим выделенным главным устройствам в системе NMS. Это могут быть сообщения о включении и отключении сетевых интерфейсов, неуспешных попытках установления связи с клиентами или сбоях аутентификации на точках доступа, включении или отключении системы и изменениях в топологии сети.

SNMP-ловушки экономят сетевые ресурсы, устраняя избыточные запросы SNMP. Также ловушки упрощают поиск и устранение неисправностей для диспетчеров SNMP. Например, если диспетчер SNMP контролирует большую сеть с множеством устройств и на каждом из этих устройств находится большое количество объектов, запрашивать данные у каждого объекта на каждом устройстве непрактично. В этом случае наиболее эффективна схема, когда каждый агент на управляемом устройстве сообщает диспетчеру о любых необычных событиях. Для отправки таких сообщений используются ловушки событий. Получив информацию о событии, диспетчер может выбрать действие, которое будет выполнено (при необходимости).

Табл. 21.2 Параметры SNMP-ловушек

| Поле | Описание |
|---|---|
| <i>Community name for traps</i> (Коллективное имя для ловушек) | Введите глобальные коллективные строковые данные, связанные с SNMP-ловушками. Это имя будет включено в ловушки, передаваемые с устройств, и будет использоваться в качестве коллективного имени. |
| <i>Hostname</i> (Имя хоста) | Укажите имя хоста DNS — имя компьютера, на который требуется отправлять SNMP-ловушки. Пример имени хоста DNS: snmptraps.teklogix.com Поскольку агент SNMP передает SNMP-ловушки произвольным образом, следует указать пункт назначения для этих ловушек. Рядом с соответствующим именем хоста должен быть установлен флажок Enabled (Включено). |

21.3.2 Обновление параметров SNMP

Для обновления параметров SNMP:

1. Перейдите на вкладку *SNMP*.
2. Внесите необходимые изменения в параметры SNMP.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

9160 G2 В РЕЖИМЕ БАЗОВОЙ СТАНЦИИ

22

| | |
|--|-----|
| 22.1 Обзор | 253 |
| 22.2 Протоколы радиосвязи | 254 |
| 22.2.1 Протокол адаптивного опроса/коллизии | 254 |
| 22.3 Меню узкополосного радиомодуля | 255 |
| 22.3.1 Параметры настройки узкополосного радиомодуля | 255 |
| 22.3.1.1 Параметры радиомодуля RA1001A | 257 |
| 22.3.2 Параметры подключений | 258 |
| 22.3.3 Параметры подключений: режим базовой станции | 258 |
| 22.3.3.1 Параметры протокола опроса. | 260 |
| 22.3.3.2 Параметры радиомодуля | 263 |
| 22.3.4 Параметры подключений: режим RRM. | 264 |
| 22.4 Меню подключений | 265 |
| 22.4.1 Параметры настройки базовой станции | 267 |
| 22.4.2 Параметры настройки групп RRM | 268 |
| 22.4.2.1 Группы RRM. | 270 |
| 22.4.2.2 Параметры протокола опроса. | 271 |
| 22.4.2.3 Параметры радиомодуля | 273 |
| 22.4.2.4 Параметры группы | 274 |
| 22.4.2.5 Удаленные радиомодули | 275 |
| 22.4.3 Параметры настройки функций радиоканала | 275 |
| 22.4.3.1 Функции радиоканала. | 277 |
| 22.4.3.2 Автоматическое назначение адреса радиомодуля. | 278 |
| 22.4.3.3 Automatic Terminal Number (Автоматическое назначение номера терминала) | 280 |
| 22.4.4 Меню Hosts (Главные устройства) | 281 |
| 22.4.4.1 Конфигурация 9010 | 284 |

22.1 Обзор

Беспроводной шлюз 9160 G2 Wireless Gateway может функционировать как проводная или беспроводная базовая станция или как удаленный радиомодуль (RRM), используя радиоканал и проприетарные протоколы Psion Teklogix для обеспечения связи с мобильными компьютерами (см. «Протоколы радиосвязи» на стр. 254).

В качестве проводной базовой станции беспроводной шлюз 9160 G2 может устанавливать связь с беспроводными мобильными компьютерами, используя протокол адаптивного опроса/коллизии (стр. 254), и подключается к сетевому контроллеру по сети.

В качестве беспроводной базовой станции беспроводной шлюз 9160 G2 устанавливает связь с проводной базовой станцией и мобильными компьютерами, используя 802.11 WDS.

В качестве удаленного радиомодуля (RRM) работа и таймирование радиоканала беспроводного шлюза 9160 G2 с мобильными компьютерами напрямую управляется сетевым контроллером, который использует протокол радиосвязи с временным уплотнением (см. «Временное уплотнение и переключение сотового канала связи» ниже). Он подключен к сетевому контроллеру по сети.

Временное уплотнение и переключение сотового канала связи

Существует два способа работы на радиоканале. Первый способ называется *переключением сотового канала связи*. Он сходен с принципом работы системы сотовой связи. Каждая базовая станция использует свой канал радиосвязи. Мобильные компьютеры следят за радиоканалом и автоматически переключаются на канал с наилучшим приемом радиосигнала. Возможность переключения сотового канала связи прозрачна для главного устройства.

Второй способ называется *временным уплотнением*. В этом случае базы удаленного радиомодуля (RRM) на месте используют один канал. По сети UDP/IP сетевой контроллер координирует последовательность опроса во избежание одновременной передачи данных удаленными радиомодулями. Возможность временного уплотнения также прозрачна для главного устройства. Временное уплотнение подходит для мест с низкой интенсивностью операций.

Переключение сотового канала связи и временное уплотнение могут использоваться вместе с одной системой Psion Teklogix: на участке могут работать один или два канала с несколькими группами мультиплексированных баз, использующих каждый канал, и переключением сотового канала.

Во всех этих случаях оператор может свободно перемещаться по участку без потери связи. Система Psion Teklogix управляет переключением каналов и передачей обслуживания между базами, не уведомляя об этом пользователя.

Для работы в качестве базовой станции или удаленного радиомодуля параметры на странице *Base Station Configuration* (Конфигурация базовой станции) на экране *Configuration Main Menu* (Главное конфигурационное меню) должны быть настроены в соответствии с описанием, приведенным в следующих разделах.

Дополнительно должны быть применены соответствующие параметры радиомодуля и главного устройства. Параметры радиомодуля находятся на экранах *Radio* (Радиомодуль) для «узкополосных» радиомодулей в соответствии с описанием, приведенным в Разд. 22.3.1. Параметры главных устройств описаны в «Разд. 22.4.4 Меню Hosts (Главные устройства)» на стр. 281.



Примечание. Прежде всего необходимо настроить основные параметры 9160 G2 в соответствии с инструкциями, изложенными в Гл. 4: «Быстрые действия по настройке и запуску оборудования» и Гл. 5: «Настройка базовых параметров». Для получения дополнительной информации о радиочастотных протоколах см. следующие разделы.

22.2 Протоколы радиосвязи

С помощью протоколов радиосвязи мобильные компьютеры устанавливают связь с базовой станцией, совместно используя канал радиосвязи с высокой эффективностью. В системах Psion Teklogix используется один из двух типов протоколов радиосвязи: протокол адаптивного опроса/коллизии компании Psion Teklogix или неproprietary протокол IEEE 802.11.

При использовании в качестве базовой станции или удаленного радиомодуля беспроводной шлюз 9160 G2 использует протокол адаптивного опроса/коллизии. Беспроводной шлюз 9160 G2 поддерживает одновременную работу базовой станции и точки доступа в режиме 802.11.

22.2.1 Протокол адаптивного опроса/коллизии

Протокол адаптивного опроса/коллизии всегда используется на узкополосных системах радиосвязи со скоростью передачи данных до 19,2 кбит/с и может использоваться в системах с расширением спектра с более высокими скоростями.

Мобильные компьютеры, работающие с этим протоколом, не передают данные, пока не получат данные опроса от беспроводного шлюза 9160 G2. Как правило, мобильные компьютеры опрашиваются в массовом порядке. При каждом опросе группам мобильных компьютеров назначаются окна ответов, в которых они могут ответить на опрос. При возникновении «коллизии», когда несколько мобильных компьютеров пытаются ответить в определенном окне, проводящий опрос беспроводной шлюз 9160 G2 делит эту группу и переназначает окна до тех пор, пока компьютеры не ответят без коллизии.

Адаптивные функции этого протокола позволяют подстраивать окна ответа под условия работы с высоким и низким трафиком данными радиообмена для предотвращения задержки данных в очереди, когда определенный мобильный компьютер имеет большой объем данных для передачи или получения.

Системы, использующие протокол адаптивного опроса/коллизии, могут применять функцию сотового канала связи для того, чтобы мобильные компьютеры использовали возможность роуминга для поддержания непрерывной связи во время перемещения между зонами покрытия.

Если сотовая базовая станция не включена, каждый раз, когда оператор переходит из зоны покрытия одной базовой станции к другой, на экране мобильного компьютера появляется сообщение «RESET: Press Enter» (СБРОС: нажмите клавишу ввода).

22.3 Меню узкополосного радиомодуля

22.3.1 Параметры настройки узкополосного радиомодуля

При выборе пункта *Radio (Радиомодуль)* в меню *Narrow Band (Узкополосный радиомодуль)* беспроводной шлюз 9160 G2 отображает страницу *Narrow Band Radio Configuration Settings (Параметры настройки узкополосного радиомодуля)* для режима, в котором работает 9160 G2 (базовая станция или удаленный радиомодуль). На этом экране вы можете настроить статус беспроводного шлюза 9160 G2 и просмотреть параметры постоянной связи карты радиомодуля RA1001A.

Рис. 22.1 Обзор параметров узкополосного радиомодуля

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

View NarrowBand radio configuration settings

Radio Card: **Installed**

Radio Card Status: ☒ Enabled ☐ Disabled

Update

General Parameters:

Modulation: 2 Level

Baud Rate: 9600

Band Start: 450 MHz

Band Size: 20 MHz

Frequency Step: 12500 Hz

Channel Bandwidth: 25000 Hz

Collision Threshold: 1154ms

TX Delay, 4 Level: 11ms

Preamble, 2 Level: 10DEL,1SOH chars

Preamble, 4 Level: 6DEL,1SOH chars

Tuning Values:

Data Squelch: 62

Frequency Adjust: -100

Power: 88

Deviation, 4 Level: 66

Deviation, 2 Level: 44

Local Oscillator Adjust: 0

Demodulator Adjust: 181

TCXO Adjust: 122

Frequencies:

| Channel | Rx | Tx |
|---------|--------------|--------------|
| 1 | 460000000 Hz | 450000000 Hz |
| 2 | 0 Hz | 0 Hz |
| 3 | 0 Hz | 0 Hz |
| 4 | 0 Hz | 0 Hz |
| 5 | 0 Hz | 0 Hz |
| 6 | 0 Hz | 0 Hz |
| 7 | 0 Hz | 0 Hz |
| 8 | 0 Hz | 0 Hz |
| 9 | 0 Hz | 0 Hz |
| 10 | 0 Hz | 0 Hz |
| 11 | 0 Hz | 0 Hz |
| 12 | 0 Hz | 0 Hz |
| 13 | 0 Hz | 0 Hz |
| 14 | 0 Hz | 0 Hz |
| 15 | 0 Hz | 0 Hz |
| 16 | 0 Hz | 0 Hz |
| 17 | 0 Hz | 0 Hz |
| 18 | 0 Hz | 0 Hz |
| 19 | 0 Hz | 0 Hz |
| 20 | 0 Hz | 0 Hz |

Статус карты радиомодуля

Этот параметр позволяет **включить** или **отключить** узкополосный радиомодуль. Карту можно **отключить** временно, если для целей тестирования необходимо отсутствие радиопомех. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

22.3.1.1 Параметры радиомодуля RA1001A

На экране *Narrow Band Radio Configuration Settings* (Параметры настройки узкополосного радиомодуля) находятся следующие параметры узкополосного радиомодуля RA1001A: *General* (Общие), *Frequencies* (Частоты) и *Tuning Values* (Настроечные значения). Эти параметры производителя нельзя изменить. Параметры приведены на рисунках ниже.

Рис. 22.2 Параметры радиомодуля RA1001A

| | |
|----------------------------|------------------|
| General Parameters: | |
| Modulation: | 2 Level |
| Baud Rate: | 9600 |
| Band Start: | 450 MHz |
| Band Size: | 20 MHz |
| Frequency Step: | 12500 Hz |
| Channel Bandwidth: | 25000 Hz |
| Collision Threshold: | 1154ms |
| TX Delay, 4 Level: | 11ms |
| Preamble, 2 Level: | 10DEL,1SOH chars |
| Preamble, 4 Level: | 6DEL,1SOH chars |

Рис. 22.3 Настроечные значения радиомодуля RA1001A

| | |
|--------------------------|------|
| Tuning Values: | |
| Data Squelch: | 62 |
| Frequency Adjust: | -100 |
| Power: | 88 |
| Deviation, 4 Level: | 66 |
| Deviation, 2 Level: | 44 |
| Local Oscillator Adjust: | 0 |
| Demodulator Adjust: | 181 |
| TCXO Adjust: | 122 |

Рис. 22.4 Частоты радиомодуля RA1001A

| Frequencies: | | |
|--------------|--------------|--------------|
| Channel | Rx | Tx |
| 1 | 460000000 Hz | 450000000 Hz |
| 2 | 0 Hz | 0 Hz |
| 3 | 0 Hz | 0 Hz |
| 4 | 0 Hz | 0 Hz |
| 5 | 0 Hz | 0 Hz |
| 6 | 0 Hz | 0 Hz |
| 7 | 0 Hz | 0 Hz |
| 8 | 0 Hz | 0 Hz |
| 9 | 0 Hz | 0 Hz |
| 10 | 0 Hz | 0 Hz |
| 11 | 0 Hz | 0 Hz |
| 12 | 0 Hz | 0 Hz |
| 13 | 0 Hz | 0 Hz |
| 14 | 0 Hz | 0 Hz |
| 15 | 0 Hz | 0 Hz |
| 16 | 0 Hz | 0 Hz |
| 17 | 0 Hz | 0 Hz |
| 18 | 0 Hz | 0 Hz |
| 19 | 0 Hz | 0 Hz |
| 20 | 0 Hz | 0 Hz |

22.3.2 Параметры подключений

При выборе этого пункта меню откроется экран, на котором вы можете выбрать режим работы беспроводного шлюза 9160 G2 — базовая станция или удаленный радиомодуль.

22.3.3 Параметры подключений: режим базовой станции

Если вы выберете пункт меню *Connectivity Options* (Параметры подключений) при работе беспроводного шлюза 9160 G2 в режиме базовой станции, будут показаны параметры «Polling Protocol» (Протокол опроса) и «Radio Parameters» (Параметры радиомодуля).

Рис. 22.5 Обзор параметров протокола опроса и радиомодуля

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Set Operating Mode and view Polling Protocol or RRM settings

Operating Mode:

Base Station

Base Station

RRM

Auto-Startup:

☒ Enabled

☐ Disabled

Shared Channel:

☐ Enabled

☒ Disabled

Polling Protocol Parameters:

Number of Poll Windows:

3

 (Range 2..4)

Size of Poll Windows:

8

 (Range 5..32)

Maximum Message Segment Size:

100

 (Range 32..116)

Number of Retries:

3

 (Range 1..7)

Collision Size:

6

 (Range 3..10)

Free Window Factor:

0

 (Range 0..7)

Message Mode Limit:

4

 (Range 0..7)

Callsign Period:

0

 (Range 0..60)

Callsign String:

Teklogix

 (Max 10 letters or digits)

Radio Parameters:

Sync Delay:

22

 (Range 3..45)

Remote Tx On:

13

 (Range 3..60)

Active Channel:

1

 (Range 1..20)

Update

Operating Mode (Режим работы)

С помощью этого параметра вы можете настроить режим работы беспроводного шлюза 9160 G2 — **Base Station** (Базовая станция) или **RRM** (Удаленный радиомодуль).

Auto-Startup (Автозапуск)

Этот параметр **включает** функцию опроса сразу после перезагрузки устройства 9160 G2. Если параметр *Auto-Startup (Автозапуск)* **отключен**, 9160 G2 будет ждать инициализации опроса со стороны сетевого контроллера.

Shared Channel (Совместно используемый канал)

Shared Channel (Совместно используемый канал) используется только в Нидерландах для соответствия требованиям органов государственного управления. Если параметр **включен**, он накладывает временные ограничения на опросы. После каждых 2 секунд опроса следует 0,5 секунды тишины — опрос не выполняется. Кроме того, если на канале обнаружен другой оператор связи, беспроводной шлюз 9160 G2 приостановит передачу радиосигналов на этом канале до его освобождения.

22.3.3.1 Параметры протокола опроса

Polling Protocol Parameters:
Number of Poll Windows: (Range 2..4)
Size of Poll Windows: (Range 5..32)
Maximum Message Segment Size: (Range 32..116)
Number of Retries: (Range 1..7)
Collision Size: (Range 3..10)
Free Window Factor: (Range 0..7)
Message Mode Limit: (Range 0..7)
Callsign Period: (Range 0..60)
Callsign String: (Max 10 letters or digits)

Number of Poll Windows (Количество окон опроса)

Этот параметр определяет количество окон опроса, которое будет использовать беспроводной шлюз 9160 G2. Значение этого параметра зависит от количества мобильных компьютеров и используемого протокола радиоканала. Табл. 22.1 описывает, как устанавливается значение параметра *Number of Poll Windows (Количество окон опроса)*.

Табл. 22.1 Количество окон опроса - протокол сотовой связи

| Количество мобильных компьютеров | Минимальное количество окон |
|----------------------------------|-----------------------------|
| 1-16 | 2 |
| 17-81 | 3 |
| 82-256 | 4 |

Size of Poll Windows (Размер окон опроса)

Значение этого параметра определяет размер самого большого сообщения, которое может быть передано беспроводным шлюзом 9160 G2 мобильному компьютеру в обычном окне опроса. Размер окна может быть изменен для передачи сообщения длиной от **5** до **32** символов.

Чем больше размер окна, тем дольше период опроса и тем больше может быть время ответа. Маленький размер окна увеличивает количество сообщений и опросов с длинными сообщениями, а также может увеличить время ответа.



Важно! В режиме «Cellular» (Сотовая связь) минимальное значение этого параметра составляет **8**.

Maximum Message Segment Size (Максимальный размер сегмента сообщения)

Этот параметр определяет максимальную длину сообщения, которое может быть передано в адрес мобильного компьютера в режиме передачи сообщений или от мобильного компьютера в режиме передачи длинных сообщений. В режиме базовой станции 9160 G2 значение этого параметра должно быть больше или совпадать со значением, указанным в сетевом контроллере или мини-контроллере 9160 G2. Диапазон значений параметра: от 32 до 116 символов. (Длинные сообщения разбиваются на несколько пакетов.) Значение по умолчанию: **100**.

Number of Retries (Количество повторов)

Этот параметр определяет количество попыток отправки сообщения беспроводным шлюзом 9160 G2 при отсутствии ответа со стороны мобильного компьютера. Повторная отправка сообщений необязательно осуществляется в ряде последовательных опросов, так как незаконченные сообщения возвращаются в конец очереди сообщений. После того, как все попытки отправки сообщений завершены, мобильный компьютер объявляется вне сети («offline»). Беспроводной шлюз 9160 G2 вновь начинает передавать сообщения мобильному компьютеру только после того, как тот объявит себя доступным в сети («online»). Возможные значения: от **1** до **7**.

Collision Size (Размер коллизии)

Этот параметр снижает вероятность того, что случайные помехи на радиоканале будут интерпретированы как коллизия между мобильными компьютерами. Время ответа увеличивается, когда 9160 G2 разрешает большое количество коллизий.

Collision Size (Размер коллизии) устанавливает верхнее ограничение на количество символов, полученных до сообщения об ошибке (CRC (циклическая проверка четности с избыточностью), CD lost (потеря CD) и т.д.). Если значение параметра равно восьми, то восемь или менее восьми символов, за которыми следует сообщение об ошибке на радиоканале, считаются помехами. Если получено более восьми символов, это считается коллизией. Возможные значения: от **3** до **10**.

Free Window Factor (Фактор свободного окна)

Значение этого параметра определяет, будет ли использоваться режим свободного окна («free window mode»). В режиме свободного окна все мобильные компьютеры, которым не назначено другое окно, будут использовать свободное окно.

Значение параметра **0** (ноль) **отключает** режим свободного окна. Увеличение значения параметра повышает вероятность того, что сообщение будет отправлено через свободное окно.

Message Mode Limit (Ограничение режима передачи сообщений)

Этот параметр определяет верхний лимит количества сообщений, которые должны добавляться в очередь на передачу перед запуском опроса в режиме передачи сообщений. Диапазон допустимых значений: от **0** до **7**, где **0** **отключает** режим передачи сообщений.



Примечание. Количество мобильных компьютеров и прошлых событий также являются частью алгоритма, определяющего, должен ли быть запущен режим передачи сообщений.

Callsign Period (Период позывного сигнала)

Позывной сигнал периодически передается в виде звукового сигнала азбуки Морзе. Этот параметр устанавливает интервал в минутах между передачей позывного сигнала. Возможные значения: от **0** до **60**. Требования федеральных агентств — министерства промышленности Канады и федерального агентства по связи США — предусматривают передачу идентификационного позывного сигнала каждой системой каждые 15 минут.

В странах, где передача позывного не является обязательной, можно установить значение этого параметра равным **0**, чтобы система не передавала позывной сигнал — это снизит время ожидания опроса на мобильных компьютерах и повысит скорость переключения каналов.

Callsign String (Строка позывного сигнала)

Длина имени должна быть не более **10** символов. Строка должна состоять только из цифр или букв. В начало передаваемого позывного сигнала необходимо добавить префикс «DE» (от).

22.3.3.2 Параметры радиомодуля

| | | |
|--------------------------|---------------------------------|---------------|
| Radio Parameters: | | |
| Sync Delay: | <input type="text" value="18"/> | (Range 3..45) |
| Remote Tx On: | <input type="text" value="4"/> | (Range 3..60) |
| Active Channel: | <input type="text" value="1"/> | (Range 1..20) |

Sync Delay (Задержка синхронизации)



Важно! Не меняйте значение этого параметра по умолчанию, если вы недостаточно хорошо знакомы с принципами таймирования протокола радиосвязи.

Sync Delay (Задержка синхронизации) устанавливает период задержки между временем передачи данных от базовой станции и первым окном ответа, измеряемый в условных отрезках времени. Значение этого параметра должно быть совместимым с другими базовыми станциями и мобильными компьютерами в системе. Радиомодуль RA1001A доступен с двух- или четырехуровневой модуляцией, обеспечивая скорость передачи данных 4800 бит/с и 9600 бит/с или 9600 бит/с и 19200 бит/с соответственно.

Значение по умолчанию для узкополосного радиомодуля с двухуровневой модуляцией и скоростью передачи данных 9600 бит/с равно **23**.

Значение по умолчанию для узкополосного радиомодуля с четырехуровневой модуляцией и скоростью передачи данных 19200 бит/с равно **31**.

Remote Txon (Включение удаленного передатчика)

Remote Txon (Включение удаленного передатчика) устанавливает время включения радиомодуля в удаленных мобильных компьютерах. Он устанавливает количество заполняющих символов, отправляемых радиомодулю до выхода реальных данных. Поскольку этот параметр основан на условных отрезках времени, количество символов зависит от скорости передачи данных радиоканала.

Значение параметра *Remote Txop* (Включение удаленного передатчика) должно быть одинаковым для всех мобильных компьютеров и оборудования базовой станции. Возможные значения: от **3** до **60**.



Важно! *Не меняйте значение этого параметра по умолчанию, если вы незнакомы с принципами таймирования протокола радиосвязи.*

Active Channel (Активный канал)

Этот параметр определяет рабочий канал связи беспроводного шлюза 9160 G2. Такой канал становится доступным для поиска мобильными компьютерами. Выбранный канал должен быть одним из тех каналов, для которых настроены частоты, согласно описанию на экране *Narrow Band Radio Configuration Settings* (Параметры настройки узкополосного радиомодуля). См. Рис. 22.4 на стр. 258 для получения информации соответствующих каналов и частот.

22.3.4 Параметры подключений: режим RRM

Если вы выберете пункт меню *Connectivity Options* (Параметры подключений) для подчиненного устройства 9160 G2, работающего в режиме удаленного радиомодуля, отобразится страница параметров RRM беспроводного шлюза 9160 G2.

Set Operating Mode and view Polling Protocol or RRM settings

Operating Mode:

Remote Radio Module Parameters:

IP Port:

IP Port (IP-порт)

С помощью этого параметра вы можете указать номер порта прослушивания беспроводного шлюза 9160 G2, работающего в режиме подчиненного удаленного радиомодуля. Возможные значения номера порта: от **1024** до **32767**.



Важно! *Номер порта должен совпадать с номером, указанным для данного беспроводного шлюза 9160 G2 в конфигурации RRM сетевого контроллера.*

22.4 Меню подключений

Беспроводной шлюз 9160 G2 Wireless Gateway может работать в режиме базовой станции или удаленного радиомодуля (RRM), способствуя установлению связи между мобильными компьютерами, беспроводными базовыми станциями и сетевым контроллером (сервером связи Psion Teklogix 9500 или беспроводным шлюзом 9160 G2 Wireless Gateway) с помощью ряда платформ. Как вариант, в роли сетевого контроллера может выступать главное устройство с запущенным Psion Teklogix SDK (обработчиком).

Беспроводной шлюз 9160 G2 также может выступать в качестве подчиненного устройства по отношению к другому шлюзу 9160 G2 в сети.

Рис. 22.6 Конфигурация базовой станции

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

View Base Station configuration settings

Slave Base Stations:

Number of configured Slave Base Stations:0

Base Station Number:1

Status:☐ Enabled ☒ Disabled

Description:Unnamed Base Station

IP Address:0.0.0.0Port:16100

Message Size:100(Range 32..116)

Auto-Startup:☒ Enabled ☐ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Base Station.

Default

Update

Cancel

22.4.1 Параметры настройки базовой станции

Базовые станции взаимодействуют по радиоканалу, используя проприетарные протоколы Psion Teklogix. Базовые станции могут быть подключены к сетевым контроллерам по протоколу TCP/IP по сетям Ethernet. Работая в режиме базовой станции, взаимодействующей с мобильными компьютерами по радиоканалу, беспроводной шлюз 9160 G2 использует протокол радиосвязи адаптивного опроса/коллизии (см. «*Протоколы радиосвязи*» на стр. 254 для получения дополнительной информации о протоколах).

Беспроводной шлюз 9160 G2 управляет работой и таймированием радиоканала. Каждая базовая станция использует свой канал радиосвязи, а мобильные компьютеры используют переключение сотового канала связи для роуминга между станциями.

Параметры, описанные на следующих страницах, позволяют настроить беспроводной шлюз 9160 G2 в качестве главной базовой станции, подключенной не более чем к 32 подчиненным базовым станциям 9160 G2 по сети Ethernet. Главная базовая станция 9160 G2 подключается к серверу связи 9500 или не более чем к шести главным устройствам с запущенным комплектом разработчика Psion Teklogix Software Development Kit. С помощью пункта *Base Station (Базовая станция)* в меню *Connectivity (Подключения)* вы сможете добавить в систему новую подчиненную базовую станцию или изменить параметры существующей подчиненной базовой станции.

Нажатие кнопки **Update** (Обновить) приведет к сохранению изменений; нажатие кнопки **Default** (По умолчанию) восстановит значения конфигурации по умолчанию для данной базовой станции.

Number of Configured Slave Base Stations (Количество настроенных подчиненных базовых станций)

Вы можете настроить до **32** подчиненных базовых станций 9160 G2.

Base Station Number (Номер базовой станции)

Значение этого параметра представляет собой номер, присвоенный базовой станции. Если выбрать параметр **Base Station Number** (Номер базовой станции) в раскрывающемся списке, отобразятся дополнительные параметры для данного устройства, которые можно изменить или удалить. Чтобы добавить новые подчиненные базовые станции, можно выбрать неиспользуемый номер и настроить связанные с ним параметры.

Status (Состояние)

Этот параметр позволяет **включить** или **отключить** подчиненную базовую станцию.

Description (Описание)

Указанное в данном параметре имя используется в качестве дополнительного способа идентификации IP-адреса подчиненной базовой станции.

IP Address (IP-адрес)

Этот параметр устанавливает соответствующий IP-адрес для подчиненной базовой станции. Параметр *IP Address (IP-адрес)* **должен иметь уникальное значение**, идентифицирующее каждую подчиненную базовую станцию в сети.

Диапазон допустимых значений: от **0.0.0.0** до **239.255.255.255**.

Значение IP-порта по умолчанию: **16100**.

Message Size (Длина сообщения)

Message Size (Длина сообщения) — максимальная длина одного сообщения, которое может быть передано мобильному компьютеру. Диапазон значений параметра: от **32** от **380** символов. (Более длинные сообщения делятся на несколько пакетов.)

Для базовых станций, работающих по протоколу опроса, максимальное значение равно **116**.

Auto-Startup (Автозапуск)

Если этот параметр **включен**, подчиненные базовые станции начинают опрос, когда включается **главная базовая станция 9160 G2**. Если параметр *Auto-Startup (Автозапуск)* **отключен**, базовые станции не начнут опрос, пока не получат команду *start polling (начать опрос)* от **главного устройства**.

22.4.2 Параметры настройки групп RRM

Кроме работы в режиме удаленного радиомодуля (RRM, см. «Параметры подключений: режим RRM» на стр. 264), беспроводной шлюз 9160 G2 может управлять другими удаленными радиомодулями. Для возможности управления удаленными радиомодулями необходимо настроить группы RRM. После настройки одной группы RRM к ней можно добавить от одного до четырех удаленных радиомодулей.

Все удаленные радиомодули в группе работают на одном канале радиосвязи. Беспроводной шлюз 9160 G2 координирует передачу данных всех удаленных радиомодулей в группе (поэтому контролирующее устройство 9160 G2 иногда называют «главным мультиплексором»).

Рис. 22.7 Обзор параметров настройки групп RRM

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

View RRM Groups configuration settings

RRM Groups:

Number of Configured RRM Groups: 0

RRM Group Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed RRM Group

Auto-Startup: ☒ Enabled ☐ Disabled

Shared Channel: ☐ Enabled ☒ Disabled

Polling Protocol Parameters:

Number of Poll Windows: 3 (Range 2..4)

Size of Poll Windows: 8 (Range 5..32)

Maximum Message Segment Size: 100 (Range 32..116)

Number of Retries: 3 (Range 1..7)

Collision Size: 6 (Range 3..10)

Free Window Factor: 0 (Range 0..7)

Message Mode Limit: 4 (Range 0..7)

Callsign Period: 0 (Range 0..60)

Callsign String: Teklogix (Max 10 letters or digits)

Radio Parameters:

Sync Delay: 22 (Range 3..45)

Remote Tx On: 13 (Range 3..60)

Active Channel: 1 (Range 1..20)

Group Parameters:

Combination 1: (Sequence of RRM indices)

Combination 2: (Sequence of RRM indices)

Remote Radio Modules:

| Enabled | Description | IP Address | Port |
|--------------------------|-------------|------------|-------|
| <input type="checkbox"/> | Unnamed RRM | 0.0.0.0 | 16132 |
| <input type="checkbox"/> | Unnamed RRM | 0.0.0.0 | 16132 |
| <input type="checkbox"/> | Unnamed RRM | 0.0.0.0 | 16132 |
| <input type="checkbox"/> | Unnamed RRM | 0.0.0.0 | 16132 |

Update

22.4.2.1 Группы RRM

RRM Groups:

Number of Configured RRM Groups: 0

RRM Group Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed RRM Group

Auto-Startup: ☒ Enabled ☐ Disabled

Shared Channel: ☐ Enabled ☒ Disabled

На этом экране пользователь может настроить параметры новой группы RRM. Каждый удаленный радиомодуль должен быть членом группы RRM; на беспроводном шлюзе 9160 G2 можно настроить несколько групп RRM. Группа RRM может включать от одного до четырех удаленных радиомодулей.

Этот экран очень похож на экран, описанный в «Параметры подключений: режим базовой станции» на стр. 258, с той разницей, что параметры, настраиваемые в описанных выше меню, используются для радиомодуля RA1001A, находящегося в 9160 G2, а параметры, описываемые здесь, используются для других, удаленных устройств 9160 G2 (удаленных радиомодулей).

Number of Configured RRM Groups (Количество настроенных групп RRM)

Показывает количество групп RRM, настроенных в данном устройстве 9160 G2.

RRM Group Number (Номер группы RRM)

Значение этого параметра представляет собой номер, присвоенный группе RRM. Если выбрать параметр **RRM Group Number** (Номер группы RRM) в раскрывающемся списке, отобразятся дополнительные параметры для данного устройства, которые можно изменить или удалить. Чтобы добавить новые группы RRM, можно выбрать неиспользуемый номер и настроить связанные с ним параметры.

Status (Состояние)

Этот параметр позволяет **включить** или **отключить** группу RRM.

Description (Описание)

В этом текстовом поле пользователь может указать имя новой группы RRM. В виде значения может выступать любой текст. Значение по умолчанию: **Unnamed RRM Group** (Группа RRM без названия).

Auto-Startup (Автозапуск)

Если этот параметр **включен**, беспроводной шлюз 9160 G2 при загрузке устанавливает связь с удаленными радиомодулями, входящими в эту группу RRM, и автоматически начинает опрос. Если параметр *Auto-Startup (Автозапуск)* **отключен**, беспроводной шлюз 9160 G2 при загрузке устанавливает связь с удаленными радиомодулями, входящими в эту группу RRM, но начинает опрос в этой группе RRM только после команды начала опроса, полученной от главного устройства. Опрос начинается, если по крайней мере один удаленный радиомодуль, входящий в группу RRM, работает при загрузке 9160 G2.

Shared Channel (Совместно используемый канал)

Если этот параметр **включен**, перед опросом беспроводной шлюз 9160 G2 проверяет наличие другого трафика на канале радиосвязи, используемом группой RRM.

Если этот параметр **отключен**, беспроводной шлюз 9160 G2 считает, что он может эксклюзивно использовать канал радиосвязи для этой группы RRM, и выполняет опрос без проверки трафика.

Этот параметр является обязательным для систем, установленных в Нидерландах.

22.4.2.2 Параметры протокола опроса



Предупреждение. Эти параметры предварительно настроены для вашей системы. Не меняйте их, если вы недостаточно хорошо знакомы с принципами их действия на радиоканал.

| Polling Protocol Parameters: | | |
|-------------------------------|---------------------------------------|----------------------------|
| Number of Poll Windows: | <input type="text" value="3"/> | (Range 2..4) |
| Size of Poll Windows: | <input type="text" value="8"/> | (Range 5..32) |
| Maximum Message Segment Size: | <input type="text" value="100"/> | (Range 32..116) |
| Number of Retries: | <input type="text" value="3"/> | (Range 1..7) |
| Collision Size: | <input type="text" value="6"/> | (Range 3..10) |
| Free Window Factor: | <input type="text" value="0"/> | (Range 0..7) |
| Message Mode Limit: | <input type="text" value="4"/> | (Range 0..7) |
| Callsign Period: | <input type="text" value="0"/> | (Range 0..60) |
| Callsign String: | <input type="text" value="Teklogix"/> | (Max 10 letters or digits) |

Number of Poll Windows (Количество окон опроса)

В этом текстовом окне пользователь может указать количество окон опроса, в которых удаленный радиомодуль прослушивает ответы мобильных компьютеров после отправки опроса. Возможные значения: от **2 до 4**. По умолчанию используется значение **3**.

Size of Poll Windows (Размер окон опроса)

В этом текстовом окне пользователь может указать размер окон опроса, в которых удаленные модули данной группы RRM прослушивают ответы мобильных компьютеров. Возможные значения: от **5 до 32**. По умолчанию используется значение **8**.

Maximum Message Segment Size (Максимальный размер сегмента сообщения)

В этом текстовом окне пользователь может указать размер самого большого сегмента сообщения (в байтах), которое будет отправляться по радиосети Psion Teklogix. Сообщения большего размера делятся на части. Возможные значения: от **32 до 116**. По умолчанию используется значение **100**.

Number of Retries (Количество повторов)

В этом текстовом поле пользователь может указать количество попыток повторной отправки сообщения удаленным радиомодулем мобильному компьютеру в случае отсутствия ответа от мобильного компьютера перед объявлением компьютера вне сети («offline»). Возможные значения: от **1 до 7**. По умолчанию используется значение **3**.

Collision Size (Размер коллизии)

В этом текстовом поле пользователь может указать минимальное количество символов помех, полученных удаленным модулем, которое будет интерпретироваться на оборудовании Psion Teklogix как помехи. При превышении этого значения удаленный радиомодуль начинает разрешение коллизии. Возможные значения: от **3 до 10**. По умолчанию используется значение **6**.

Free Window Factor (Фактор свободного окна)

В этом текстовом поле пользователь может указать вероятность добавления в опрос удаленного радиомодуля свободное окно, через которое ответ может передать любой мобильный компьютер. Возможные значения: от **0 до 7**. По умолчанию используется значение **0**.

Message Mode Limit (Ограничение режима передачи сообщений)

В этом текстовом поле пользователь может указать вероятность добавления опроса в режиме отправки сообщений. Возможные значения: от **0 до 7**. По умолчанию используется значение **4**.

Callsign Period (Период позывного сигнала)

В этом текстовом поле пользователь может указать период времени между передачами позывного сигнала. Значение параметра измеряется в минутах. Значение 0 (ноль) означает, что позывной передаваться не будет. Возможные значения: от **0** до **60**. По умолчанию используется значение **0**.

Callsign String (Строка позывного сигнала)

В этом текстовом поле пользователь может указать строку текста позывного сигнала удаленного радиомодуля. Передача текста выполняется в формате азбуки Морзе. По умолчанию используется значение **Teklogix**.

22.4.2.3 Параметры радиомодуля

| | | |
|--------------------------|---------------------------------|---------------|
| Radio Parameters: | | |
| Sync Delay: | <input type="text" value="22"/> | (Range 3..45) |
| Remote Tx On: | <input type="text" value="13"/> | (Range 3..60) |
| Active Channel: | <input type="text" value="1"/> | (Range 1..20) |

Так как некоторые параметры радиомодуля совпадают с параметрами группы удаленных модулей, работающих в режиме временного уплотнения, они могут быть настроены один раз на беспроводном шлюзе 9160 G2, который затем передаст эти параметры удаленным радиомодулям в группе. В эти параметры входят задержка синхронизации (*Sync Delay*), удаленное включение передатчика (*Remote Txon*) и номер используемого канала (*Active Channel*).

Хотя узкополосный радиомодуль RA1001A в каждом радиомодуле группы RRM настраивается отдельно, беспроводной шлюз 9160 G2 считает, что они настраиваются одинаково. Чтобы убедиться в этом, шлюз 9160 G2 смотрит на некоторые параметры, возвращаемые каждым удаленным радиомодулем. Эти параметры включают скорость передачи данных и время включения передатчика.

Значения параметров сравниваются со значениями, возвращенными другими удаленными радиомодулями в той же группе. Если значения не совпадают, появляются сообщения об ошибке, но для использования выбирается значение наихудшего случая.



Предупреждение. Эти параметры предварительно настроены для вашей системы. Не меняйте их, если вы недостаточно хорошо знакомы с принципами их действия на радиоканал.

Sync Delay (Задержка синхронизации)

В этом текстовом поле пользователь может указать количество символов задержки, вставляемое между передачей данных удаленным радиомодулем и первым окном ответа. Возможные значения: от **3 до 45**. По умолчанию используется значение **22**.

Remote Txon (Включение удаленного передатчика)

В этом текстовом поле пользователь может указать количество заполняющих символов, отправляемых радиомодулями мобильных компьютеров перед тем, как мобильные компьютеры отправят данные сообщений. Возможные значения: от **3 до 60**. По умолчанию используется значение **13**.

Active Channel (Активный канал)

В этом текстовом поле пользователь может указать радиоканал, который будет использоваться всеми удаленными радиомодулями в группе RRM. Возможные значения: от **1 до 20**. По умолчанию используется значение **1**.

22.4.2.4 Параметры группы

Group Parameters:
Combination 1: (Sequence of RRM indices)
Combination 2: (Sequence of RRM indices)

Combination (Комбинация)

В этих текстовых полях пользователь может указать подгруппы RRM, которые называются *комбинациями (combinations)*. Если зоны покрытия двух или нескольких удаленных радиомодулей в данной группе RRM не пересекаются, непересекающиеся удаленные радиомодули могут выполнять опрос одновременно. Это улучшает время ответа системы и снижает количество переданных сигналов в сети. Удаленные радиомодули, не включенные в комбинации, выполняют опрос индивидуально после опросов комбинаций.

Например, если в группе RRM из трех удаленных радиомодулей радиомодули 1 и 3 не пересекаются, из них может быть сформирована одна комбинация (*Combination 1*). Эти радиомодули будут выполнять опрос одновременно. Удаленный модуль 2 может быть помещен в другую подгруппу (*Combination 2*). Эти две подгруппы выполняют опросы по очереди.

Чтобы настроить комбинацию, введите номера удаленных радиомодулей в текстовое поле для этой комбинации. Эти номера должны соответствовать номерам удаленных радиомодулей, указанных в списке удаленных радиомодулей на странице меню *Remote Radio Modules (Удаленные радиомодули)* (см. стр. 275). Например, значение «13» в текстовом поле для комбинации 1 (*Combination 1*) добавляет в эту подгруппу удаленные радиомодули 1 и 3.



Примечание. При настройке комбинаций RRM убедитесь, что номера настраиваемых удаленных модулей введены последовательно и не указаны отсутствующие номера, что может произойти при удалении радиомодулей и последующем добавлении удаленных радиомодулей. Комбинации используют удаленные радиомодули в том порядке, в каком они появляются в списке, а не в том, в каком они перечислены в списке.

22.4.2.5 Удаленные радиомодули

| Remote Radio Modules: | | | |
|---------------------------------------|-------------|-------------------|-------|
| Enabled | Description | IP Address : Port | |
| 1 <input checked="" type="checkbox"/> | Built-in | 10.128.75.174 | 16132 |
| 2 <input type="checkbox"/> | Unnamed RRM | 0.0.0.0 | 16132 |
| 3 <input type="checkbox"/> | Unnamed RRM | 0.0.0.0 | 16132 |
| 4 <input type="checkbox"/> | Unnamed RRM | 0.0.0.0 | 16132 |

В этом меню отображаются удаленные радиомодули, которые входят в данную группу RRM, включая такие параметры как «Description» (Описание), «IP address» (IP-адрес) и «Port number» (Номер порта), установленные в подменю *Connectivity Options (Параметры подключений)* беспроводного шлюза 9160 G2, работающего в режиме удаленного радиомодуля (см. «Параметры подключений: режим RRM» на стр. 264). Каждый радиомодуль может быть включен и отключен из этого меню.

22.4.3 Параметры настройки функций радиоканала

В меню *Connectivity (Подключения)* выберите пункт *Radio Link Features (Функции радиоканала)*, чтобы открыть экран параметров настройки для режимов опроса и сотовой связи.

Рис. 22.8 Обзор параметров настройки функций радиоканала

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

View Radio Link Features configuration settings

Radio Link Features:

Operate in Cellular Mode: ☒ Enabled ☐ Disabled

Poll ID: Range (0..255)

Polling Protocol Terminal Timeout: Range (1..240)

Percent Polling Protocol Terminal Timeout: Range (50..90)

Direct TCP Connections for TekTerm: ☐ Enabled ☒ Disabled

Direct TCP Check Duplicate Terminal Number: ☒ Enabled ☐ Disabled

Expiration period (in days) for Automatic Radio Address and Terminal Number: Range (2..365)

Automatic Radio Address

First Address: Last Address: Ranges (1..3840)

Automatic Terminal Number

Group Ranges (1..1024)

| | | | | Comments |
|---|--------------------------------|-----|--------------------------------|----------|
| 1 | <input type="text" value="0"/> | ... | <input type="text" value="0"/> | |
| 2 | <input type="text" value="0"/> | ... | <input type="text" value="0"/> | |
| 3 | <input type="text" value="0"/> | ... | <input type="text" value="0"/> | |
| 4 | <input type="text" value="0"/> | ... | <input type="text" value="0"/> | |
| 5 | <input type="text" value="0"/> | ... | <input type="text" value="0"/> | |

Update

22.4.3.1 Функции радиоканала

| | |
|--|---|
| Radio Link Features: | |
| Operate in Cellular Mode: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Poll ID: | <input type="text" value="35"/> Range (0..255) |
| Polling Protocol Terminal Timeout: | <input type="text" value="60"/> Range (1..240) |
| Percent Polling Protocol Terminal Timeout: | <input type="text" value="75"/> Range (50..90) |
| Direct TCP Connections for TekTerm: | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Direct TCP Check Duplicate Terminal Number: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Expiration period (in days) for Automatic Radio Address and Terminal Number: <input type="text" value="2"/> Range (2..365) | |

Operate in Cellular Mode (Работа в режиме сотовой связи)

Для работы в режиме сотовой базовой станции этот параметр должен быть **включен**.



Примечание. Сервер связи 9500 также должен быть настроен для работы в режиме сотовой связи.

Poll ID (Идентификатор опроса)

В протоколе адаптивного опроса/коллизии для узкополосных радиомодулей параметр *Poll ID (Идентификатор опроса)* используется для назначения уникального адреса для каждой базовой станции. По мере перемещения мобильных компьютеров от одной базовой станции к другой этот адрес передается базовыми станциями мобильным компьютерам для идентификации каждого устройства 9160 G2 в системе с несколькими базовыми станциями.

Polling Protocol Terminal Timeout (Время ожидания завершения протокола опроса)

Этот параметр определяет время (в минутах), в течение которого мобильный компьютер может быть неактивным до того, как 9160 G2 объявит его вне сети («offline»). Прежде чем это случится, мобильный компьютер будет объявлен вне сети параметром *Percent Polling Protocol Terminal Timeout (Время ожидания завершения протокола опроса в процентах)* (см. ниже).

После удаления мобильного компьютера из системы для установки связи с беспроводным шлюзом 9160 G2 ему нужно пройти повторную инициализацию. Этот параметр снижает общие издержки использования радиоканала, вызванные поддержкой невзаимодействующих мобильных компьютеров. Возможные значения: от **1** до **240**.

Percent Polling Protocol Terminal Timeout (Время ожидания завершения протокола опроса в процентах)

Этот параметр определяет время, в течение которого мобильный компьютер может быть неактивным до того, как 9160 G2 объявит его вне сети («offline»). Время определяется в процентах от значения параметра *Polling Protocol Terminal Timeout (Время ожидания завершения протокола опроса)* (см. выше). Например, если значение параметра *Polling Protocol Terminal Timeout (Время ожидания завершения протокола опроса)* равно 60, а значение этого параметра равно 75%, тогда время ожидания составит $60 \text{ мин.} \times 75\% = 45 \text{ мин.}$

Мобильный компьютер, находящийся вне сети, все еще считается частью системы. Сообщения, предназначенные для таких мобильных компьютеров, ставятся в очередь на беспроводном шлюзе 9160 G2. Мобильный компьютер остается вне сети до тех пор, пока не отправит сообщение по сети. Диапазон значений параметра: от **50** до **90**.

Direct TCP Connections for TekTerm (Прямые TCP-подключения для TekTerm)

Включение этого параметра позволяет программе *TekTerm*, установленной на мобильных компьютерах Psion Teklogix, подключаться непосредственно к беспроводному шлюзу 9160 G2, работающего в режиме базовой станции по отношению к главному устройству по протоколу TCP/IP.

Direct TCP Check Duplicate Terminal Number (Проверка дублирования номера терминала при прямом TCP-подключении)

Если этот параметр включен, беспроводной шлюз 9160 G2 будет отклонять подключение мобильных компьютеров по прямому протоколу TCP с использованием номера терминала, который уже используется другим мобильным компьютером. Если параметр отключен, связь устанавливается с мобильным компьютером, который запрашивал подключение последним из компьютеров, использующих одинаковый номер терминала.

22.4.3.2 Автоматическое назначение адреса радиомодуля

| | | |
|--------------------------------|-----------------------------------|---|
| Automatic Radio Address | | |
| First Address: | <input type="text" value="1024"/> | Last Address: <input type="text" value="2048"/> |
| Ranges (1..3840) | | |

Каждый мобильный компьютер Psion Teklogix, использующий радиоканал, имеет уникальный адрес радиомодуля, который может быть назначен автоматически беспроводным шлюзом 9160 G2 при включении этого параметра.

Чтобы **включить** параметр, значения первого и последнего адреса радиомодулей должны быть в пределах от **1** до **3840**. Значения по умолчанию для диапазона: **1024 ... 2084**. Чтобы **отключить** параметр, установите значение **0**.



Примечания. При включении параметра должны выполняться следующие условия:

1. *Прямые TCP-подключения для TekTerm должны быть отключены (см. стр. 278).*
2. *Параметр «Auto ID» (Автоматическое назначение идентификатора) на мобильном компьютере должен быть включен, чтобы радиомодулю можно было назначить адрес автоматически.*
3. *Не включайте параметр «Auto Startup» (Автоматический запуск) (см. стр. 343) на базовых станциях 9150 или 9160 G2, работающих в режиме 802.IQ с сеансами, использующими параметры «Automatic Radio Address» (Автоматическое назначение адреса радиомодуля) и «Automatic Terminal Number» (Автоматическое назначение номера терминала).*

Expiration Period (Срок действия)

Этот параметр устанавливает период в днях, в течение которого определенный адрес радиомодуля или номер терминала должен быть неактивным до того, как беспроводной шлюз 9160 G2 объявит его истекшим («expired»). Адрес или номер терминала с истекшим сроком действия может быть назначен другому радиомодулю или сеансу.



Примечание. Для использования этой функции рекомендуется включить функцию *SNTP* и установить сервер *SNTP* для точного расчета срока действия.

22.4.3.3 Automatic Terminal Number (Автоматическое назначение номера терминала)

Номер терминала назначается для каждого сеанса приложения, созданного на мобильном компьютере. Этот номер является уникальным идентификатором всех переданных и полученных данных сеанса.

| Automatic Terminal Number | | | |
|---------------------------|--------------------------------|------------------------------------|----------------------|
| Group | Ranges (1..1024) | | Comments |
| 1 | <input type="text" value="0"/> | ... <input type="text" value="0"/> | <input type="text"/> |
| 2 | <input type="text" value="0"/> | ... <input type="text" value="0"/> | <input type="text"/> |
| 3 | <input type="text" value="0"/> | ... <input type="text" value="0"/> | <input type="text"/> |
| 4 | <input type="text" value="0"/> | ... <input type="text" value="0"/> | <input type="text"/> |
| 5 | <input type="text" value="0"/> | ... <input type="text" value="0"/> | <input type="text"/> |

Номера терминалов могут быть автоматически назначены сеансом приложений. Кроме того, контроллер присваивает групповой номер для использования с сеансами TESS и ANSI. Можно определить не более пяти групп сеансов терминала, каждой из которых присваивается свой диапазон номеров терминала для автоматического назначения. Диапазоны разных групп не должны пересекаться.

Такие группы можно определять только для сеансов TESS и ANSI. На мобильном компьютере приложения терминалов TESS или ANSI указывают, к какой группе они принадлежат, и используют диапазон номеров терминалов для автоматического назначения, принадлежащий этой группе.

Для всех других типов сеансов используется диапазон номеров терминалов для автоматического назначения от 1 до 3840 и не используется параметр группы. Типы сеансов, отличные от ANSI и TESS, для которых используется автоматическое назначение номеров терминалов (например, «Remote Sockets» (Удаленные сокет)), должны иметь собственный диапазон терминалов, начинающийся со значения 1, и достаточно большой для обеспечения всех мобильных компьютеров.

Экран *Radio Link Features (Функции радиоканала)* имеет несколько параметров для каждой группы автоматического назначения номера терминала: диапазон номеров терминалов от наименьшего до наибольшего и комментарий. Комментарий представляет собой строку текста в формате ASCII, который может использоваться для описания группы.



Примечания. При включении функции «*Automatic Terminal Number*» (Автоматическое назначение номера терминала) должны соблюдаться следующие условия:

1. Прямые TCP-подключения для *TekTerm* должны быть отключены (см. стр. 278).
2. Параметр «*Auto Session*» (Автоматический сеанс) на мобильном компьютере должен быть включен, чтобы сеансу можно было назначить номер сеанса автоматически.

22.4.4 Меню *Hosts* (Главные устройства)

Когда беспроводной шлюз 9160 G2 работает в режиме базовой станции, он должен взаимодействовать с «хостом» — сервером связи 9500 или главным компьютером, на котором установлен Psion Teklogix Software Development Kit (SDK). Поэтому каждый главный сетевой контроллер, хост SDK или главная базовая станция, взаимодействующая с устройством 9160 G2, должна быть настроена как главное устройство. На экране *Hosts* (Главные устройства) в меню *Connectivity* (Подключения) отображается описание главного устройства, выбранного из раскрывающегося списка (см. Рис. 22.9 на стр. 282).

Это меню содержит имена главных устройств, присутствующих в системе. Поддерживается максимум шесть главных устройств. После настройки параметров главного устройства можно выбрать пункт **Host Number** (Номер главного устройства). При этом отображается список дополнительных параметров, которые можно изменить или удалить.

Рис. 22.9 Обзор параметров настройки главного устройства базовой станции

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

View the configuration settings for a Base Station's Host

Hosts:

Number of configured Hosts: 0

Host Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed Host

First Terminal: 1

Last Terminal: 32

9010 Configuration:

No Online/Offline: ☐ Enabled ☒ Disabled

Monitor Poll: ☐ Enabled ☒ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host. Default

Update

Cancel

Number Of Configured Hosts (Число настроенных главных устройств)

На экране *Hosts* (Главные устройства) в меню *Connectivity* (Подключения) отображается число главных устройств, настроенных в системе. Поддерживается максимум шесть главных устройств.

Host Number (Номер главного устройства)

Значение этого параметра представляет собой номер, присвоенный главному устройству. Если выбрать параметр **Host Number** (Номер главного устройства) в раскрывающемся списке, отобразятся дополнительные параметры для данного устройства, которые можно изменить или удалить. Чтобы добавить новое главное устройство, можно выбрать неиспользуемый номер и настроить связанные с ним параметры.

Номер главного устройства также отображается на экране мобильного компьютера с поддержкой радиосвязи при переключении между главными устройствами (если в системе присутствует несколько таких устройств).

Status (Состояние)

Чтобы мобильные компьютеры могли устанавливать связь с этим главным устройством, для параметра «Status» (Состояние) необходимо выбрать значение **Enabled** (Включено).

Description (Описание)

В этом текстовом поле можно ввести имя протокола, используемого главным устройством. Протоколы — это способы установления связи между мобильными и главными компьютерами в различных физических средах, таких как сеть Ethernet и подключения радиоканалов.

Когда устройство 9160 G2 используется в качестве базовой станции, оно связывается с главным устройством **9010/ TCP/IP** с помощью сетевого подключения. Протокол 9010 — это частный асинхронный протокол, разработанный компанией Psion Teklogix. Этот протокол используется для передачи потоков данных TESS (Teklogix Screen Subsystem) или ANSI на мобильные компьютеры. Для получения подробных сведений см. разделы по *серверу связи 9500, SDK, TESS* или *ANSI* в соответствующем *Руководстве пользователя Psion Teklogix*.

First Terminal/Last Terminal (Первый терминал/последний терминал)

Значения этих параметров определяют первый и последний терминалы в рабочем диапазоне мобильных компьютеров, взаимодействующих с главным устройством. Указанные здесь номера терминалов сопоставляются с конкретным главным устройством. В качестве номера терминала можно указать число от **1** до **3840**.

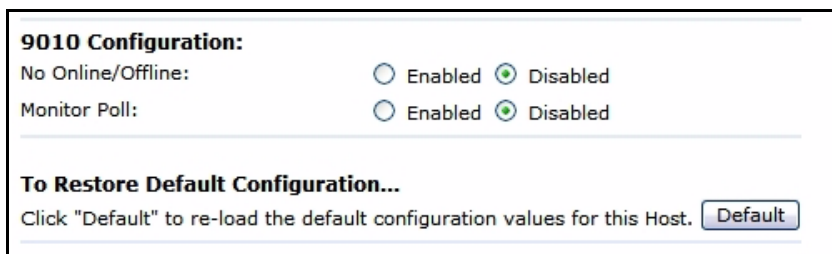
To Restore Default Configuration (Восстановление конфигурации по умолчанию)

В нижней части вкладки меню «Host» (Главное устройство) находится кнопка **Default** (По умолчанию), нажав на которую, можно повторно загрузить значения конфигурации по умолчанию для данного главного устройства.

Updating Settings (Обновление параметров)

В процессе настройки главного устройства можно обновить параметры нажатием на кнопку *Update* (Обновить) или отменить внесенные изменения нажатием на кнопку *Cancel* (Отмена) в нижней части экрана.

22.4.4.1 Конфигурация 9010



9010 Configuration:

No Online/Offline: ☐ Enabled ☒ Disabled

Monitor Poll: ☐ Enabled ☒ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host.

No Online/Offline (Без уведомлений об изменении сетевого статуса)

Если этот параметр **включен**, 9160 G2 **не уведомляет** главное устройство об изменениях сетевого статуса мобильного компьютера. Если этот параметр **отключен**, 9160 G2 **уведомляет** главное устройство об изменениях сетевого статуса мобильного компьютера. По умолчанию этот параметр **отключен**.

Monitor Poll (Мониторинг опроса)

Как правило, отправка сообщений или нулевых опросов беспроводному шлюзу 9160 G2 занимает приблизительно 40 секунд. Если этот параметр **включен**, базовая станция 9160 G2 выполняет мониторинг сообщений и опросов своего главного устройства; если сообщение или опрос не поступают в течение 40 секунд, он закрывает соединение. По умолчанию этот параметр **отключен**.

КОНФИГУРАЦИЯ МИНИ-КОНТРОЛЛЕРА

23

| | |
|--|-----|
| 23.1 Обзор | 287 |
| 23.2 Меню настройки мини-контроллера | 288 |
| 23.3 Меню Hosts (Главные устройства) | 288 |
| 23.4 Параметры меню Host (Главное устройство). | 292 |
| 23.4.1 Эмуляция 3274 | 292 |
| 23.4.1.1 Параметры эмуляции | 292 |
| 23.4.1.2 Параметры TESS | 294 |
| 23.4.1.3 Параметры протокола Telnet | 305 |
| 23.4.1.4 Параметры функциональных клавиш | 309 |
| 23.4.2 Эмуляция 5250 | 310 |
| 23.4.2.1 Параметры эмуляции | 310 |
| 23.4.2.2 Параметры TESS | 311 |
| 23.4.2.3 Параметры протокола Telnet | 323 |
| 23.4.2.4 Параметры функциональных клавиш | 327 |
| 23.4.3 Эмуляция ANSI | 328 |
| 23.4.3.1 Параметры эмуляции | 328 |
| 23.4.3.2 Параметры протокола Telnet | 333 |
| 23.4.3.3 Auto-Telnet/Auto-login (Автоматическое подключение Telnet/Автоматический вход) | 335 |
| 23.4.3.4 Параметры функциональных клавиш | 340 |

23.1 Обзор

Сетевой контроллер выполняет ряд важных функций в системе Psion Teklogix. Одной из этих функций является *эмуляция*. Под эмуляцией подразумевается преобразование данных из протокола главного компьютера в протокол, используемый мобильными компьютерами Psion Teklogix.

Данные, которые передаются с главного компьютера, выводятся на экран мобильного компьютера и возвращаются на главный компьютер после выполнения определенных операций на мобильном компьютере, называются потоком данных. С главных компьютеров на мобильные могут передаваться различные типы потоков данных.

Мобильные компьютеры Psion Teklogix могут непосредственно принимать только два типа потоков данных: *TESS* и *ANSI*. TESS (Teklogix Screen Subsystem) — частный формат потоков данных, используемый мобильными компьютерами Psion Teklogix. ANSI — стандартный тип потоков данных, используемый проводными мобильными компьютерами ANSI. Другие типы потоков данных, передаваемые с главного компьютера на мобильные компьютеры Psion Teklogix, необходимо преобразовывать в формат TESS или ANSI, иначе обработка этих данных будет невозможна. Все эти преобразования выполняются программами эмуляции, установленными на сетевом контроллере.

Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает функции эмуляции, что позволяет использовать его в качестве мини-контроллера. Если устройство 9160 G2 настроено для работы в качестве мини-контроллера, мобильные компьютеры Psion Teklogix могут эмулировать мобильные компьютеры ANSI, 5250 или 3274, используя устройство 9160 G2 вместо сервера связи 9500.



Важно! *Устройства 9160 G2, выполняющие функции мини-контроллеров, предназначены для небольших площадок с низкой интенсивностью операций. Сервер связи 9500 является обязательным компонентом систем, в которых требуется поддержка более 50 мобильных компьютеров.*

Беспроводной шлюз 9160 G2 Wireless Gateway, выполняющий функции мини-контроллера, может поддерживать до 32 объединенных в сеть базовых станций и до 50 мобильных компьютеров. Мини-контроллер 9160 G2 также может использоваться для управления конфигурациями беспроводных сетей.

Устройство 9160 G2, настроенное для работы в качестве мини-контроллера, поддерживает следующие типы эмуляций:

- эмуляция устройств 5250 с использованием TCP/IP по Ethernet LAN;

- эмуляция устройств 3274 с использованием TCP/IP по Ethernet LAN;
- эмуляция устройств ANSI с использованием TCP/IP по Ethernet LAN.



Примечание. Прежде всего необходимо настроить основные параметры 9160 G2 в соответствии с инструкциями, изложенными в предыдущих главах данного руководства.

Устройства 9160 G2 также можно интегрировать в системы mapRF с помощью протокола 802.IQv2 (для получения дополнительной информации см. раздел «Меню функций 802.IQ v2» на стр. 347).



Примечание. Функция мини-контроллера становится доступна только после ее разблокировки с помощью пароля, введенного в консоли.

23.2 Меню настройки мини-контроллера

Чтобы использовать устройство в качестве мини-контроллера, необходимо правильно настроить параметры на экранах *Hosts (Главные устройства)*. Если выбрать пункт *Hosts (Главные устройства)* в списке параметров *Connectivity (Подключения)*, отобразится экран *Configuration Settings For A Base Station's Host (Параметры настройки для главного устройства базовой станции)*. Для получения информации о настройке параметров протоколов радиосвязи см. раздел «Параметры настройки функций радиоканала» на стр. 275.

23.3 Меню Hosts (Главные устройства)

Это меню содержит имена главных устройств, присутствующих в системе. Поддерживается максимум шесть главных устройств. Параметры главного устройства необходимо настроить для каждого главного компьютера, взаимодействующего с мини-контроллером 9160 G2. После настройки параметров главного устройства можно выбрать пункт **Host Number** (Номер главного устройства). При этом отображается список дополнительных параметров, которые можно изменить или удалить.

Рис. 23.1 Обзор параметров настройки главных устройств

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Maintenance

Configuration

Upgrade

View the configuration settings for a Base Station's Host

Hosts:

Number of configured Hosts: 0

Host Number: 1

Status: Enabled Disabled

Description: Unnamed Host

First Terminal: 1

Last Terminal: 32

Emulation: 5250

5250 Emulation Options:

Write Error Code: Advisory text

Use International EBCDIC:

Allow null character in fixed fields:

TESS Options:

Field Underline Remapping: None

Alarm:

Clear:

Pass thru:

Procedures:

Local:

Host Print:

Remote Print:

Pages: 8

Transmit Line: 0

AIAG: 0

Visible Match Character: 0

Hidden Match character: 0

Serial I/O: 0

Print Line: 0

Print Form Length: 0

Barcode: 0

Entry Line: 0

Field Overhead: 5

Command Region: 0, 0, 0, 0

Telnet Protocol Options:

Terminal Type: IBM-5251-11

Host Port: 23

Maximum Sessions per Terminal: 4

First Local Terminal Port: 10000

Local IP Address to Bind: 0.0.0.0

First Terminal Listen Port: 0

Actively Negotiate with Host:

Auto-telnet: DISABLE

Auto-telnet Host:

Auto-telnet without User Action:

Enable Virtual Device Names:

Configure Device Names: Configure

Device Name Prefix:

Function Key Mappings:

F1: F1 F14: F14 F27: F17

F2: F2 F15: F15 F28: F18

F3: F3 F16: CLEAR F29: UP

F4: F4 F17: PRINT F30: SESS

F5: F5 F18: HELP F31: ENTER

F6: F6 F19: F19 F32: ENTER

F7: F7 F20: F20 F33: ENTER

F8: F8 F21: F21 F34: ENTER

F9: F9 F22: F22 F35: ENTER

F10: F10 F23: F23 F36: ENTER

F11: F11 F24: F24 F37: ENTER

F12: F12 F25: DOWN F38: SELECTOR

F13: F13 F26: F16 F39: ENTER

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host. Default

Update Cancel

When the 9160 acts as a Base Station, it must communicate with a "host" - a 9500 or 9400 network Controller, or a host computer using Psion Teklogix Software Development Kit (TSDK).

This page allows you to select the host names present on the system. Up to six hosts can be supported. A "host" must be configured for each master network controller, TSDK host, or master Base Station that communicates with the 9160.

Number Of Configured Hosts (Число настроенных главных устройств)

В разделе настроек *Connectivity* (Подключения) на экране *Hosts* (Главные устройства) отображается число главных устройств, настроенных в системе. Поддерживается максимум шесть главных устройств.

Host Number (Номер главного устройства)

Значение этого параметра представляет собой номер, присвоенный главному устройству. Если выбрать параметр **Host Number** (Номер главного устройства) в раскрывающемся списке, отобразятся дополнительные параметры для данного устройства, которые можно изменить или удалить. Чтобы добавить новое главное устройство, можно выбрать неиспользуемый номер и настроить связанные с ним параметры.

Номер главного устройства также отображается на экране мобильного компьютера с поддержкой радиосвязи при переключении между главными устройствами (если в системе присутствует несколько таких устройств).

Status (Состояние)

Чтобы мобильные компьютеры могли устанавливать связь с этим главным устройством, для параметра «Status» (Состояние) необходимо выбрать значение **Enabled** (Включено).

Description (Описание)

В этом текстовом поле можно ввести имя протокола, используемого главным устройством. Протоколы — это способы установления связи между мобильными и главными компьютерами в различных физических средах, таких как сеть Ethernet и подключения радиоканала.

Когда устройство 9160 G2 используется в качестве базовой станции, оно связывается с главным устройством **9010/ TCP/IP** с помощью сетевого подключения. Протокол 9010 — это частный асинхронный протокол, разработанный компанией Psion Teklogix. Этот протокол используется для передачи потоков данных TESS (Teklogix Screen Subsystem) или ANSI на мобильные компьютеры. Для получения подробных сведений см. разделы по *серверу связи 9500*, *SDK*, *TESS* или *ANSI* в соответствующем *Руководстве пользователя Psion Teklogix*.

First Terminal/Last Terminal (Первый терминал/последний терминал)

Значения этих параметров определяют первый и последний терминалы в рабочем диапазоне мобильных компьютеров, взаимодействующих с главным устройством. Указанные здесь номера терминалов сопоставляются с конкретным главным устройством. В качестве номера терминала можно указать число от **1** до **3840**.

Emulation (Эмуляция)

В этом раскрывающемся списке можно выбрать типы эмуляции главного устройства, поддерживаемые беспроводным шлюзом 9160 G2 Wireless Gateway. Взаимодействуя с мобильными компьютерами и базовыми станциями Psion Teklogix, устройство 9160 G2 может эмулировать мобильные компьютеры IBM 3278-2, 5251-11 и 5555-B01, а также мобильные компьютеры ANSI.

Протоколы — это способы установления связи между мобильными и главными компьютерами в различных средах, таких как сеть Ethernet и подключения радиоканала. Устройство 9160 G2 поддерживает протокол TCP/IP. Поддерживаемые типы эмуляции:

- 9010/TCP/IP (подробнее далее в этом разделе);
- 3274 Emulation (Эмуляция 3274) (см. описание параметров настройки на стр. 292–309);
- 5250 Emulation (Эмуляция 5250) (см. описание параметров настройки на стр. 310–327);
- ANSI Emulation (Эмуляция ANSI) (см. описание параметров настройки на стр. 328–340).

Когда беспроводной шлюз 9160 G2 Wireless Gateway функционирует как базовая станция, для соединения с сервером связи 9500 или главным устройством используется эмуляция 9010 (частный асинхронный протокол, разработанный компанией Psion Teklogix) и пакет Psion Teklogix Software Development Kit (SDK). Информацию о настройке режима работы базовой станции и эмуляции 9010 на устройстве 9160 G2 см. в Гл. 22: «9160 G2 в режиме базовой станции».

Когда беспроводной шлюз 9160 G2 Wireless Gateway функционирует как мини-контроллер, для связи с главными устройствами IBM используются протоколы эмуляции 3274 и 5250, а для связи с мобильными компьютерами ANSI — протокол эмуляции ANSI.

To Restore Default Configuration (Восстановление конфигурации по умолчанию)

В нижней части вкладки меню Host (Главное устройство) находится кнопка **Default** (По умолчанию), нажав на которую, можно повторно загрузить значения конфигурации по умолчанию для данного главного устройства.

Updating Settings (Обновление параметров)

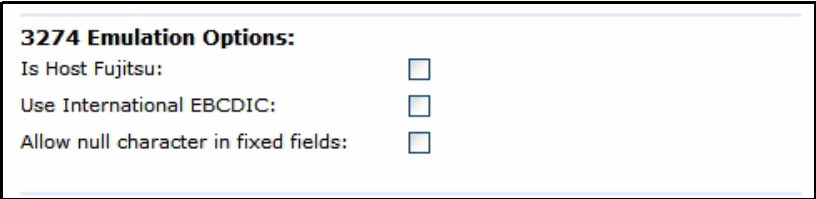
В процессе настройки главного устройства можно обновить параметры нажатием на кнопку *Update* (Обновить) или отменить внесенные изменения нажатием на кнопку *Cancel* (Отмена) в нижней части экрана.

23.4 Параметры меню Host (Главное устройство)

Если выбрать существующее значение *Host Number* (Номер главного устройства), устройство 9160 G2 отобразит параметры настройки для этого главного устройства. Для протоколов эмуляции 5250, 3274 и ANSI предусмотрено четыре подменю: *Emulation Options* (Параметры эмуляции), *TESS Options* (Параметры TESS), *Telnet Protocol Options* (Параметры протокола Telnet) и *Function Key Mappings* (Параметры функциональных клавиш). Обзор этого экрана см. на Рис. 23.1 на стр. 289.

23.4.1 Эмуляция 3274

23.4.1.1 Параметры эмуляции



При эмуляции IBM 3274 или IBM 5250 мини-контроллер 9160 G2 преобразует поток данных приложения, передаваемый главным устройством, в команды TESS (Teklogix Screen Subsystem). Некоторые параметры на этом экране регулируют преобразование данных главного устройства в данные TESS.

Is Host Fujitsu (Главное устройство Fujitsu)

Если этот параметр **включен**, мини-контроллер 9160 G2 будет ожидать передачи от главного устройства данных (например, команд), специфичных для главных устройств Fujitsu. Если включен этот параметр, стандартные коды форматирования IBM (начало поля, указание буфера и т. д.) заменяются кодами, характерными для главных компьютеров Fujitsu.

Use International EBCDIC (Использовать международный EBCDIC)

Если этот параметр **включен**, мини-контроллер 9160 G2 использует международную кодировку EBCDIC, меняя местами символы ! и].

Allow null character in fixed fields: (Разрешить пустые символы в фиксированных полях:)

Если этот параметр **включен**, мини-контроллер 9160 G2 разрешает использование пустых символов в пробелах в полях, имеющих визуальные атрибуты видео, например негативное видеоизображение. По умолчанию эмуляция главных устройств 3274 **отключена**.

23.4.1.2 Параметры TESS

TESS Options:

Alarm:

☐

Clear:

☐

Passthru:

☐

Procedures:

☐

Local:

☐

Host Print:

☐

Remote Print:

☐

Pages:

8

(Range 1..79)

Transmit Line:

0

(Range 0..24)

AIAG:

0

(Range 0..255)

Visible Match Character:

0

(Range 0..255)

Hidden Match character:

0

(Range 0..255)

Serial I/O:

0

(Range 0..255)

Print Line:

0

(Range 0..24)

Print Form Length:

0

(Range 0..24)

Barcode:

0

(Range 0..255)

Entry Line:

0

(Range 0..24)

Field Overhead:

5

(Range 0..80)

Command Region:

0

,

0

,

0

,

0

Alarm (Аварийный сигнал)

Если этот параметр **включен**, мобильные компьютеры подают звуковой сигнал, когда на экране приложения в области, заданной параметром *Command Region* (Командная область), отображается слово «ALARM» (АВАРИЙНЫЙ СИГНАЛ) (см. стр. 304). Слово «ALARM» должно представлять собой поле, доступное только для отображения.



Примечание. Чтобы использовать этот параметр, необходимо включить параметр «Command Region» (Командная область).

Clear (Очистить)

Если этот параметр **включен**, мини-контроллер 9160 G2 создает *пустое* поле ввода для поля ввода, заполненного пробелами.

Некоторые приложения на главных устройствах используют видео-атрибуты отображаемых символов для выделения полей, в частности полей ввода. Например, экран приложения может определить все поля ввода с негативным видеоизображением и заполнить это поле пробелами. Эта функция доступна для мобильных компьютеров, поддерживающих негативное видеоизображение. Если компьютер не поддерживает негативное видеоизображение, это поле может стать невидимым, так как оно полностью состоит из пробелов.

По умолчанию все пустые поля ввода, отображаемые на экране мобильного компьютера Psion Teklogix, выделяются с помощью «символа ввода», заданного в конфигурации мобильного компьютера.



Примечание. Эта операция выполняется только на экранах, полученных от главного устройства. Данные, передаваемые на главное устройство, остаются без изменений.

Passthru (Сквозная пересылка)

Если этот параметр **включен**, устройство 9160 G2 разрешает главному устройству пересылать данные непосредственно на последовательный порт мобильного компьютера с поддержкой радиосвязи. В большинстве случаев эта функция используется для печати.

Подготовка экранов главного устройства к сквозной пересылке

На экране, пересылаемом через последовательный порт мобильного компьютера, в первой строке, начиная со второго столбца, должно находиться слово **PASSTHRU** (заглавными буквами). Фактические данные, передаваемые на мобильный компьютер, могут начинаться с любого места под первой строкой.

При эмуляции 5250 или 3274 атрибуты располагаются в буфере экрана. Атрибут, размещенный между столбцом 2 и окончанием слова «PASSTHRU», смещает все последующие символы на одну позицию вправо. Следовательно, все требуемые атрибуты необходимо размещать в столбце 1 первой строки (непосредственно перед словом «PASSTHRU»).

Пример:

| |
|---------------------------------|
| столбец: 1 2 3 4 5 6 7 8 9 |
| строка 1: @ P A S S T H R U @ |
| строка 2: @ P A R T : 1 2 3 4 5 |

где @ является атрибутом.

После завершения отправки данных на принтер мобильного компьютера устройство 9160 G2 передает на главное устройство ключ *ENTER*. Главное устройство находится в режиме ожидания и не передает остальные экраны (в том числе другие экраны PASSTHRU) на этот мобильный компьютер до получения ключа *ENTER*.



Примечание. Информацию о настройке параметров сквозной передачи на мобильном компьютере можно найти в руководстве пользователя соответствующей модели мобильного компьютера.

Procedures (Инструкции)

Если этот параметр **включен**, главное устройство может передавать инструкции TESS через устройство 9160 G2 на мобильные компьютеры. Инструкция TESS — это группа команд TESS, запускаемых командой *TESS execute procedure*.

Local (Локальные)

Если этот параметр **включен**, устройство 9160 G2 позволяет главному устройству предоставлять страницы для загрузки в виде локальных инструкций TESS на мобильных компьютерах.

Локальные инструкции выбираются в меню на мобильном компьютере. Эти инструкции могут выполняться на мобильных компьютерах, когда они работают в автономном режиме. Когда мобильные компьютеры снова подключаются к сети, результаты выполнения инструкций передаются на главное устройство.



*Примечание. Чтобы использовать параметр Local (Локальные), необходимо **включить** параметр Procedures (Инструкции).*

Host Print (Печать с главного устройства)

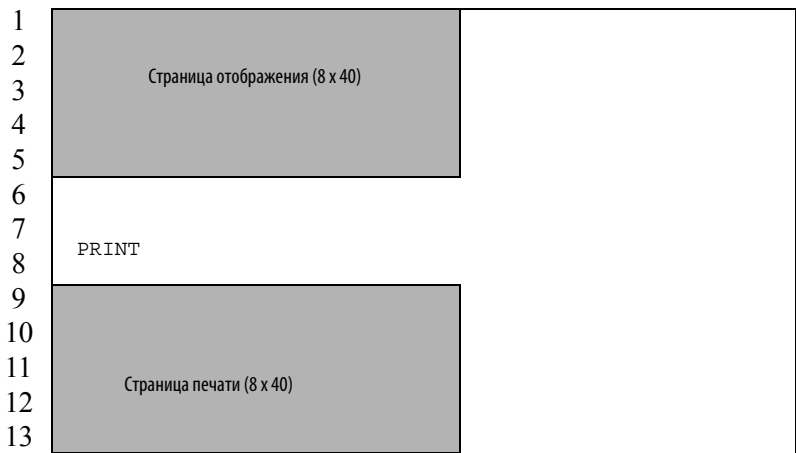
Когда этот параметр **включен**, главное устройство может вывести на экраны мобильных компьютеров дополнительные данные и передать на мобильный компьютер команду на печать этих данных. В этом заключается отличие данной функции от функции *Local Print (Локальная печать)*, при использовании которой запрос на печать инициируется мобильным компьютером.

Текст, пересылаемый на принтер, форматируется по размеру экрана приложения 24 x 80. Если главное устройство может инициировать печать, этот текст будет распечатан. Устройство 9160 G2 распознает дополнительный текст как страницу печати благодаря слову «PRINT», *набранному заглавными буквами* и размещенному в начале 2-го столбца в строке 13 на экране 24 x 80. Слово «PRINT» должно быть определено как текст, *доступный только для отображения*.

Страница печати располагается под страницей отображения мобильного компьютера (см. рисунок ниже). Размер страницы печати всегда соответствует размеру страницы отображения мобильного компьютера (при условии, что в конфигурации мобильного компьютера задана длина страницы менее 12 строк).

Если параметр *Host Print (Печать с главного устройства)* **включен**, устройство 9160 G2 передает страницу печати на мобильный компьютер после получения экрана приложения от главного устройства.

Рис. 23.2 Экран приложения со страницей печати





Примечания.

1. В отличие от параметра «Passthru» (Сквозная пересылка), при использовании параметра «Host Print» (Печать с главного устройства) невозможно передавать на принтер управляющие команды.
2. На мобильном компьютере должна быть включена поддержка печати с помощью команды «Printer» (Принтер) в меню «Features» (Функции) TESS; дополнительные сведения см. в руководстве пользователя соответствующей модели мобильного компьютера.

Remote Print (Удаленная печать)

Когда этот параметр **включен**, устройство 9160 G2 передает страницу печати на мобильный компьютер каждый раз, когда мобильный компьютер отправляет соответствующий запрос. При этом мобильный компьютер передает функциональный ключ «F17» или ключ «PRINT» (в более старых версиях мобильных компьютеров). Устройство 9160 G2 передает результат функции обратно на главное устройство.

В этом заключается отличие данной функции от функции *Host Print (Печать с главного устройства)*, при использовании которой запрос на печать инициируется главным устройством.



Примечание. На мобильном компьютере должна быть включена поддержка печати. Для получения дополнительной информации см. руководство пользователя соответствующей модели мобильного компьютера.

Pages (Страницы)

Этот параметр определяет число экранов (или страниц) главного устройства, сохраняемых на мобильном компьютере (максимальное число – **79**).

Устройство 9160 G2 сокращает объем данных, передаваемых на мобильные компьютеры, используя возможность мобильного компьютера сохранять страницу данных для каждого отображаемого экрана. 9160 G2 сохраняет изображение каждой страницы, хранящейся на мобильном компьютере. После получения экрана приложения устройство 9160 G2 пытается сопоставить этот экран с сохраненной страницей. Если в памяти мобильного компьютера уже есть похожая страница, 9160 G2 передает на мобильный компьютер команду повторного отображения копии этой страницы; с контроллера передаются только необходимые изменения. Если совпадений не найдено, страница полностью пересылается на мобильный компьютер по радиоканалу.



*Примечание. На мобильном компьютере также предусмотрен соответствующий параметр, и **фактическое** число сохраненных страниц соответствует **меньшему** из значений этих двух параметров.*

Transmit Line (Строка передачи)

Если эта функция **включена**, все измененные на мобильном компьютере данные автоматически передаются, когда оператор вводит данные в поле *transmit-upon-entry*.

Значение в этом текстовом поле определяет строку на экране, которая называется *transmit line (строка передачи)*. Последнее поле ввода, находящееся над строкой передачи или на этой строке, определяется как поле *transmit-upon-entry*. Если в строках ниже строки передачи есть другие поля ввода, ни одно из полей ввода не считается полем *transmit-upon-entry*.

Если в поле указано значение **0** (ноль), функция отключена. Если указано значение **24**, *последнее* поле ввода на каждом экране приложения определяется как поле *transmit-upon-entry*.

AIAG

Этот параметр предоставляет функции автообнаружения и заполнения для входных данных, поступающих от сканеров штрихкодов. При вводе данных штрихкода в мобильный компьютер на текущей странице осуществляется поиск полей «AIAG», которые можно заполнить данными штрихкода. Данные, предварительно подставленные в поле «AIAG» программным приложением, определяют, будут ли приняты данные штрихкода.

На мини-контроллере 9160 G2 задается десятичное значение символа ASCII от **0** до **255**, соответствующее идентификатору поля AIAG («AIAG Field Identifier»), указанному на главном устройстве. Если указано значение **0**, функция отключена.

Предварительно подставляемые данные имеют следующий формат:

<mode> <AIAG prefix(data)>

Символ «mode», используемый в сочетании с командой, позволяет включать различные рабочие режимы для определенных операций приложения. Операция автоматического обнаружения и заполнения применяется только к данным, полученным со сканера штрихкодов. Описания режимов и префиксов AIAG приведены в Табл. 23.1 на стр. 300. Эти режимы настраиваются на главном устройстве.

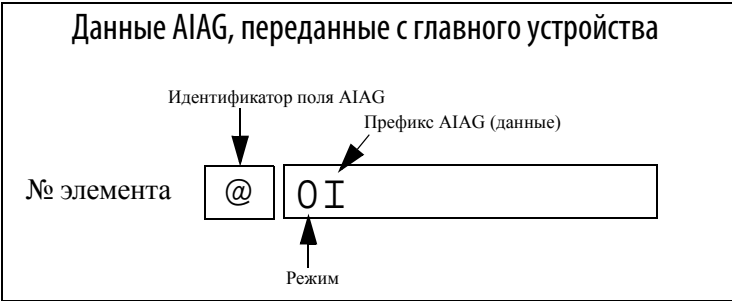
Табл. 23.1 Описание функций режимов и префиксов AIAG

| Режим | Функция |
|--|--|
| 0 | Отобразить префикс, передать префикс на главное устройство. |
| 1 | Не отображать префикс, передать префикс на главное устройство. |
| 2 | Отобразить префикс, не передавать префикс на главное устройство. |
| 3 | Не отображать префикс, не передавать префикс на главное устройство. |
| +4 | Если добавить 4 к вышеперечисленным значениям, данные будут передаваться на главное устройство, когда будут заполнены все поля AIAG с набором 4. Функция 0 применяется «принудительно», если в данном наборе бит есть поля и все они заполнены данными, введенными оператором. |
| +8 | Если добавить 8 к вышеперечисленным значениям, будут перезаписаны все данные, введенные ранее. |
| +16 | Добавление цифры 16 к вышеперечисленным значениям позволяет указать приоритет позиции курсора для поиска и заполнения. |
| AIAG Prefix (data) (Префикс AIAG (данные)) | Текст для поиска соответствий в поле AIAG. |

Пример.

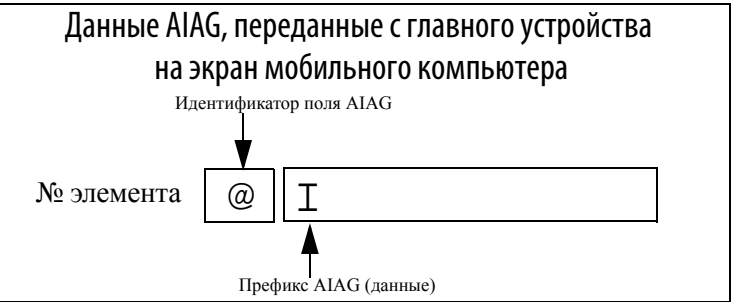
В этом примере показан экран с данными, определенными на главном устройстве и передаваемыми с этого устройства. Данные включают в себя «AIAG Identifier» (Идентификатор AIAG) – тег, определяющий поле AIAG – после которого указан режим, в данном случае «Mode 0» (Режим 0), и «AIAG Prefix» (Префикс AIAG) – I.

Рис. 23.3 Поле AIAG, передаваемое с главного устройства



Когда переданная информация выводится на экран мобильного компьютера, система находит соответствующее поле AIAG для отсканированных данных с помощью идентификатора AIAG. Поскольку на главном устройстве задан режим «Mode 0», префикс AIAG (I) отображается на экране мобильного компьютера, а после заполнения этого экрана отправляется обратно на главное устройство.

Рис. 23.4 Поле AIAG, отправленное на мобильный компьютер



Символ явного совпадения

Если вставить специальный символ ASCII непосредственно перед полем ввода, приложение сможет отличить «поле совпадения» от поля ввода. Допустим, что в качестве символа, определяющего поля явного совпадения, используется угловая скобка «>».

Если вставить символ «>» сразу перед полем ввода, оно будет определено как поле совпадения (см. ниже).

Part #> _____

Диапазон значений этого параметра – от 0 до 255 – представляет десятичные значения символов ASCII. Если указано значение 0, функция отключена.

Десятичное значение ASCII, заданное на устройстве 9160 G2, должно совпадать со значением, заданным в приложении.

При использовании функции *Visible Match (Явное совпадение)* главный компьютер предварительно подставляет данные в поле ввода совпадения; эти данные выводятся на экран мобильного компьютера. Предварительно загруженные данные, которые передаются на мобильный компьютер, могут состоять из конкретных символов, специальных символов совпадений или сочетаний этих символов. Информацию о символах совпадений, распознаваемых мобильными компьютерами Psion Teklogix, см. в Табл. 23.2.

Если поле ввода не совпадает с предварительно подставленными данными, данные отображаются на экране, мобильный компьютер подает звуковой сигнал и курсор перемещается на начальную позицию в поле совпадения. Оператор может ввести в поле совпадения другие данные или переместить курсор в другое поле. Когда в поле совпадения вводятся данные (даже если они не совпадают с предварительно загруженными данными), эти данные передаются на главное устройство вместе с другими данными, измененными на мобильном компьютере, во время следующего сеанса передачи.

Табл. 23.2 Символы совпадений

| Символ | Описание |
|--------|---|
| # | Совпадение с числом. |
| & | Совпадение с буквой (в любом регистре). |
| ^ | Совпадение с буквой в верхнем регистре. |
| _ | Совпадение с буквой в нижнем регистре. |
| | Совпадение с буквенно-числовым символом. |
| " | Совпадение с буквой, числом или пробелом. |
| ? | Совпадение с символом пунктуации. |
| ' | Совпадение с любым символом. |
| : | Совпадение всех позиций символов в поле с предшествующим символом. |
| ; | Совпадение любых оставшихся символов, но не обязательно остальных символов поля, с предшествующим символом. |

Пример.

Допустим, что в поле ввода необходимо предварительно подставить номер детали. Если вам известен номер детали, вы можете предварительно подставить его в это поле. Если требуется более гибкий подход, при котором номер детали всегда начинается с двух буквенных символов, за которыми следуют дефис и четыре цифры, строка совпадения для данного поля будет иметь следующий вид: **&&-####**.

Символ скрытого совпадения

В отличие от данных в поле «явного совпадения» данные, предварительно подставленные в поле «скрытого совпадения», не отображаются на экране мобильного компьютера.



Примечание. Для получения подробных сведений о сопоставлении полей см. раздел «Символ явного совпадения» на стр. 301.

Диапазон значений этого параметра – от **0** до **255** – представляет десятичные значения символов ASCII. Если указано значение **0**, функция отключена. Десятичное значение ASCII, заданное на устройстве 9160 G2, должно совпадать со значением, заданным в приложении.

Serial I/O (Последовательный ввод/вывод)

Поля *Serial I/O (Последовательный ввод/вывод)* представляют собой поля ввода и фиксированные поля, которые заполняются входными и выходными данными, передаваемыми через последовательный порт. Приложение определяет поле как поле *последовательного ввода/вывода*, если этому полю предшествует специальный символ.

Если этот символ предшествует фиксированному полю, данные будут отправлены на последовательный порт мобильного компьютера. Если этот символ предшествует полю ввода, это поле будет заполнено данными, принятыми через последовательный порт мобильного компьютера.

Диапазон значений этого параметра – от **0** до **255** – представляет десятичные значения символов ASCII. Если в поле указано значение **0** (ноль), функция отключена.

Print Line (Строка печати)

Этот параметр позволяет указать начальное число в строке страницы печати на экране приложения (см. также *Entry Line (Строка ввода)*). Если указано значение до **24**, страница отображения будет распечатана; если указано значение **0** (ноль), функция отключена.

Print Form Length (Длина формы печати)

Этот параметр определяет длину формы принтера в строках. Возможные значения: от **0** до **24**.

Barcode (Штрихкод)

Поля *barcode-input-only* представляют собой специальные поля ввода, которые заполняются только данными, полученными от сканера штрихкодов. Приложение определяет поле ввода как поле *barcode-input-only*, если этому полю предшествует специальный символ.

Диапазон значений этого параметра — от **0** до **255** — представляет десятичные значения символов ASCII. Если в поле указано значение **0** (ноль), функция отключена.

Entry Line (Строка ввода)

Этот параметр определяет число первой строки, которая отображается, если в левой верхней части экрана нет полей ввода и если поле ввода находится на этой строке или под ней.

Параметр *Entry Line (Строка ввода)* позволяет автоматически сместить экран главного устройства так, чтобы в области, отображаемой на экране мобильного компьютера, поместилось поле ввода, которое в противном случае находилось бы за пределами этой области. На некоторых мобильных компьютерах Psion Teklogix с небольшим дисплеем отображается только левый верхний угол экрана приложения.

Field Overhead (Дополнительный интервал между полями)

Этот параметр определяет максимально допустимое число символов между двумя *фиксированными* полями, при котором 9160 G2 по-прежнему может объединить эти два поля в одно.

Устройство 9160 G2 иногда объединяет два смежных фиксированных поля в одно и передает их в таком виде. Это позволяет сократить излишние нагрузки на радиоканал.

Например, если два поля находятся на расстоянии 4 символов друг от друга, а в качестве значения параметра выбрано число 5, эти поля будут объединены в одно.

Command Region (Командная область)

Этот параметр определяет область на экране главного устройства, которую устройство 9160 G2 проверяет на наличие зарезервированных команд.

Четыре числа, указанные в текстовых полях раздела *Command Region* (Командная область), представляют собой адреса строк и столбцов левого верхнего угла и правого нижнего угла командной области. Первое текстовое поле в каждой из этих пар содержит число строки, а второе — число столбца. Возможные значения строк — от 0 до 24; возможные значения столбцов — от 0 до 80.

Например, чтобы определить две последних строки на экране главного устройства как командную область, можно ввести значения 23, 1 и 24, 80.

В настоящее время поддерживается только одна команда *ALARM* (подробное описание этой команды см. на стр. 294). Когда на любой позиции в командной области размещается слово «ALARM», устройство 9160 G2 передает на мобильный компьютер команду TESS *beep*, вызывающую звуковой сигнал.

23.4.1.3 Параметры протокола Telnet

Telnet Protocol Options:

| | |
|---|---|
| Terminal Type: | IBM-3278-2 |
| Host Port: | 23 (Range 1..32767) |
| Maximum Sessions per Terminal: | 4 (Range 1..127) |
| First Local Terminal Port: | 10000 (Range 1..32767) |
| Local IP Address to Bind: | 0.0.0.0 |
| First Terminal Listen Port: | 0 (Range 0..32767) |
| Actively Negotiate with Host: | <input type="checkbox"/> |
| Configure LU Names: | <input type="checkbox"/> Configure |
| LU Name Prefix: | |
| Send IAC Interrupt Process as a System Request: | <input type="checkbox"/> |
| Send IAC Break as an Attention Key: | <input type="checkbox"/> |
| Auto-telnet: | DISABLE |
| Auto-telnet Host: | |
| Auto-telnet without User Action: | <input checked="" type="checkbox"/> |

Terminal Type (Тип терминала)

Этот параметр позволяет выбрать тип мобильного компьютера, который будет эмулироваться устройством 9160 G2 для данного главного устройства. В настоящее время для типа эмуляции 3274 Emulation (Эмуляция 3274) можно выбрать мобильные компьютеры **IBM 3278-2** и **IBM 3278-2-E**.

Host Port (Порт главного устройства)

Этот параметр позволяет указать номер порта главного устройства для выбранного подключения *3274 Emulation (Эмуляция 3274)*. По умолчанию используется значение **23**.

Maximum Sessions per Terminal (Максимальное число сеансов на терминал)

Этот параметр определяет максимально допустимое число сеансов Telnet, иницируемых каждым мобильным компьютером. Возможные значения: от **1** до **127**, по умолчанию используется значение **4**.

First Local Terminal Port (Локальный порт первого терминала)

Этот параметр определяет номер локального порта, через который первый мобильный компьютер будет подключаться к исходящим сеансам Telnet. По умолчанию используется значение **10000**.

Local IP Address to Bind (Локальный IP-адрес для привязки)

Этот параметр определяет IP-адрес сетевого адаптера на устройстве 9160 G2, через который первый мобильный компьютер будет подключаться к исходящим сеансам Telnet.

First Terminal Listen Port (Порт прослушивания первого терминала)

Этот параметр определяет первый номер порта, который будет прослушиваться устройством 9160 G2 на наличие запросов подключения к мобильным компьютерам по протоколу Telnet. Чтобы **включить** этот параметр, необходимо выбрать значение не меньше **1024**. Чтобы **отключить** порт прослушивания, необходимо указать значение **0**.

По умолчанию используется значение **0** (отключено).

Actively Negotiate with Host (Активное согласование с главным устройством)

Если этот параметр включен, устройство 9160 G2 начинает процесс согласования с главным устройством во время установления соединения Telnet. Для большинства главных устройств этот параметр использовать не рекомендуется.

Configure LU Names (Настройка имен LU)

Telnet Terminal Naming

To remove an LU Name, click the "Remove" button. Ensure that you have selected at least one terminal. See the Help panel for more information.

| <input type="checkbox"/> Edit | Terminal Number | LU Name |
|---------------------------------|-----------------|---------|
| <input type="checkbox"/> [Edit] | 1 | ABC |
| <input type="checkbox"/> [Edit] | 5 | THING |

Selected Terminals:

Add a Terminal...

To associate an LU Name with a Terminal, fill in the fields below and click "Add Name".

Terminal Number:

LU Name:

Для каждого настроенного мобильного компьютера требуется одно имя LU («LU Name»). На этом экране можно назначить имена LU (см. также *LU Name Prefix (Префикс имени LU)* далее в этом разделе). Имя LU должно быть уникальным и должно быть связано с номером терминала («Terminal Number»), присвоенным мобильному компьютеру. Имя LU может состоять максимум из 10 буквенно-числовых символов. Символы нижнего регистра при вводе автоматически преобразуются в символы верхнего регистра.

LU Name Prefix (Префикс имени LU)

Если мобильному компьютеру не присвоено имя LU, устройство 9160 G2 создает полное имя LU, добавляя к префиксу LU («LU Prefix») номер терминала («Terminal Number») (пять цифр, при необходимости в начале можно ввести нули).

Send IAC Interrupt Process as a System Request (Передавать команду прерывания процесса IAC как системный запрос)

Если этот параметр включен, устройство 9160 G2 передает запрос на прерывание процесса IAC на главное устройство как системный запрос 3274.

Send IAC Break as an Attention Key (Назначить IAC Break ключом прерывания)

Если этот параметр включен, устройство 9160 G2 передает запрос IAC Break на главное устройство как ключ прерывания 3274.

Auto-telnet (Автоматическое подключение Telnet)

Этот параметр позволяет разрешить или запретить автоматическое подключение мобильных компьютеров к данному главному устройству через сеансы Telnet.

Доступные значения: **Disable** (Отключить) и **Auto-telnet** (Автоматическое подключение Telnet). По умолчанию используется значение **Disable** (Отключить).

Когда параметр *Auto-telnet* (Автоматическое подключение Telnet) **отключен**, сеансы подключения Telnet к главному устройству необходимо инициировать вручную на мобильных компьютерах.

Когда параметр *Auto-telnet* (Автоматическое подключение Telnet) **включен**, устройство 9160 G2 инициирует один сеанс Telnet на каждом мобильном компьютере, номер терминала которого соответствует данному главному устройству. На каждом мобильном компьютере можно инициировать дополнительные сеансы Telnet для подключения к главному устройству, но это необходимо делать вручную.

Когда параметр *Auto-telnet* (Автоматическое подключение Telnet) **включен**, устройство 9160 G2 автоматически устанавливает соединение Telnet с главным устройством, как при запуске, так и при завершении сеанса.



Примечание. Сеансы автоматического подключения Telnet инициируются только для мобильных компьютеров, которые находятся «в сети» (включены и корректно функционируют в радиосети Psion Teklogix).

Auto-telnet Host (Главное устройство для автоматического подключения Telnet)

Этот параметр определяет имя или IP-адрес главного устройства, с которым устройство 9160 G2 соединяет автоматические сеансы Telnet.



Примечание. Имя компьютера, указанное в этом текстовом поле, должно иметь формат, распознаваемый устройством 9160 G2: 9160 G2 должно иметь возможность получить IP-адрес для этого имени. Например, здесь можно указать имя, соответствующее записи в таблице главных устройств 9160 G2, или 9160 G2 может отправить запрос на сервер доменных имен.

В качестве имени главного устройства можно указать любое имя, которое можно использовать в команде TCP> на мобильном компьютере.

Auto-telnet Without User Action (Автоматическое подключение Telnet без участия пользователя)

Если этот параметр включен, контроллер немедленно открывает подключение к главному устройству для каждого инициализированного мобильного компьютера без нажатия на клавишу [ENTER].

23.4.1.4 Параметры функциональных клавиш

Function Key Mappings:

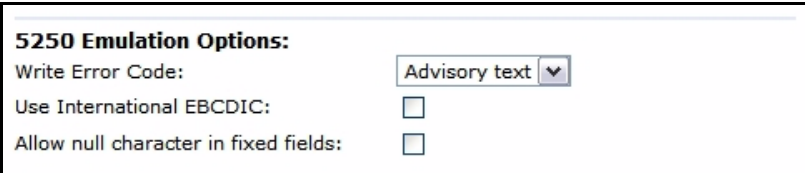
| | | |
|---------------------------------------|--|---|
| F1: <input type="text" value="F1"/> | F14: <input type="text" value="PA2"/> | F27: <input type="text" value="F13"/> |
| F2: <input type="text" value="F2"/> | F15: <input type="text" value="PA3"/> | F28: <input type="text" value="F14"/> |
| F3: <input type="text" value="F3"/> | F16: <input type="text" value="CLEAR"/> | F29: <input type="text" value="F15"/> |
| F4: <input type="text" value="F4"/> | F17: <input type="text" value="F17"/> | F30: <input type="text" value="SESS"/> |
| F5: <input type="text" value="F5"/> | F18: <input type="text" value="F18"/> | F31: <input type="text" value="F16"/> |
| F6: <input type="text" value="F6"/> | F19: <input type="text" value="F19"/> | F32: <input type="text" value="ENTER"/> |
| F7: <input type="text" value="F7"/> | F20: <input type="text" value="F20"/> | F33: <input type="text" value="ENTER"/> |
| F8: <input type="text" value="F8"/> | F21: <input type="text" value="F21"/> | F34: <input type="text" value="ENTER"/> |
| F9: <input type="text" value="F9"/> | F22: <input type="text" value="F22"/> | F35: <input type="text" value="ENTER"/> |
| F10: <input type="text" value="F10"/> | F23: <input type="text" value="F23"/> | F36: <input type="text" value="ENTER"/> |
| F11: <input type="text" value="F11"/> | F24: <input type="text" value="F24"/> | F37: <input type="text" value="ENTER"/> |
| F12: <input type="text" value="F12"/> | F25: <input type="text" value="SYSREQ"/> | F38: <input type="text" value="ENTER"/> |
| F13: <input type="text" value="PA1"/> | F26: <input type="text" value="ATTN"/> | F39: <input type="text" value="ENTER"/> |

Функциональная клавиша n

Параметр *Function Key* (Функциональная клавиша) позволяет выбрать код, который будет передан на главное устройство при нажатии функциональной клавиши на мобильном компьютере. Для каждой функциональной клавиши можно выбрать вариант из одного и того же списка доступных кодов. Однако по умолчанию всем функциональным клавишам назначены разные коды. Значения по умолчанию представлены на этой странице.

23.4.2 Эмуляция 5250

23.4.2.1 Параметры эмуляции



5250 Emulation Options:

Write Error Code: Advisory text ▼

Use International EBCDIC: ☐

Allow null character in fixed fields: ☐

При эмуляции IBM 5250 или IBM 3274 мини-контроллер 9160 G2 преобразует поток данных приложения, передаваемый главным устройством, в команды TESS (Teklogix Screen Subsystem). Некоторые параметры на этом экране регулируют преобразование данных главного устройства в данные TESS.

Write Error Code (Вывод кода ошибки)

Если для этого параметра выбрано значение *advisory text* (информационный текст), устройство 9160 G2 передает коды ошибок на экран мобильного компьютера в виде информационного сообщения, которое выводится в нижней части экрана. Если для этого параметра выбрано значение *screen text* (экранный текст), устройство 9160 G2 передает коды ошибок в виде обычного экранного текста.

Use International EBCDIC (Использовать международный EBCDIC)

Если этот параметр **включен**, устройство 9160 G2 поменяет местами символы ! и | в таблице символов EBCDIC.

Allow null character in fixed fields: (Разрешить пустые символы в фиксированных полях:)

Если этот параметр **включен**, мини-контроллер 9160 G2 разрешает использование пустых символов в пробелах в полях, имеющих визуальные атрибуты видео (например, негативное видеоизображение). По умолчанию эмуляция главных устройств 5250 **включена**.

23.4.2.2 Параметры TESS

TESS Options:

Field Underline Remapping:

None

Alarm:

☐

Clear:

☐

Passthru:

☐

Procedures:

☐

Local:

☐

Host Print:

☐

Remote Print:

☐

Pages:

8

(Range 1..79)

Transmit Line:

0

(Range 0..24)

AIAG:

0

(Range 0..255)

Visible Match Character:

0

(Range 0..255)

Hidden Match character:

0

(Range 0..255)

Serial I/O:

0

(Range 0..255)

Print Line:

0

(Range 0..24)

Print Form Length:

0

(Range 0..24)

Barcode:

0

(Range 0..255)

Entry Line:

0

(Range 0..24)

Field Overhead:

5

(Range 0..80)

Command Region:

0

,

0

,

0

,

0

Field Underline Remapping (Изменение параметров выделения полей)

Вы можете изменить видеоатрибуты отображаемых символов для выделения полей ввода. Доступные значения: *None (Нет)*, *Blink (Мигание)*, *Bold (Полужирный)* и *Reverse (Негатив)*.

Alarm (Аварийный сигнал)

Если этот параметр **включен**, мобильные компьютеры подают звуковой сигнал, когда на экране приложения в области, заданной параметром *Command Region (Командная область)*, заглавными буквами отображается слово «ALARM» (АВАРИЙНЫЙ СИГНАЛ) (см. стр. 322). Слово «ALARM» должно представлять собой поле, *доступное только для отображения*.



Примечание. Чтобы использовать этот параметр, необходимо **включить** параметр «*Command Region*» (Командная область).

Clear (Очистить)

Если этот параметр **включен**, мини-контроллер 9160 G2 создает *пустое* поле ввода для поля ввода, заполненного пробелами.

Некоторые приложения на главных устройствах используют видео-атрибуты отображаемых символов для выделения полей, в частности полей ввода. Например, экран приложения может определить все поля ввода с негативным видеоизображением и заполнить это поле пробелами. Эта функция доступна для мобильных компьютеров, поддерживающих негативное видеоизображение. Если компьютер не поддерживает негативное видеоизображение, это поле может стать невидимым, так как оно полностью состоит из пробелов.

По умолчанию все пустые поля ввода, отображаемые на экране мобильного компьютера Psion Teklogix, выделяются с помощью «символа ввода», заданного в конфигурации мобильного компьютера. Функция *Clear (Очистить)* создает пустое поле ввода на месте поля ввода, заполненного пробелами.



Примечание. Эта операция выполняется только на экранах, полученных **от главного устройства**. Данные, передаваемые **на главное устройство**, остаются без изменений.

Passthru (Сквозная пересылка)

Если этот параметр **включен**, устройство 9160 G2 разрешает главному устройству пересылать данные непосредственно на последовательный порт мобильного компьютера с поддержкой радиосвязи. В большинстве случаев эта функция используется для печати.

Подготовка экранов главного устройства к сквозной пересылке

На экране, пересылаемом через последовательный порт мобильного компьютера, в первой строке, начиная со второго столбца, должно находиться слово «PASSTHRU» (заглавными буквами). Фактические данные, передаваемые на мобильный компьютер, могут начинаться с любого места под первой строкой.

При эмуляции 5250 или 3274 атрибуты располагаются в буфере экрана. Атрибут, размещенный между столбцом 2 и окончанием слова «PASSTHRU», смещает все последующие символы на одну позицию вправо. Следовательно, все требуемые атрибуты необходимо размещать в столбце 1 первой строки (непосредственно перед словом «PASSTHRU»).

Пример.

| | | | | | | | | | | | |
|-----------|---|---|---|---|---|---|---|---|---|---|---|
| столбец: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | | |
| строка 1: | @ | P | A | S | S | T | H | R | U | @ | |
| строка 2: | @ | P | A | R | T | : | 1 | 2 | 3 | 4 | 5 |

где @ является атрибутом.

После завершения отправки данных на принтер мобильного компьютера устройство 9160 G2 передает на главное устройство ключ «ENTER». Главное устройство находится в режиме ожидания и не передает остальные экраны (в том числе другие экраны «PASSTHRU») на этот мобильный компьютер до получения ключа «ENTER».



Примечание. Информацию о настройке параметров сквозной передачи на мобильном компьютере можно найти в руководстве пользователя соответствующей модели мобильного компьютера.

Procedures (Инструкции)

Если этот параметр **включен**, главное устройство может передавать инструкции TESS через устройство 9160 G2 на мобильные компьютеры. Инструкция TESS — это группа команд TESS, запускаемых командой TESS *execute procedure*.

Local (Локальные)

Если этот параметр **включен**, устройство 9160 G2 позволяет главному устройству предоставлять страницы для загрузки в виде локальных инструкций TESS на мобильных компьютерах.

Локальные инструкции выбираются в меню на мобильном компьютере. Эти инструкции могут выполняться на мобильных компьютерах, когда они работают в автономном режиме. Когда мобильные компьютеры снова подключаются к сети, результаты выполнения инструкций передаются на главное устройство.



*Примечание. Чтобы использовать параметр Local (Локальные), необходимо **включить** параметр Procedures (Инструкции).*

Host Print (Печать с главного устройства)

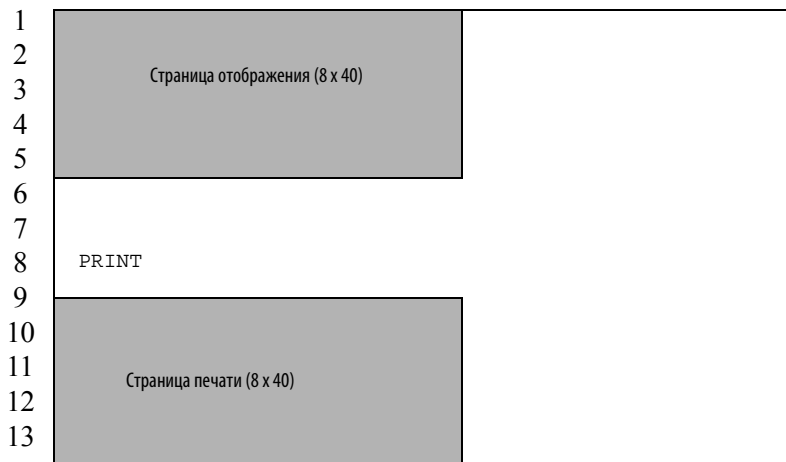
Когда этот параметр **включен**, главное устройство может вывести на экраны мобильных компьютеров дополнительные данные и передать на мобильный компьютер команду на печать этих данных. В этом заключается отличие данной функции от функции *Local Print (Локальная печать)*, при использовании которой запрос на печать инициируется мобильным компьютером.

Текст, пересылаемый на принтер, форматируется по размеру экрана приложения 24 x 80. Если главное устройство может инициировать печать, этот текст будет распечатан. Устройство 9160 G2 распознает дополнительный текст как страницу печати благодаря слову «PRINT», *набранному заглавными буквами* и размещенному в начале 2-го столбца в строке 13 на экране 24 x 80. Слово «PRINT» должно быть определено как текст, *доступный только для отображения*.

Страница печати располагается под страницей отображения мобильного компьютера (см. Рис. 23.5 на стр. 315). Размер страницы печати всегда соответствует размеру страницы отображения мобильного компьютера (при условии, что в конфигурации мобильного компьютера задана длина страницы менее 12 строк).

Если параметр *Host Print (Печать с главного устройства)* **включен**, устройство 9160 G2 передает страницу печати на мобильный компьютер после получения экрана приложения от главного устройства.

Рис. 23.5 Экран приложения со страницей печати



Примечания.

1. В отличие от параметра «Passthru» (Сквозная пересылка), при использовании параметра «Host Print» (Печать с главного устройства) невозможно передавать на принтер управляющие команды.
2. На мобильном компьютере должна быть включена поддержка печати (с помощью команды «Printer» (Принтер) в меню «Features» (Функции) TESS); дополнительные сведения см. в руководстве пользователя соответствующей модели мобильного компьютера.

Remote Print (Удаленная печать)

Когда этот параметр **включен**, устройство 9160 G2 передает страницу печати на мобильный компьютер каждый раз, когда мобильный компьютер отправляет соответствующий запрос. При этом мобильный компьютер передает функциональный ключ «F17» или ключ «PRINT» (в более старых версиях мобильных компьютеров). Устройство 9160 G2 передает результат функции обратно на главное устройство.

В этом заключается отличие данной функции от функции *Host Print (Печать с главного устройства)*, при использовании которой запрос на печать инициируется главным устройством.



Примечание. На мобильном компьютере должна быть включена поддержка печати. Для получения дополнительной информации см. руководство пользователя соответствующей модели мобильного компьютера.

Pages (Страницы)

Этот параметр определяет число экранов (или страниц) главного устройства, сохраняемых на мобильном компьютере (максимальное число – **79**).

Устройство 9160 G2 сокращает объем данных, передаваемых на мобильные компьютеры, используя возможность мобильного компьютера сохранять страницу данных для каждого отображаемого экрана. 9160 G2 сохраняет изображение каждой страницы, хранящейся на мобильном компьютере. После получения экрана приложения устройство 9160 G2 пытается сопоставить этот экран с сохраненной страницей.

Если в памяти мобильного компьютера уже есть похожая страница, 9160 G2 передает на мобильный компьютер команду повторного отображения копии этой страницы; с контроллера передаются только необходимые изменения. Если совпадений не найдено, страница полностью пересылается на мобильный компьютер по радиоканалу.



*Примечание. На мобильном компьютере также предусмотрен соответствующий параметр, и **фактическое** число сохраненных страниц соответствует **меньшему** из значений этих двух параметров.*

Transmit Line (Строка передачи)

Если эта функция **включена**, все измененные на мобильном компьютере данные автоматически передаются, когда оператор вводит данные в поле *transmit-upon-entry*.

Значение в этом текстовом поле определяет строку на экране, которая называется *transmit line (строка передачи)*. Последнее поле ввода, находящееся над строкой передачи или на этой строке, определяется как поле *transmit-upon-entry*. Если в строках ниже строки передачи есть другие поля ввода, ни одно из полей ввода не считается полем *transmit-upon-entry*.

Если в поле указано значение **0** (ноль), функция отключена. Если указано значение **24**, *последнее* поле ввода на каждом экране приложения определяется как поле *transmit-upon-entry*.

AIAG

Этот параметр предоставляет функции автообнаружения и заполнения для входных данных, поступающих от сканеров штрихкодов. При вводе данных штрихкода в мобильный компьютер на текущей странице осуществляется поиск полей «AIAG», которые можно заполнить данными штрихкода. Данные, предварительно подставленные в поле «AIAG» программным приложением, определяют, будут ли приняты данные штрихкода. На мини-контроллере 9160 G2 задается десятичное значение символа ASCII от 0 до 127, соответствующее идентификатору поля AIAG («AIAG Field Identifier»), указанному на главном устройстве. Если указано значение 0, функция отключена.

Предварительно подставляемые данные имеют следующий формат:

`<mode> <AIAG prefix(data)>`

Символ «mode», используемый в сочетании с командой, позволяет включать различные рабочие режимы для определенных операций приложения. Операция автоматического обнаружения и заполнения применяется только к данным, полученным со сканера штрихкодов. Описания режимов и префиксов AIAG приведены в таблице ниже. Эти режимы настраиваются на главном устройстве.

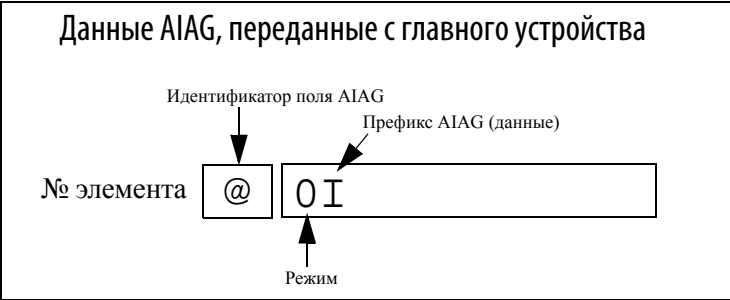
Табл. 23.3 Описание функций режимов и префиксов AIAG

| Режим | Функция |
|--|--|
| 0 | Отобразить префикс, передать префикс на главное устройство. |
| 1 | Не отображать префикс, передать префикс на главное устройство. |
| 2 | Отобразить префикс, не передавать префикс на главное устройство. |
| 3 | Не отображать префикс, не передавать префикс на главное устройство. |
| +4 | Если добавить 4 к вышеперечисленным значениям, данные будут передаваться на главное устройство, когда будут заполнены все поля AIAG с набором 4. Функция 0 применяется «принудительно», если в данном наборе бит есть поля и все они заполнены данными, введенными оператором. |
| +8 | Если добавить 8 к вышеперечисленным значениям, будут перезаписаны все данные, введенные ранее. |
| +16 | Добавление цифры 16 к вышеперечисленным значениям позволяет указать приоритет позиции курсора для поиска и заполнения. |
| AIAG Prefix (data) (Префикс AIAG (данные)) | Текст для поиска соответствий в поле AIAG. |

Пример.

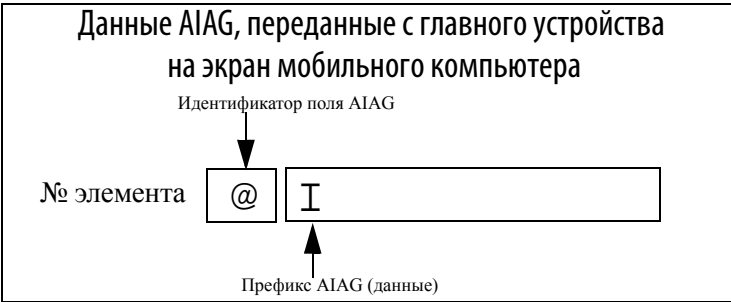
В этом примере показан экран с данными, определенными на главном устройстве и передаваемыми с этого устройства. Данные включают в себя «AIAG Identifier» (Идентификатор AIAG) – тег, определяющий поле AIAG – после которого указан режим, в данном случае «Mode 0» (Режим 0), и «AIAG Prefix» (Префикс AIAG) – I.

Рис. 23.6 Поле AIAG, передаваемое с главного устройства



Когда переданная информация выводится на экран мобильного компьютера, система находит соответствующее поле AIAG для отсканированных данных с помощью идентификатора AIAG. Поскольку на главном устройстве задан режим «Mode 0», префикс AIAG (I) отображается на экране мобильного компьютера, а после заполнения этого экрана отправляется обратно на главное устройство.

Рис. 23.7 Поле AIAG, отправленное на мобильный компьютер



Символ явного совпадения

Если вставить специальный символ ASCII непосредственно перед полем ввода, приложение сможет отличить «поле совпадения» от поля ввода. Допустим, что в качестве символа, определяющего поля явного совпадения, используется угловая скобка «>». Если вставить символ «>» сразу перед полем ввода, оно будет определено как поле совпадения (см. ниже).

Part #> _____

Диапазон значений этого параметра – от **0** до **255** – представляет десятичные значения символов ASCII. Если указано значение **0**, функция отключена. Десятичное значение ASCII, заданное на устройстве 9160 G2, должно совпадать со значением, заданным в приложении.

При использовании функции *Visible Match* (*Явное совпадение*) главный компьютер предварительно подставляет данные в поле ввода совпадения; эти данные выводятся на экран мобильного компьютера. Предварительно загруженные данные, которые передаются на мобильный компьютер, могут состоять из конкретных символов, специальных символов совпадений или сочетаний этих символов. Информация о символах совпадений, распознаваемых мобильными компьютерами Psion Teklogix, приведена в следующей таблице.

Если поле ввода не совпадает с предварительно подставленными данными, данные отображаются на экране, мобильный компьютер подает звуковой сигнал и курсор перемещается на начальную позицию в поле совпадения. Оператор может ввести в поле совпадения другие данные или переместить курсор в другое поле. Когда в поле совпадения вводятся данные (даже если они не совпадают с предварительно загруженными данными), эти данные передаются на главное устройство вместе с другими данными, измененными на мобильном компьютере, во время следующего сеанса передачи.

Табл. 23.4 Символы совпадений

| Символ | Описание |
|--------|---|
| # | Совпадение с числом. |
| & | Совпадение с буквой (в любом регистре). |
| ^ | Совпадение с буквой в верхнем регистре. |
| _ | Совпадение с буквой в нижнем регистре. |

Табл. 23.4 Символы совпадений (Продолжение)

| Символ | Описание |
|--------|---|
| | Совпадение с буквенно-числовым символом. |
| " | Совпадение с буквой, числом или пробелом. |
| ? | Совпадение с символом пунктуации. |
| ' | Совпадение с любым символом. |
| : | Совпадение всех позиций символов в поле с предшествующим символом. |
| ; | Совпадение любых оставшихся символов, но не обязательно остальных символов поля, с предшествующим символом. |

Пример.

Допустим, что в поле ввода необходимо предварительно подставить номер детали. Если вам известен номер детали, вы можете предварительно подставить его в это поле. Если требуется более гибкий подход, при котором номер детали всегда начинается с двух буквенных символов, за которыми следуют дефис и четыре цифры, строка совпадения для данного поля будет иметь следующий вид: **&&-####**.

Символ скрытого совпадения

В отличие от данных в поле «явного совпадения» данные, предварительно подставленные в поле «скрытого совпадения», *не* отображаются на экране мобильного компьютера.



Примечание. Для получения подробных сведений о сопоставлении полей см. раздел «Символ явного совпадения» на стр. 319.

Диапазон значений этого параметра – от **0** до **255** – представляет десятичные значения символов ASCII. Если указано значение **0**, функция отключена. Десятичное значение ASCII, заданное на устройстве 9160 G2, должно совпадать со значением, заданным в приложении.

Serial I/O (Последовательный ввод/вывод)

Поля *Serial I/O (Последовательный ввод/вывод)* представляют собой поля ввода и фиксированные поля, которые заполняются входными и выходными данными, передаваемыми через последовательный порт. Приложение определяет поле как поле *последовательного ввода/вывода*, если этому полю предшествует специальный символ.

Если этот символ предшествует фиксированному полю, данные будут отправлены на последовательный порт мобильного компьютера. Если этот символ предшествует полю ввода, это поле будет заполнено данными, принятыми через последовательный порт мобильного компьютера.

Диапазон значений этого параметра – от **0** до **255** – представляет десятичные значения символов ASCII. Если в поле указано значение **0** (ноль), функция отключена.

Print Line (Строка печати)

Этот параметр позволяет указать начальное число в строке страницы печати на экране приложения (см. также *Entry Line (Строка ввода)*). Если указано значение до **24**, страница отображения будет распечатана; если указано значение **0** (ноль), функция отключена.

Print Form Length (Длина формы печати)

Этот параметр определяет длину формы принтера в строках. Возможные значения: от **0** до **24**.

Barcode (Штрихкод)

Поля *barcode-input-only* представляют собой специальные поля ввода, которые заполняются только данными, полученными от сканера штрихкодов. Приложение определяет поле ввода как поле *barcode-input-only*, если этому полю предшествует специальный символ.

Диапазон значений этого параметра – от **0** до **255** – представляет десятичные значения символов ASCII. Если в поле указано значение **0** (ноль), функция отключена.

Entry Line (Строка ввода)

Этот параметр определяет число первой строки, которая отображается, если в левой верхней части экрана нет полей ввода и если поле ввода находится на этой строке или под ней.

Параметр *Entry Line (Строка ввода)* позволяет автоматически сместить экран главного устройства так, чтобы в области, отображаемой на экране мобильного компьютера, поместилось поле ввода, которое в противном случае находилось бы за пределами этой области. На некоторых мобильных компьютерах Psion Teklogix с небольшим дисплеем отображается только левый верхний угол экрана приложения.

Field Overhead (Дополнительный интервал между полями)

Этот параметр определяет максимально допустимое число символов между двумя *фиксированными* полями, при котором 9160 G2 по-прежнему может объединить эти два поля в одно.

Устройство 9160 G2 иногда объединяет два смежных фиксированных поля в одно и передает их в таком виде. Это позволяет сократить излишние нагрузки на радиоканал.

Например, если два поля находятся на расстоянии 4 символов друг от друга, а в качестве значения параметра выбрано число 5, эти поля будут объединены в одно.

Command Region (Командная область)

Этот параметр определяет область на экране главного устройства, которую устройство 9160 G2 проверяет на наличие зарезервированных команд.

Четыре числа, указанные в текстовых полях раздела *Command Region (Командная область)*, представляют собой адреса строк и столбцов левого верхнего угла и правого нижнего угла командной области. Первое текстовое поле в каждой из этих пар содержит число строки, а второе — число столбца. Возможные значения строк — от **0** до **24**; возможные значения столбцов — от **0** до **80**.

Например, чтобы определить две последних строки на экране главного устройства как командную область, можно ввести значения 23, 1 и 24, 80.

В настоящее время поддерживается только одна команда *ALARM* (подробное описание этой команды см. на стр. 312). Когда на любой позиции в командной области размещается слово «ALARM», устройство 9160 G2 передает на мобильный компьютер команду TESS *beep*, вызывающую звуковой сигнал.

23.4.2.3 Параметры протокола Telnet

| | |
|----------------------------------|-------------------------------------|
| Telnet Protocol Options: | |
| Terminal Type: | IBM-5251-11 ▼ |
| Host Port: | 23 (Range 1..32767) |
| Maximum Sessions per Terminal: | 4 (Range 1..127) |
| First Local Terminal Port: | 10000 (Range 1..32767) |
| Local IP Address to Bind: | 0.0.0.0 |
| First Terminal Listen Port: | 0 (Range 0..32767) |
| Actively Negotiate with Host: | <input type="checkbox"/> |
| Auto-telnet: | DISABLE ▼ |
| Auto-telnet Host: | |
| Auto-telnet without User Action: | <input checked="" type="checkbox"/> |
| Enable Virtual Device Names: | <input type="checkbox"/> |
| - Configure Device Names: | Configure |
| - Device Name Prefix: | |

Terminal Type (Тип терминала)

Этот параметр позволяет выбрать тип мобильного компьютера, который будет эмулироваться устройством 9160 G2 для данного главного устройства. В настоящее время для типа эмуляции *5250 Emulation (Эмуляция 5250)* можно выбрать мобильные компьютеры **IBM 5251-11**, **IBM 5555-B01** и **IBM 3179-2**.

Host Port (Порт главного устройства)

Этот параметр позволяет указать номер порта главного устройства для выбранного подключения *5250 Emulation (Эмуляция 5250)*. По умолчанию используется значение **23**.

Maximum Sessions per Terminal (Максимальное число сеансов на терминал)

Этот параметр определяет максимально допустимое число сеансов Telnet, иницируемых каждым мобильным компьютером. Возможные значения: от **1** до **127**, по умолчанию используется значение **4**.

First Local Terminal Port (Локальный порт первого терминала)

Этот параметр определяет номер локального порта, через который первый мобильный компьютер будет подключаться к исходящим сеансам Telnet. По умолчанию используется значение **10000**.

Local IP Address to Bind (Локальный IP-адрес для привязки)

Этот параметр определяет IP-адрес сетевого адаптера, через который первый мобильный компьютер будет подключаться к исходящим сеансам Telnet.

First Terminal Listen Port (Порт прослушивания первого терминала)

Этот параметр определяет первый номер порта, который будет прослушиваться устройством 9160 G2 на наличие запросов подключения к мобильным компьютерам по протоколу Telnet. Чтобы **включить** этот параметр, необходимо выбрать значение не меньше **1024**. Чтобы **отключить** порт прослушивания, необходимо указать значение **0**.

По умолчанию используется значение **0** (отключено).

Actively Negotiate with Host (Активное согласование с главным устройством)

Если этот параметр включен, устройство 9160 G2 начинает процесс согласования с главным устройством во время установления соединения Telnet. Для большинства главных устройств этот параметр использовать не рекомендуется.

Auto-telnet (Автоматическое подключение Telnet)

Этот параметр позволяет разрешить или запретить автоматическое подключение мобильных компьютеров к данному главному устройству через сеансы Telnet.

Доступные значения: **Disable** (Отключить) и **Auto-telnet** (Автоматическое подключение Telnet). По умолчанию используется значение **Disable** (Отключить).

Когда параметр *Auto-telnet* (*Автоматическое подключение Telnet*) **отключен**, сеансы подключения Telnet к главному устройству необходимо инициировать вручную на мобильных компьютерах.

Когда параметр *Auto-telnet* (*Автоматическое подключение Telnet*) **включен**, устройство 9160 G2 инициирует один сеанс Telnet на каждом мобильном компьютере, номер терминала которого соответствует данному главному устройству. На каждом мобильном компьютере можно инициировать дополнительные сеансы Telnet для подключения к главному устройству, но это необходимо делать вручную.

Когда параметр *Auto-telnet* (Автоматическое подключение Telnet) **включен**, устройство 9160 G2 автоматически устанавливает соединение Telnet с главным устройством, как при запуске, так и при завершении сеанса.



Примечание. Сеансы автоматического подключения Telnet иницируются только для мобильных компьютеров, которые находятся «в сети» (включены и корректно функционируют в радиосети Psion Teklogix).

Auto-telnet Host (Главное устройство для автоматического подключения Telnet)

Этот параметр определяет имя или IP-адрес главного устройства, с которым устройство 9160 G2 соединяет автоматические сеансы Telnet.



Примечание. Имя компьютера, указанное в этом текстовом поле, должно иметь формат, распознаваемый устройством 9160 G2: 9160 G2 должно иметь возможность получить IP-адрес для этого имени. Например, здесь можно указать имя, соответствующее записи в таблице главных устройств 9160 G2, или 9160 G2 может отправить запрос на сервер доменных имен. В качестве имени главного устройства можно указать любое имя, которое можно использовать в команде TCP> на мобильном компьютере.

Auto-telnet Without User Action (Автоматическое подключение Telnet без участия пользователя)

Если этот параметр включен, контроллер немедленно открывает подключение к главному устройству для каждого инициализированного мобильного компьютера без нажатия на клавишу [ENTER].

Enable Virtual Device Names (Разрешить имена виртуальных устройств)

Если этот параметр включен, устройство 9160 G2 осуществляет согласование с главным устройством для получения имени виртуального устройства, используемого в подключении Telnet.

Configure Device Names (Настройка имен устройств)

Telnet Terminal Naming

To remove an LU Name, click the "Remove" button. Ensure that you have selected at least one terminal. See the Help panel for more information.

| <input type="checkbox"/> Edit | Terminal Number | LU Name |
|---------------------------------|-----------------|---------|
| <input type="checkbox"/> [Edit] | 1 | ABC |
| <input type="checkbox"/> [Edit] | 5 | THING |

Selected Terminals:

Add a Terminal...

To associate an LU Name with a Terminal, fill in the fields below and click "Add Name".

Terminal Number:

LU Name:

Для каждого настроенного мобильного компьютера требуется одно имя LU («LU Name»). На этом экране можно назначить имена LU (см. также *Device Name Prefix (Префикс имени устройства)* далее в этом разделе). Имя LU должно быть уникальным и должно быть связано с номером терминала («Terminal Number»), присвоенным мобильному компьютеру. Имя LU может состоять максимум из 10 буквенно-числовых символов. Символы нижнего регистра при вводе автоматически преобразуются в символы верхнего регистра.

Device Name Prefix (Префикс имени устройства)

Если мобильному компьютеру не присвоено имя LU, устройство 9160 G2 создает полное имя LU, добавляя к префиксу LU («LU Prefix») номер терминала («Terminal Number») (пять цифр, при необходимости в начале можно ввести нули).

23.4.2.4 Параметры функциональных клавиш

Function Key Mappings:

| | | | | | |
|------|-----|------|-------|------|----------|
| F1: | F1 | F14: | F14 | F27: | F17 |
| F2: | F2 | F15: | F15 | F28: | F18 |
| F3: | F3 | F16: | CLEAR | F29: | UP |
| F4: | F4 | F17: | PRINT | F30: | SESS |
| F5: | F5 | F18: | HELP | F31: | ENTER |
| F6: | F6 | F19: | F19 | F32: | ENTER |
| F7: | F7 | F20: | F20 | F33: | ENTER |
| F8: | F8 | F21: | F21 | F34: | ENTER |
| F9: | F9 | F22: | F22 | F35: | ENTER |
| F10: | F10 | F23: | F23 | F36: | ENTER |
| F11: | F11 | F24: | F24 | F37: | ENTER |
| F12: | F12 | F25: | DOWN | F38: | SELECTOR |
| F13: | F13 | F26: | F16 | F39: | ENTER |

Функциональная клавиша n

Параметр *Function Key* (Функциональная клавиша) позволяет выбрать код, который будет передан на главное устройство при нажатии функциональной клавиши на мобильном компьютере. Для каждой функциональной клавиши можно выбрать вариант из одного и того же списка доступных кодов. Однако по умолчанию всем функциональным клавишам назначены разные коды. Значения по умолчанию представлены на этой странице.

23.4.3 Эмуляция ANSI

23.4.3.1 Параметры эмуляции

ANSI Emulation Options:

Maximum Screen Size:

24

 rows

80

 columns

Host Timeout:

15

 (Range 0..255)

Escape Timeout:

12

 (Range 0..255)

Threshold:

200

 (Range 0..999)

Echo:

☒

Function Key Remapping:

☐

Arrow Key Remapping:

☐

Page Saving:

☒

Page Saving consider Double Byte Characters:

☐

RLE:

☐

Convert 7 to 8 bits:

☐

Lower Character Set (GL):

ASCII

▼

Upper Character Set (GR):

ASCII

▼

Terminal Initialization Data:

Host Initialization Data:

Maximum Screen Size (Максимальный размер экрана)

Параметр *Maximum Screen Size* (Максимальный размер экрана) позволяет задать максимальный требуемый размер экрана на мобильных компьютерах, измеряемый в строках и столбцах. Эта функция позволяет более эффективно использовать ресурсы памяти при использовании функции сохранения страниц (см. раздел «Page Saving (Сохранение страниц)» на стр. 330).

Минимальный размер — **24 x 80**, максимальный — **60 x 132**. По умолчанию используется значение **24 x 80**.

Host Timeout (Таймаут главного устройства)

Параметр *Host Timeout* (*Таймаут главного устройства*) определяет интервал (в *терциях*, или шестидесятых долях секунды) между пакетами данных, поступающих от главного устройства. Возможные значения: от **0** до **255**, по умолчанию используется значение **15**.

Если по истечении заданного таймаута устройство 9160 G2 не получает от главного устройства ни одного символа, считается, что главное устройство завершило отправку данных и ожидает ввода данных на стороне пользователя (другими словами, предполагается, что экран данных заполнен).



Важно! Чтобы изменить значение параметра «Host Timeout» (Таймаут главного устройства), необходимо включить параметр «Page Saving» (Сохранение страниц) (см. стр. 330).

Escape Timeout (Таймаут управляющей последовательности)

Параметр *Escape Timeout* (Таймаут управляющей последовательности) определяет промежуток времени (в *терциях*, или шестидесятых долях секунды), в течение которого устройство 9160 G2 удерживает команду «ESC», полученную от главного устройства, и считает следующий полученный байт частью управляющей последовательности. Возможные значения: от 0 до 255, по умолчанию используется значение 12.

По истечении указанного таймаута главному устройству потребуется отправить еще один символ «ESC», чтобы начать управляющую последовательность.



Примечание. Это особенно важно, когда символ ESC находится в конце пакета данных.

Threshold (Порог)

Параметр *Threshold* (Порог) определяет минимальное число байт данных обновления для экрана мобильного компьютера, которые должны быть получены от главного устройства до того, как устройство 9160 G2 создаст копию экрана, сохранив его как новую страницу. Возможные значения: от 0 до 999, по умолчанию используется значение 200.



Важно! Чтобы изменить значение параметра «Threshold» (Порог), необходимо включить параметр «Page Saving» (Сохранение страниц) (см. стр. 330).

Echo (Эхо)

Если этот параметр **включен**, устройство 9160 G2 использует режим «Smart» Echo. Этот режим сокращает объем данных, пересылаемых на мобильный компьютер, путем уменьшения числа сеансов радиопередачи.

В обычном случае, когда используется режим символов, каждое нажатие клавиши передается на главное устройство за один сеанс передачи, а в другом сеансе передачи главное устройство использует эхо этого символа. Если режим «Smart» Echo **включен**, устройство 9160 G2 не будет передавать эхо главного устройства на мобильные компьютеры, если оно совпадает с данными, отправленными с мобильного компьютера. Таким образом, число сеансов радиопередачи сокращается.

Этот режим также сокращает или устраняет задержку между вводом символа с клавиатуры и отображением символа, переданного эхом с главного устройства. Максимальное число символов, ожидающих эха, составляет **25**. Любые дополнительные символы будут переданы на главное устройство, но не будут выведены на экран.



Примечания.

1. Также этот параметр регулирует возможность отправки запроса параметра ANSI на мобильный компьютер.
2. Режим «Smart» Echo также необходимо включить на мобильном компьютере (см. руководство пользователя соответствующей модели мобильного компьютера).

Function Key Remapping (Переназначение функциональных клавиш)

Если этот параметр **включен**, устройство 9160 G2 перенастроит параметры функциональных клавиш, заданные на экране «Function Key Remapping» (Переназначение функциональных клавиш) (см. стр. 340), для текущего сеанса подключения к главному устройству.

Arrow Key Remapping (Переназначение клавиш со стрелками)

Если этот параметр **включен**, устройство 9160 G2 перенастроит параметры клавиш со стрелками, заданные на экране «Function Key Remapping» (Переназначение функциональных клавиш) (см. стр. 340), для текущего сеанса подключения к главному устройству.

Page Saving (Сохранение страниц)

Если этот параметр **включен**, устройство 9160 G2 будет использовать функцию сохранения страниц, которая позволяет сократить объем данных, передаваемых на мобильные компьютеры.

9160 G2 сохраняет изображение каждой страницы, хранящейся на мобильном компьютере. После получения экрана приложения устройство 9160 G2 пытается сопоставить этот экран с сохраненной страницей. Если такая страница уже существует на мобильном компьютере, устройство 9160 G2 передает на мобильный компьютер команду повторного отображения сохраненной копии страницы; это позволяет избежать повторной передачи данных этой страницы по радиоканалу. Если устройство 9160 G2 не обнаружит совпадения для страницы, она будет передана на мобильный компьютер полностью. По умолчанию этот параметр **включен**.



***Примечания.** Когда параметр сохранения страниц включен, на мобильном компьютере можно задать число сохраняемых страниц. Подробную информацию см. в руководстве пользователя соответствующей модели мобильного компьютера.*

При использовании двухбайтовых наборов символов, таких как китайские или корейские иероглифы, рекомендуется настроить параметр «Page Saving Consider Double Byte Character» (Сохранение страниц с учетом двухбайтовых символов).

Page Saving Consider Double Byte Character (Сохранение страниц с учетом двухбайтовых символов)

При использовании двухбайтовых наборов символов, таких как китайские или корейские иероглифы, вышеописанная функция *Page Saving (Сохранение страниц)* позволяет частично перезаписывать двухбайтовые символы, что может привести к появлению отдельных непечатаемых экранных данных или новых случайных символов, составленных из двух частей различных символов. Кроме того, мобильный компьютер может изменить расположение данных на экране с целью усечения поврежденных данных.

Когда параметр *Page Saving Consider Double Byte Character (Сохранение страниц с учетом двухбайтовых символов)* **включен**, функция *Page Saving (Сохранение страниц)* заменяет все разрозненные части двухбайтовых символов на пробелы, предотвращая отображение измененных символов и усеченных данных на экране мобильного компьютера. По умолчанию этот параметр **отключен**.



***Примечание.** Этот параметр следует использовать только при работе с двухбайтовыми наборами символов.*

RLE

Если этот параметр **включен**, устройство 9160 G2 применяет к данным, передаваемым по радиоканалу, кодирование по длине серий (RLE). Кодирование *RLE* приводит к сжатию повторяющихся символов, передаваемых с главного устройства на мобильный компьютер. Если в потоке данных обнаруживаются повторяющиеся символы, то сначала пересылается первый из этих символов, а затем передается короткая управляющая последовательность (3 или 4 символа), по которой мобильный компьютер определяет, сколько раз необходимо повторить этот символ. Таким образом кодирование RLE обеспечивает сжатие данных и уменьшает общий объем трафика на радиоканале.

Convert 7 to 8 Bits (Преобразование 7 бит в 8 бит)

Если этот параметр **включен**, устройство 9160 G2 преобразует 7-битные управляющие последовательности в 8-битные эквиваленты в потоках данных ANSI, передаваемых на мобильные компьютеры. При этом двухсимвольные управляющие последовательности заменяются на эквивалентные односимвольные, что обеспечивает сжатие данных.

Lower Character Set (GL) (Набор символов нижнего регистра)

Здесь необходимо выбрать тот же набор символов, что и на мобильном компьютере. Этот параметр используется, только если включена функция сохранения страниц.

Upper Character Set (GR) (Набор символов верхнего регистра)

Здесь необходимо выбрать тот же набор символов, что и на мобильном компьютере. Этот параметр используется, только если включена функция сохранения страниц.

Terminal Initialization Data/Host Initialization Data (Данные инициализации терминала/Данные инициализации главного устройства)

Введенные в этих полях данные будут передаваться с контроллера на мобильный компьютер или с контроллера на главное устройство при каждой перезагрузке мобильного компьютера. Например, эти данные можно использовать для отправки запроса на обновление главного устройства или для сброса наборов символов, заданных в параметрах мобильного компьютера главным устройством при входе в систему.

Непечатаемые данные можно вводить либо в шестнадцатеричном формате \xnn, либо в восьмеричном формате \nnn. Например, символ «ескаре» можно представить в формате \x1b или \033.

Длина значений этих параметров не должна превышать 256 символов. Если оставить эти поля пустыми, не будут передаваться никакие данные.

23.4.3.2 Параметры протокола Telnet

| Telnet Protocol Options: | |
|--|---|
| Terminal Type: | <input type="text" value="VT100"/> |
| Host Port: | <input type="text" value="23"/> (Range 1..32767) |
| Maximum Sessions per Terminal: | <input type="text" value="4"/> (Range 1..127) |
| Close Host sessions on Terminal reset: | <input type="checkbox"/> |
| First Local Terminal Port: | <input type="text" value="10000"/> (Range 1..32767) |
| Local IP Address to Bind: | <input type="text" value="0.0.0.0"/> |
| First Terminal Listen Port: | <input type="text" value="0"/> (Range 0..32767) |
| TCP Session Request Key: | <input type="text" value="1"/> (Range 0..255) |
| Session Cycle Key: | <input type="text" value="2"/> (Range 0..255) |
| Last Active Session Key: | <input type="text" value="5"/> (Range 0..255) |

Terminal Type (Тип терминала)

Этот параметр позволяет указать тип мобильного компьютера, который будет эмулироваться устройством 9160 G2. В этом текстовом поле можно ввести строку ASCII длиной **не более 32** символов, распознаваемую главным устройством. По умолчанию используется значение **VT100**.

Host Port (Порт главного устройства)

Этот параметр определяет номер порта главного устройства для выбранного подключения к главному устройству ANSI. По умолчанию используется значение **23**.

Maximum Sessions per Terminal (Максимальное число сеансов на терминал)

Этот параметр определяет максимально допустимое число сеансов Telnet, иницируемых каждым мобильным компьютером. Возможные значения: от **1** до **127**, по умолчанию используется значение **4**.

Close Host Sessions on Terminal Reset (Закрывать сеансы связи с главным устройством при перезагрузке терминала)

Когда этот параметр **включен**, при получении сообщения о перезагрузке терминала сеанс связи с главным устройством для этого номера терминала будет закрыт. По умолчанию этот параметр **отключен**.

First Local Terminal Port (Локальный порт первого терминала)

Этот параметр определяет номер порта, на котором устройство 9160 G2 будет пытаться установить подключение Telnet для первого мобильного компьютера. По умолчанию используется значение **10000**. Дополнительным сеансам Telnet присваиваются более высокие значения портов.

Local IP Address to Bind (Локальный IP-адрес для привязки)

Этот параметр определяет IP-адрес интерфейса 9160 G2, устанавливающего подключение к главному устройству. Этот адрес используется наряду с номерами локальных портов для создания уникальных сокетов для каждого терминального сеанса.

First Terminal Listen Port (Порт прослушивания первого терминала)

Этот параметр определяет первый номер порта, который будет прослушиваться устройством 9160 G2 на наличие запросов подключения к мобильным компьютерам по протоколу Telnet. Чтобы **включить** этот параметр, необходимо выбрать значение не меньше **1024**. Чтобы **отключить** порт прослушивания, необходимо указать значение **0**.

По умолчанию используется значение **0** (отключено).

TCP Session Request Key (Ключ запроса на сеанс TCP)

Этот параметр определяет десятичный символ кодировки ASCII, который будет инициировать отправку запроса на новый терминальный сеанс ANSI с мобильного компьютера. Возможные значения: от **0** до **255**, по умолчанию используется значение **1**.

Session Cycle Key (Ключ цикла сеанса)

Этот параметр определяет десятичный символ кодировки ASCII, который будет инициировать отображение следующего терминального сеанса ANSI на мобильном компьютере. Возможные значения: от **0** до **255**, по умолчанию используется значение **2**.

Last Active Session Key (Последний активный ключ сеанса)

Этот параметр определяет десятичный символ кодировки ASCII, который будет инициировать отображение последнего терминального сеанса ANSI на мобильном компьютере. Возможные значения: от 0 до 255, по умолчанию используется значение 5.

23.4.3.3 Auto-Telnet/Auto-login (Автоматическое подключение Telnet/Автоматический вход)

| | |
|---|-------------------------------------|
| Auto-Telnet / Auto-Login: | |
| Auto-telnet/login Enable: | DISABLE ▾ |
| Auto-telnet Host: | <input type="text"/> |
| Auto-telnet Terminal Prompt: | Press ENTER to login. |
| Auto-login User ID: | <input type="text"/> |
| Auto-login Password: | <input type="password"/> |
| Auto-login User ID prompt: | gin: <input type="text"/> |
| Auto-login Password prompt: | word: <input type="password"/> |
| Auto-login failed login: | incorrect |
| Auto-telnet without User Action: | <input type="checkbox"/> |
| Auto-telnet without User Action Timing Delay: | 25 (Range 0..255) |
| Maximum of Auto-telnet Retries: | 0 (Range 0..255) |
| Allow TCP Sessions: | <input checked="" type="checkbox"/> |

Auto-telnet/login Enable (Разрешить автоматическое подключение Telnet/автоматический вход)

Этот параметр позволяет разрешить или запретить автоматическое подключение мобильных компьютеров к данному главному устройству через сеансы Telnet. Доступные значения: **DISABLE** (ОТКЛЮЧИТЬ); **AUTO-TELNET** (АВТОМАТИЧЕСКОЕ ПОДКЛЮЧЕНИЕ TELNET); **AUTO-TELNET/LOGIN** (АВТОМАТИЧЕСКОЕ ПОДКЛЮЧЕНИЕ TELNET/АВТОМАТИЧЕСКИЙ ВХОД). По умолчанию используется значение **DISABLE** (ОТКЛЮЧИТЬ).

Когда параметр *Auto-telnet* (Автоматическое подключение Telnet) **отключен**, сеансы подключения Telnet к главному устройству необходимо инициировать вручную на мобильных компьютерах.

Когда параметр *Auto-telnet* (Автоматическое подключение Telnet) **включен**, устройство 9160 G2 инициирует один сеанс Telnet на каждом мобильном компьютере, номер терминала которого соответствует данному главному устройству. На каждом мобильном компьютере можно инициировать дополнительные сеансы Telnet для подключения к главному устройству, но это необходимо делать вручную.



Примечание. Сеансы автоматического подключения Telnet инициируются только для мобильных компьютеров, которые находятся «в сети» (включены и корректно функционируют в радиосети Psion Teklogix).

Когда параметры *Auto-telnet* (Автоматическое подключение Telnet) и *Auto-login* (Автоматический вход) **включены**, устройство 9160 G2 инициирует один сеанс Telnet на каждом мобильном компьютере, номер терминала которого соответствует данному главному устройству. Затем устройство регистрирует каждый сеанс на главном устройстве с помощью идентификатора пользователя и пароля, заданных на этом экране.



Примечание. Для всех сеансов автоматического подключения Telnet, зарегистрированных на данном главном устройстве, используется один и тот же идентификатор пользователя и пароль.

Auto-telnet Host (Главное устройство для автоматического подключения Telnet)

Этот параметр определяет имя или IP-адрес главного устройства, с которым устройство 9160 G2 соединяет автоматические сеансы Telnet.



Примечание. Имя компьютера, указанное в этом текстовом поле, должно иметь формат, распознаваемый устройством 9160 G2: 9160 G2 должно иметь возможность получить IP-адрес для этого имени. Например, здесь можно указать имя, соответствующее записи в таблице главных устройств 9160 G2, или 9160 G2 может отправить запрос на сервер доменных имен.

В качестве имени главного устройства можно указать любое имя, которое можно использовать в команде TCP> на мобильном компьютере.

Auto-telnet Terminal Prompt (Терминальный запрос на автоподключение Telnet)

В этом поле можно ввести текст, который будет отображаться на экране входа в систему. Здесь можно ввести любую строку символов ASCII или числовую управляющую последовательность в восьмеричном или шестнадцатеричном формате.

Восьмеричная управляющая последовательность может иметь следующий вид: \0d, \Odd или \Oddd, где вместо каждого символа «d» можно подставить любую цифру от 0 до 7. Если число «ddd» больше десятичного числа 256, в качестве кодового значения символа будет использоваться остаток десятичного числа «ddd/256».

Шестнадцатеричная управляющая последовательность может иметь следующий вид: \xh или xhh, где вместо каждого символа «h» можно подставить любую цифру от 0 до 9 либо любое буквенное значение a-f или A-F.



Примечание. \0 считается символом с кодовым значением 0.

Максимально допустимая длина строки составляет 60 символов. По умолчанию текст отсутствует, и для входа в систему достаточно просто нажать клавишу <ENTER>.

Auto-login User ID (Идентификатор пользователя для автоматического входа)

Этот параметр определяет идентификатор пользователя, который передается устройством 9160 G2 на главное устройство при регистрации сеансов автоматического входа. В этом текстовом поле можно ввести строку ASCII длиной **не более 32** символов, распознаваемую главным устройством.

Auto-login Password (Пароль для автоматического входа в систему)

Этот параметр определяет пароль, который передается устройством 9160 G2 на главное устройство при регистрации сеансов автоматического входа. В этом текстовом поле можно ввести строку ASCII длиной **не более 32** символов, распознаваемую главным устройством.

Auto-login User ID Prompt (Запрос идентификатора пользователя для автоматического входа)

Устройство 9160 G2 сравнивает текст, введенный в это поле, с текстом, полученным от главного устройства. Если эти данные совпадают, устройство 9160 G2 определяет запрос имени пользователя, отправленный главным устройством, и передает на главное устройство идентификатор пользователя, заданный в настройке *Auto-Login User ID (Идентификатор пользователя для автоматического входа)*. В этом текстовом поле можно ввести строку ASCII длиной **не более 32** символов. По умолчанию используется текст **gin:**



Примечание. Длина совпадающей строки должна быть как можно меньше, но ее должно быть достаточно для того, чтобы эта строка могла служить уникальным запросом на идентификатор пользователя. Не следует указывать составные слова, разделенные пробелами, так как некоторые главные устройства передают другие символы для отображения пробелов на экране.

Auto-login Password Prompt (Запрос пароля для автоматического входа)

Устройство 9160 G2 сравнивает текст, введенный в это поле, с текстом, полученным от главного устройства. Если эти данные совпадают, устройство 9160 G2 определяет запрос пароля, отправленный главным устройством, и передает на главное устройство пароль, заданный в настройке *Auto-Login Password* (*Пароль для автоматического входа*). В этом текстовом поле можно ввести строку ASCII длиной **не более 32** символов. По умолчанию используется текст **word**:



Примечание. Длина совпадающей строки должна быть как можно меньше, но ее должно быть достаточно для того, чтобы эта строка могла служить уникальным запросом на пароль. Не следует указывать составные слова, разделенные пробелами, так как некоторые главные устройства передают другие символы для отображения пробелов на экране.

Auto-login Failed Login (Неуспешный автоматический вход)

Устройство 9160 G2 сравнивает текст, введенный в это поле, с текстом, полученным от главного устройства. Если эти данные совпадают, устройство 9160 G2 определяет передачу с главного устройства строковых данных, информирующих мобильный компьютер о неуспешной попытке входа. Устройство 9160 G2 выводит запрос *Auto-telnet Terminal Prompt* (*Терминальный запрос на автоподключение Telnet*) на экране мобильного компьютера, чтобы пользователь выполнил вход вручную. В этом текстовом поле можно ввести строку ASCII длиной **не более 32** символов. По умолчанию используется текст **incorrect**.



Примечание. Длина совпадающей строки должна быть как можно меньше, но ее должно быть достаточно для того, чтобы эта строка могла служить уникальным запросом неуспешной попытки входа. Не следует указывать составные слова, разделенные пробелами, так как некоторые главные устройства передают другие символы для отображения пробелов на экране.

Auto-telnet Without User Action (Автоматическое подключение Telnet без участия пользователя)

Если этот параметр включен, контроллер немедленно открывает подключение к главному устройству для каждого инициализированного мобильного компьютера без нажатия на клавишу [ENTER]. Если этот параметр включен, рекомендуется изменить значение параметра *Auto Telnet Terminal Prompt* (Терминальный запрос на автоматическое подключение Telnet), чтобы на экране отображалась рекомендация дождаться установки соединения.

Auto-telnet Without User Action Timing Delay (Автоматическое подключение Telnet без участия пользователя с задержкой по времени)

Когда включен этот параметр, при выполнении команды *Auto-telnet Without User Action* (Автоматическое подключение Telnet без участия пользователя) между попытками подключения будет применяться задержка по времени (в миллисекундах).

Maximum Of Auto-telnet Retries (Максимальное число повторных попыток автоматического подключения Telnet)

Число попыток автоматического подключения, совершаемых до установленного предела.

Allow TCP Sessions (Разрешить сеансы TCP)

Когда этот параметр **включен**, устройство 9160 G2 позволяет пользователю мобильного компьютера переключаться между запросами или сеансами, находясь на экране запроса (автоматического входа или сеанса TCP). Если параметр *Allow TCP Sessions* (Разрешить сеансы TCP) **отключен**, все новые сеансы будут открываться как сеансы автоматического входа.

Запрос сеансов (который, как правило, отправляется при нажатии <CTRL> a на мобильном компьютере) может использоваться на уровне экранов запроса для изменения типа запроса (если доступно несколько типов).

Также поддерживается возможность переключения сеансов на уровне экранов запроса (на мобильном компьютере для этого необходимо нажать <CTRL> b [следующий сеанс] или <CTRL> e [последний сеанс]). При переключении между сеансами на экране запроса состояние мобильного компьютера (вход не выполнен) будет меняться в соответствии с сеансом, на который переключается пользователь.

По умолчанию этот параметр **включен**.

23.4.3.4 Параметры функциональных клавиш

Function Key Mappings:

| | | |
|-------------------------------|-------------------------------|--------------------------------|
| F1: 1b,4f,50,00,00,00,00,00 | F11: 1b,5b,32,33,7e,00,00,00 | F21: 1b,5b,31,7e,00,00,00,00 |
| F2: 1b,4f,51,00,00,00,00,00 | F12: 1b,5b,32,34,7e,00,00,00 | F22: 1b,5b,32,7e,00,00,00,00 |
| F3: 1b,4f,52,00,00,00,00,00 | F13: 1b,5b,32,35,7e,00,00,00 | F23: 1b,5b,33,7e,00,00,00,00 |
| F4: 1b,4f,53,00,00,00,00,00 | F14: 1b,5b,32,36,7e,00,00,00 | F24: 1b,5b,34,7e,00,00,00,00 |
| F5: 1b,5b,31,36,7e,00,00,00 | F15: 1b,5b,32,38,7e,00,00,00 | F25: 1b,5b,35,7e,00,00,00,00 |
| F6: 1b,5b,31,37,7e,00,00,00 | F16: 1b,5b,32,39,7e,00,00,00 | F26: 1b,5b,36,7e,00,00,00,00 |
| F7: 1b,5b,31,38,7e,00,00,00 | F17: 1b,5b,33,31,7e,00,00,00 | F27: 1b,5b,34,31,7e,00,00,00 |
| F8: 1b,5b,31,39,7e,00,00,00 | F18: 1b,5b,33,32,7e,00,00,00 | F28: 1b,5b,34,32,7e,00,00,00 |
| F9: 1b,5b,32,30,7e,00,00,00 | F19: 1b,5b,33,33,7e,00,00,00 | F29: 1b,5b,34,33,7e,00,00,00 |
| F10: 1b,5b,32,31,7e,00,00,00 | F20: 1b,5b,33,34,7e,00,00,00 | F30: 1b,5b,34,34,7e,00,00,00 |
| Up: 1b,5b,41,00,00,00,00,00 | Down: 1b,5b,42,00,00,00,00,00 | Right: 1b,5b,43,00,00,00,00,00 |
| Left: 1b,5b,44,00,00,00,00,00 | | |

Функциональная клавиша n

Параметр *Function Key* (Функциональная клавиша) позволяет выбрать код, который будет передан на главное устройство при нажатии функциональной клавиши на мобильном компьютере. Для каждой функциональной клавиши можно выбрать вариант из одного и того же списка доступных кодов. Однако по умолчанию всем функциональным клавишам назначены разные коды. Значения по умолчанию показаны на экране выше.

| | | |
|--------|---|-----|
| 24.1 | Функции 802.IQ | 343 |
| 24.1.1 | Общие функции протоколов 802.IQ v1/v2 | 343 |
| 24.1.2 | Функции 802.IQ v1 | 346 |
| 24.1.3 | Меню функций 802.IQ v2 | 347 |
| 24.2 | Обновление параметров 802.IQ | 347 |

24.1 Функции 802.IQ

802.IQ — это частный протокол Psion Teklogix стандарта 802.11, позволяющий мобильным компьютерам работать в беспроводной сети, поддерживающей одновременное использование протоколов TCP/IP и 802.IQ. Доступны две версии протокола 802.IQ: 802.IQ v1 и 802.IQ v2. Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает одновременное использование обеих версий протокола (мобильные компьютеры должны использовать только одну версию).

Протокол 802.IQ v1 представляет собой схему маршрутизации беспроводной сети, обеспечивающей большую производительность беспроводной сети 802.11 по сравнению с маршрутизацией через TCP/IP. Мобильный компьютер может взаимодействовать с точкой доступа 9160 G2 по протоколу TCP/IP или 802.IQ v1, реализуя систему с двойной функциональностью. Для получения дополнительной информации и ознакомления с меню настройки протокола 802.IQv1 см. стр. 346.

Протокол 802.IQ v2 является расширенной версией протокола 802.IQ v1, обеспечивающей передачу пакетов на уровне UDP. Он поддерживает все возможности протокола 802.IQ v1, функции обновления программного обеспечения по радиоканалу, возможность добавления сторонних точек доступа между контроллерами и мобильными компьютерами, а также интеграцию в систему MapRF (при необходимости). Информацию о настройке мини-контроллера 802.IQ v2 см. на стр. 347.

24.1.1 Общие функции протоколов 802.IQ v1/v2



Важно! Протокол 802.IQ следует использовать только на проводных устройствах 9160 G2.

Не следует настраивать протокол 802.IQ в проводных сетях 9160 G2, соединенных мостами, так как в этом случае маячки 802.IQ будут передаваться по соединению WDS из одной сети в другую (см. Гл. 20: «Распределенная беспроводная система»).

Auto-Startup (Автозапуск)

Этот параметр **включает** протокол 802.IQ сразу после перезагрузки устройства 9160 G2. Если устройство 9160 G2 используется в качестве базовой станции под управлением сетевого контроллера или мини-контроллера 9160 G2, этот параметр необходимо **отключить**.

По умолчанию этот параметр **отключен**.



Важно! Неправильная настройка параметра Auto Startup (Автозапуск) может привести к некорректной работе мобильных компьютеров.

Beacon Period (Интервал маячка)

Маячок 802.IQ — это широковещательный сигнал, передаваемый на все мобильные компьютеры с поддержкой протокола 802.IQ. С помощью этого маячка мобильные компьютеры определяют переключение между базовыми станциями. Также этот сигнал сообщает мобильному компьютеру о перезагрузке базовой станции или контроллера и содержит инструкции по восстановлению соединения в случае перезагрузки. Если контроллер был перезагружен, мобильный компьютер завершает все сеансы и выполняет полную повторную инициализацию. Если базовая станция была перезагружена или мобильный компьютер переключился на другую точку доступа 9160 G2, выполняется «горячая» инициализация (без потери данных).

Для параметра *Beacon Period* (Интервал маячка) можно выбрать значение от **1** до **20** секунд. По умолчанию используется значение **2**.

Terminal Offline Timeout (Таймаут уведомления об отключении терминального сеанса)

Этот параметр позволяет задать отсрочку (в минутах) перед тем, как процесс 802.IQ на устройстве 9160 G2 отправит сотовому контроллеру уведомление об отключении мобильного компьютера от сети.

Возможные значения: от **1** до **240**. По умолчанию используется значение **5**.

Рис. 24.1 Обзор параметров настройки 802.IQ

| | |
|---------------------------|--|
| Basic Settings | Modify 802.IQ settings |
| User Management | |
| Cluster | 802.IQ v1/v2 Common Features: |
| Access Points | Auto-Startup: <input type="checkbox"/> |
| Sessions | Beacon Period: <input type="text" value="2"/> (Range 1..20) |
| Channel Management | Terminal Offline Timeout: <input type="text" value="5"/> (Range 1..240) |
| Wireless Neighborhood | |
| Security | 802.IQ v1 Features: |
| Status | Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Interfaces | Initial RTT: <input type="text" value="1000"/> (Range 10..10000) |
| Events | Protocol Type ID: <input type="text" value="2457"/> (Range 1501..65535) |
| Transmit/Receive | Forward 802.IQ packets only: <input type="checkbox"/> |
| Client Associations | 802.IQ v1 Beacon Interfaces: |
| Neighboring Access Points | Wired: <input type="checkbox"/> |
| | WLAN0: <input type="checkbox"/> |
| | WLAN1: <input type="checkbox"/> |
| | WDS0: <input type="checkbox"/> |
| | WDS1: <input type="checkbox"/> |
| | WDS2: <input type="checkbox"/> |
| | WDS3: <input type="checkbox"/> |
| Manage | |
| Ethernet Settings | 802.IQ v2 Features: |
| 802.11 Settings | Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| 802.11 Advanced Settings | Beacon UDP port: <input type="text" value="8888"/> (Range 5001..65535) |
| VWN | <input type="button" value="Update"/> |
| WDS | |
| Guest Login | |
| MAC Filtering | |
| Load Balancing | |
| Services | |
| QoS | |
| Time | |
| SNMP | |
| Narrow Band | |
| Radio | |
| Connectivity Options | |
| Connectivity | |
| Base Station | |
| RRM Groups | |
| Radio Link Features | |
| Hosts | |
| 802.IQ | |

24.1.2 Функции 802.IQ v1

Доступ к меню *802.IQ v1 Features (Функции 802.IQ v1)* выполняется на вкладке *802.IQ* в разделе *Connectivity (Подключения)* (см. Рис. 24.1 на стр. 345).

Enabled (Включено)

Этот параметр позволяет включить или отключить функцию 802.IQ v1. По умолчанию этот параметр **отключен**.

Initial RTT (Исходное время RTT)

Параметр *Initial RTT (Исходное время RTT)* позволяет указать время (в миллисекундах), которое должно пройти между передачей сигнала от *точки доступа* и *подтверждением приема сигнала на терминале* (время кругового обращения сигнала). Точка доступа постоянно корректирует время кругового обращения сигнала, вычисляя среднее время, затраченное на передачу нескольких сигналов, для каждого мобильного компьютера. Если время, затраченное на подтверждение приема сигнала, оказывается больше среднего времени, вычисленного точкой доступа, точка доступа передает сигнал повторно.

Поскольку точка доступа может подсчитать *среднее* время кругового обращения сигнала только по нескольким сеансам передачи, требуется точка отсчета, или «исходное время кругового обращения сигнала». Точка доступа использует значение параметра «Initial RTT» (Исходное время RTT) для вычисления времени кругового обращения сигнала. Когда точка доступа начинает обмениваться данными с мобильным компьютером, это значение корректируется с в соответствии с фактическим средним временем кругового обращения между передачей сигналов и подтверждением их приема.

Возможные значения: от **10** до **10000**. По умолчанию используется значение **1000**.

Protocol Type ID (Идентификатор типа протокола)

Этот параметр определяет тип протокола 802.IQ и позволяет предотвратить конфликты с другими созданными пакетами типа Ethernet, использующими такой же тип протокола.

Возможные значения: от **1536** до **65535**. По умолчанию используется значение **2457**.



Важно! В большинстве случаев значение параметра *Protocol Type ID (Идентификатор типа протокола)*, установленное по умолчанию, менять не требуется. При изменении типа протокола необходимо внести соответствующие изменения на всех мобильных устройствах.

Forward 802.IQ Packets Only (Пересылать только пакеты 802.IQ)

При передаче пакетов по мостовому соединению между беспроводной и проводной сетью этот параметр позволяет устройствам 9160 G2 автоматически отфильтровывать и отбрасывать пакеты, относящиеся к другим типам (не 802.IQ v1). По умолчанию этот параметр **отключен**.

802.IQ v1 Beacon Interfaces (Интерфейсы маячка 802.IQ v1)

Выберите интерфейс, который будет использоваться для рассылки маячков.

Доступные интерфейсы: *Wired (Проводной)*, *WLAN0*, *WLAN1*, *WDS0*, *WDS1*, *WDS2*, *WDS3*.

24.1.3 Меню функций 802.IQ v2

Доступ к меню *802.IQ v2 Features (Функции 802.IQ v2)* выполняется на вкладке *802.IQ* в разделе *Connectivity (Подключения)* (см. Рис. 24.1 на стр. 345).

Enabled (Включено)

Этот параметр позволяет включить или отключить функцию 802.IQ v2.

По умолчанию этот параметр **отключен**.

Beacon UDP Port (Порт маячка UDP)

Этот параметр определяет порт UDP для широковещательной передачи маячка. Если в сети находится несколько контроллеров 802.IQv2, значение этого параметра следует изменить, чтобы отделить эти системы друг от друга. Кроме того, значение этого параметра должно совпадать со значением того же параметра на мобильном компьютере. Возможные значения: от **5001** до **65535**. По умолчанию используется значение **8888**.

24.2 Обновление параметров 802.IQ

Для обновления параметров 802.IQ:

1. Перейдите на экран *802.IQ Settings (Параметры 802.IQ)*.
2. Внесите необходимые изменения в параметры.
3. Нажмите кнопку **Update (Обновить)**, чтобы применить изменения.

СЕТЕВОЙ ПРОТОКОЛ СИНХРОНИЗАЦИИ ВРЕМЕНИ

25

| | |
|---|-----|
| 25.1 Переход к параметрам времени. | 351 |
| 25.2 Включение и отключение сервера сетевого протокола синхронизации времени (NTP) | 352 |
| 25.3 Обновление параметров. | 353 |

Сетевой протокол синхронизации времени (NTP) — это стандартный интернет-протокол, синхронизирующий время компьютеров в сети. Серверы NTP передают *всемирное координированное время (UTC)*, также известное как *среднее время по Гринвичу*) клиентским системам. Протокол NTP периодически отправляет временные запросы серверам, используя возвращаемую метку времени для корректировки часов и часового пояса. Метка времени будет использоваться для обозначения даты и времени каждого события, записанного в сообщениях журнала регистрации. См. <http://www.ntp.org> для получения общей информации о протоколе NTP. В следующих разделах описан процесс настройки беспроводного шлюза 9160 G2 Wireless Gateway для использования определенного сервера NTP.

25.1 Переход к параметрам времени

Чтобы включить сервер *NTP*, перейдите на вкладку *Services (Службы) > Time (Время)* и внесите изменения в настройки, как указано ниже.

Рис. 25.1 Параметры времени

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

Modify how the access point discovers the time

Local Time

Mon Jun 18 18:41:53 UTC 2007

Network Time Protocol (NTP)

☒ Enabled ☐ Disabled

NTP Server

pool.ntp.org

Time Zone

CustomUTC +0000

Update

25.2 Включение и отключение сервера сетевого протокола синхронизации времени (NTP)

Чтобы настроить точку доступа для использования сервера сетевого протокола синхронизации времени (NTP), сначала необходимо **включить** использование протокола NTP, а затем выбрать нужный сервер NTP. Для отключения службы NTP в сети отключите протокол NTP на точке доступа.

Табл. 25.1 Параметры NTP

| Поле | Описание |
|---|---|
| <i>Local Time (Местное время)</i> | Текущее местное время отображается при каждом обновлении. |
| <i>Network Time Protocol (NTP) (Сетевой протокол синхронизации времени)</i> | <p>С помощью протокола NTP точка доступа получает информацию о времени от сетевого сервера и использует ее. Использование сервера NTP дает возможность точке доступа фиксировать точное время в сообщениях журнала регистрации событий и информации о сеансах.</p> <p>Для получения дополнительной информации о протоколе NTP см. http://www.ntp.org.</p> <p>Включите или отключите использование сервера сетевого протокола синхронизации времени (NTP):</p> <ul style="list-style-type: none">• Чтобы включить сервер NTP, нажмите Enabled (Включено).• Чтобы отключить сервер NTP, нажмите Disabled (Отключено). |
| <i>Сервер NTP</i> | <p>Если использование сервера NTP включено, выберите нужный сервер NTP.</p> <p>Можно указать сервер NTP по имени хоста или IP-адресу, но использование IP-адреса не рекомендуется, так как он может изменяться.</p> |
| <i>Часовой пояс</i> | <p>Список часовых поясов (например, «EST (-05:00)») представлен в раскрывающемся меню, в котором также можно указать собственное значение. Если выбрано значение <i>Custom (Другой)</i>, рядом с полем выбора появляются два текстовых поля, где можно ввести свое значение и смещение относительно UTC. Смещение от UTC необходимо указать в часах и минутах к востоку от UTC. Например, значение -0800 означает смещение на 8 часов к западу от UTC (т.е. стандартное тихоокеанское время), а значение +0930 — смещение на 9 часов 30 минут к востоку (т.е. австралийское центральное стандартное время).</p> <p>Функция перехода на летнее время недоступна.</p> |

25.3 Обновление параметров

Для обновления параметров времени:

1. Перейдите на вкладку *Time (Время)*.
2. Внесите необходимые изменения в параметры времени.
3. Нажмите кнопку **Update** (Обновить), чтобы применить изменения.

СОЗДАНИЕ РЕЗЕРВНОЙ КОПИИ И ВОССТАНОВЛЕНИЕ КОНФИГУРАЦИИ **26**

| | |
|--|-----|
| 26.1 Переход к параметрам настройки точки доступа | 357 |
| 26.2 Сброс конфигурации до заводских настроек по умолчанию | 358 |
| 26.3 Сохранение текущей конфигурации в резервный файл | 358 |
| 26.4 Восстановление конфигурации из предыдущего сохраненного файла | 359 |
| 26.5 Перезагрузка точки доступа | 359 |
| 26.6 Обновление прошивки | 360 |
| 26.6.1 Установка обновления | 361 |
| 26.6.2 Проверка обновления прошивки | 362 |

Вы можете сохранить копию текущих параметров на беспроводном шлюзе 9160 G2 Wireless Gateway в резервный конфигурационный файл. В дальнейшем резервный файл может быть использован для восстановления предыдущей сохраненной конфигурации точки доступа.

26.1 Переход к параметрам настройки точки доступа

Для управления конфигурацией точки доступа перейдите на вкладку *Maintenance (Обслуживание)* > *Configuration (Конфигурация)* и при работе со страницей следуйте приведенным ниже инструкциям.

Рис. 26.1 Обзор конфигурации точки доступа

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Maintenance

Configuration

Manage this Access Point's Configuration

To Restore Factory Default Configuration ...

Click "Reset" to load the factory defaults in place of the current configuration for this AP.

[Reset](#)

To Save the Current Configuration to a Backup File ...

Click the link below to download a file containing the current configuration for this AP.

☐ Encrypt the configuration file

[download configuration](#)

To Restore the Configuration from a Previously Saved File ...

Enter the path and file name of the configuration backup file you want to use, or click "Browse" to open a dialog where you can locate and select the file. Then click "Restore" to load this file in place of the current configuration.

[Browse...](#)

[Restore](#)

To Reboot the Access Point ...

Click the "Reboot" button.

[Reboot](#)

26.2 Сброс конфигурации до заводских настроек по умолчанию

Если при возникновении проблем на беспроводном шлюзе 9160 G2 Wireless Gateway вы выполнили все доступные действия по устранению неполадок, но проблема не была устранена, используйте функцию *Reset Configuration (Сброс конфигурации)*. С помощью этой функции параметры, включая новый пароль и настройки беспроводной сети, будут сброшены до заводских настроек по умолчанию.

1. Перейдите на вкладку **Maintenance (Обслуживание) > Configuration (Конфигурация)**.
2. Нажмите кнопку **Reset (Сбросить)**.

Будут восстановлены заводские настройки по умолчанию.



Примечание. Помните, что если вы сбросите конфигурацию на этом экране, настройки будут восстановлены только для этой точки доступа; настройки на других точках доступа в кластере останутся прежними.

Для получения информации о заводских настройках по умолчанию см. «Значения по умолчанию беспроводного шлюза 9160 G2 Wireless Gateway» на стр. 29.

26.3 Сохранение текущей конфигурации в резервный файл

Чтобы сохранить копию текущих параметров точки доступа в резервный конфигурационный файл (в формате .cbk), выполните следующие действия:

1. Нажмите ссылку **download configuration** (загрузить конфигурацию).
Откроется диалоговое окно *File Download or Open (Загрузить или открыть файл)*.
2. Выберите *Save (Сохранить)* в этом диалоговом окне.
Откроется диспетчер файлов.
3. В диспетчере файлов выберите каталог, в который вы хотите сохранить файл, и нажмите **ОК** для сохранения.

Можно оставить имя резервного файла по умолчанию (config.cbk) или переименовать файл, сохранив его расширение — .cbk.

26.4 Восстановление конфигурации из предыдущего сохраненного файла

Чтобы восстановить предыдущие сохраненные параметры точки доступа, выполните следующие действия:

1. Выберите нужный резервный конфигурационный файл, указав полный путь к файлу и имя файла в текстовом поле *Restore (Восстановить)* или нажмите **Browse** (Обзор) и выберите файл.

(Для функции восстановления можно использовать только те файлы, которые были созданы с помощью функции Backup (Резервная копия) и сохранены как резервные конфигурационные файлы с расширением .cbk, например config.cbk.)



Важно! *Конфигурационный файл можно восстановить только для той же модели беспроводного шлюза 9160, на которой он был создан.*

Например, на модели беспроводного шлюза 9160 G2 «9160 Wireless Gateway» невозможно восстановить конфигурацию из файла, созданного на модели 9160 G2 «9160 Wireless Gateway (Dual Radio)».

2. Нажмите кнопку **Restore** (Восстановить).

Точка доступа будет перезагружена.



*Примечание. При нажатии кнопки **Restore** (Восстановить) точка доступа будет перезагружена. Откроется диалоговое окно подтверждения перезагрузки, после чего отобразится сообщение о состоянии перезагрузки. Дождитесь, когда закончится процесс перезагрузки (это занимает минуту или две). Затем попробуйте перейти на веб-страницы администрирования, следуя приведенным ниже инструкциям; эти страницы будут доступны только после полного завершения процесса перезагрузки.*

После перезагрузки точки доступа перейдите на веб-страницы администрирования, нажав на одну из вкладок (если пользовательский интерфейс еще будет отображаться) или введя IP-адрес точки доступа в адресную строку браузера. Вы должны увидеть, что параметры настройки восстановились до оригинальных настроек, извлеченных из резервного файла.

26.5 Перезагрузка точки доступа

Для целей обслуживания или выполнения действий по устранению неисправностей вы можете перезагрузить беспроводной шлюз 9160 G2 Wireless Gateway следующим образом.

1. Перейдите на вкладку *Maintenance (Обслуживание)* > *Configuration (Конфигурация)*.
2. Нажмите кнопку **Restore** (Восстановить).

Точка доступа будет перезагружена.

26.6 Обновление прошивки

По мере выхода новых версий прошивки беспроводного шлюза 9160 G2 Wireless Gateway вы можете обновлять прошивку на своих устройствах, чтобы воспользоваться новыми функциями и улучшениями.



Важно! *Нельзя обновлять прошивку с беспроводного клиента, ассоциированного с точкой доступа, которую вы обновляете. В этом случае процесс обновления не будет выполнен. Кроме того, все беспроводные клиенты будут диссоциированы, и их нельзя будет ассоциировать снова.*

Если вы столкнетесь в такой проблемой, используйте проводной клиент для получения доступа к точке доступа следующим образом.

- *Создайте проводное подключение Ethernet между компьютером и точкой доступа.*
- *Откройте интерфейс администрирования.*

Повторите процедуру обновления с помощью проводного клиента.

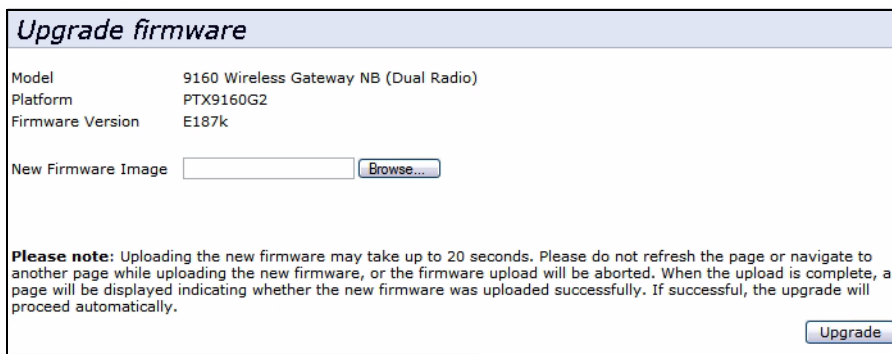


Примечание. *Необходимо выполнить эти действия для каждой точки доступа, так как невозможно обновить прошивку автоматически для всего кластера.*

Помните, что при успешном обновлении прошивки конфигурационные настройки точки доступа возвращаются к заводским настройкам по умолчанию. (см. «Значения по умолчанию беспроводного шлюза 9160 G2 Wireless Gateway» на стр. 29).

Чтобы обновить прошивку на определенной точке доступа, выполните следующие действия:

1. Перейдите на вкладку *Maintenance (Обслуживание)* > *Upgrade (Обновление)* на веб-страницах администрирования точки доступа.



Upgrade firmware

Model 9160 Wireless Gateway NB (Dual Radio)
Platform PTX9160G2
Firmware Version E187k

New Firmware Image

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

Вы увидите информацию о текущей версии прошивки и получите возможность обновить прошивку до новой версии.

2. Если вы знаете путь к файлу образа новой версии прошивки, введите его в текстовое поле *New Firmware Image (Образ новой версии прошивки)*. В противном случае нажмите кнопку **Browse (Обзор)** и выберите файл образа прошивки.



Примечание. Файл обновления прошивки должен иметь следующий формат: <FileName>.upgrade.tar

Не используйте файлы <FileName>.bin или файлы других форматов для обновления — они не будут работать.

26.6.1 Установка обновления

1. Нажмите **Update (Обновить)**, чтобы применить новый образ прошивки.
При нажатии кнопки «Update» (Обновить) откроется окно подтверждения процесса обновления.
2. Нажмите **ОК** для подтверждения установки обновления и запуска процесса.



Важно! Обновление прошивки начнется после нажатия кнопки «Update» (Обновить) и кнопки «ОК» в окне подтверждения.

Процесс обновления может занять несколько минут, в течение которых точка доступа будет недоступна. Не отключайте питание точки доступа во время процесса обновления. По завершении обновления точка доступа будет перезагружена и на ней будут восстановлены заводские параметры настройки по умолчанию.

26.6.2 Проверка обновления прошивки

Для подтверждения успешного обновления прошивки проверьте номер версии прошивки на вкладке *Upgrade (Обновление)* (а также на вкладке *Basic Settings (Базовые параметры)*). При успешном обновлении будет отображаться новая версия микропрограммы.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ **27**

| | |
|---|-----|
| 27.1 Физические характеристики | 365 |
| 27.2 Условия эксплуатации | 365 |
| 27.3 Требования к питанию от источника переменного тока | 365 |
| 27.4 Требования к питанию через Ethernet. | 366 |
| 27.5 Процессор и память | 366 |
| 27.6 Сетевые интерфейсы | 366 |
| 27.7 Радиомодули | 366 |



Примечание. Технические характеристики являются номинальными и могут быть изменены без предварительного уведомления.

27.1 Физические характеристики

| | |
|----------|---|
| Корпус: | Черный цвет, материал: Bayblend FR2000 |
| Размеры: | $\leq 30 \times 20 \times 12,5$ см (11,8 x 7,9 x 4,9 дюймов) |
| Вес: | $\leq 2,25$ кг (5 фунтов) (исключая радиомодули, антенны и дополнительные аксессуары) |

27.2 Условия эксплуатации

| | |
|---|--|
| Рабочая температура: | от 0 до 45°C (от 32 до 113°F) |
| Относительная влажность воздуха при эксплуатации: | от 10 до 90% |
| Температура хранения: | от 0 до 70°C (от 32 до 158°F) |
| Класс защиты от пыли и влаги: | IP42 или выше |
| Вибрация: | EH0002 (вибрация только при перевозке) |
| Наработка на отказ: | 25000 часов (MIL-HDBK-217F) |

27.3 Требования к питанию от источника переменного тока

Универсальный входной разъем питания переменного тока через стандартный коннектор IEC320. Отключает питание через Ethernet (стандарт 802.3af) при подключении.

| | |
|---------------------------|--------------------------------------|
| Входное напряжение: | 100-240 В переменного тока (номинал) |
| Сила электрического тока: | максимум 5 А |



Предупреждение. К винту заземления, расположенному на быстроразъемной опоре, и соответствующей клемме заземления беспроводного шлюза 9160 G2, подключенного к внешней антенне, должен быть подключен заземляющий провод длиной не более 3 м.

27.4 Требования к питанию через Ethernet

Соответствует стандарту IEEE 802.3af (отключается при подключенном источнике переменного тока).

Входное напряжение: 37-57 В пост. тока

Встроенные компоненты

Источник питания: 2,5 Вт (при $\eta=0,8$ при полных 12,5 Вт от Ethernet)

Два радиомодуля 802.11b: 4 Вт

Основная материнская плата: 6 Вт

27.5 Процессор и память

Процессор: Intel IXP420, 266 МГц

Флэш-память ROM: 8 МБ

SDRAM: 32 МБ

27.6 Сетевые интерфейсы

Встроенный Ethernet: карта 10BaseT/100BaseT (10/100 Мб/с) с функцией автоматического согласования, полудуплекс и полный дуплекс.
Автораспознавание скорости передачи данных.

27.7 Радиомодули

Радиомодуль 802.11A/G с картой Mini-PCI без интегрированной антенны

Радиомодуль 802.11G с картой Mini-PCI без интегрированной антенны

Мощность передатчика: 100 мВт для стран-членов FCC; 50 мВт для стран-членов ETSI

Диапазон частот: 2,4-2,5 ГГц (802.11b/g); 5,15-5,825 ГГц (802.11a)

Скорость передачи данных: 802.11b: 1, 2, 5,5, 11 Мб/с
802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с

| | | |
|--------------------|--------|-------------------------------|
| Количество каналов | FCC: | 11 (802.11b/g) и 12 (802.11a) |
| | ETSI: | 13 (802.11b/g) и 19 (802.11a) |
| | Китай: | 13 (802.11b/g) и 4 (802.11a) |



*Примечание. Все каналы 802.11a являются неперекрывающимися.
Перекрывающиеся каналы отсутствуют на частоте 2,4 ГГц.*

RA1001A — узкополосный радиомодуль

Узкополосная модуляция Psion Teklogix (2/4 уровень FSK)

Форм-фактор: PC Card типа III

Мощность передачи: 1 Вт или 0,5 Вт

Диапазон частот: 403-422 МГц, 419-435 МГц, 435-451 МГц,
450-470 МГц, 464-480 МГц,
480-496 МГц, 496-512 МГц

Чувствительность приемника: < -110 дБм при 19,2 Кбит/с (4 уровень FSK)

Скорость передачи данных: 4800 бит/с, 9600 бит/с, 19,2 Кбит/с

ПРИЛОЖЕНИЕ А

КОНФИГУРАЦИИ ПОРТОВ И СХЕМЫ КАБЕЛЬНЫХ СОЕДИНЕНИЙ

А.1 Консольный порт

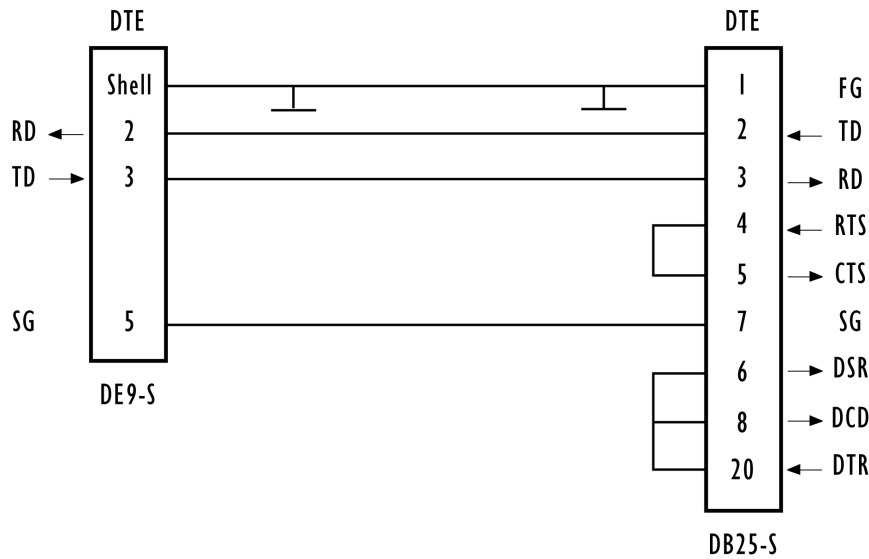
| № контакта | Название | Функция | Направление |
|------------|----------|--|-------------|
| 3 | TD | Передача данных | Выход |
| 2 | RD | Получение данных | Вход |
| 5 | SG | Заземление сигнала | – |
| 4* | DTR | Сигнал готовности терминала обработки данных | Выход |
| 7* | RTS | Запрос на передачу данных | Выход |

* всегда должен иметь смещение к уровню питающего напряжения

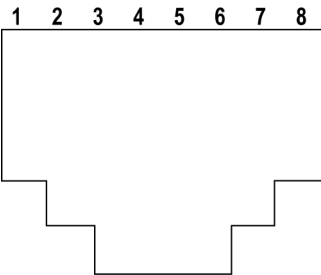
А.2 Описание последовательных кабелей

| № кабеля | Функция | Подключение | Стандартная длина |
|----------|----------------------|-------------|-------------------|
| 19387 | От 9160 G2 к консоли | Прямое | 6 футов (1,8 м) |

Кабель консольного порта № 19387



A.3 Выводы разъема RJ-45 (10BaseT/100BaseT Ethernet)



| 9160 G2, использующий переменный ток | | 9160 G2, использующий Ethernet как источник питания* | |
|--------------------------------------|-----------------|---|-----|
| | | | |
| 1 | TD+ | 1 | TD+ |
| 2 | TD- | 2 | TD- |
| 3 | RD+ | 3 | RD+ |
| 4 | Не используется | 4 | |
| 5 | Не используется | 5 | |
| 6 | RD- | 6 | RD- |
| 7 | Не используется | 7 | |
| 8 | Не используется | 8 | |
| | | * Беспроводной шлюз 9160 G2 также может принимать 48 В постоянного тока по парам каналов данных (1,2) и (3,6) от таких систем, обеспечивающих питание через Ethernet. | |



Примечание. Как правило, для подключения витой пары (10BaseT или 100BaseT) к сетевому концентратору требуется простое подключение.

ПРИЛОЖЕНИЕ В

ПАРАМЕТРЫ БЕЗОПАСНОСТИ НА БЕСПРОВОДНЫХ КЛИЕНТАХ/RADIUS-СЕРВЕРЕ

| | |
|--|----|
| В.1 Сетевая инфраструктура; выбор между встроенным и внешним сервером аутентификации. | 8 |
| В.1.1 Использование встроенного сервера аутентификации (EAP-PEAP). | 8 |
| В.1.2 Использование внешнего RADIUS-сервера с сертификатами EAP-TLS или EAP-PEAP | 9 |
| В.2 Убедитесь, что у вас установлена последняя версия беспроводного клиентского ПО. | 9 |
| В.3 Доступ к параметрам безопасности беспроводных клиентов Microsoft Windows | 9 |
| В.4 Настройка доступа клиента к незащищенной сети (с отключенным режимом безопасности) | 12 |
| В.5 Настройка статического WEP-шифрования на клиенте | 14 |
| В.6 Настройка режима безопасности IEEE 802.1x на клиенте. | 17 |
| В.6.1 Клиенты с режимом безопасности IEEE 802.1x и протоколом EAP/PEAP . . . | 17 |
| В.6.2 Клиенты с режимом безопасности IEEE 802.1x, использующим сертификат EAP/TLS | 21 |
| В.7 Настройка режима безопасности WPA/WPA2 Enterprise (RADIUS) на клиенте . . . | 25 |
| В.7.1 Клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) с использованием протокола EAP/PEAP. | 25 |
| В.7.2 Клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) с использованием сертификата EAP-TLS | 30 |
| В.8 Настройка режима безопасности WPA/WPA2 Personal (PSK) на клиенте | 34 |
| В.9 Настройка внешнего RADIUS-сервера для распознавания 9160 G2 | 37 |
| В.10 Получение сертификата TLS-EAP для клиента | 41 |
| В.11 Настройка RADIUS-сервера для тегов VLAN. | 47 |
| В.11.1 Настройка RADIUS-сервера | 47 |

Как правило, для подключения к различным сетям (точкам доступа) пользователи настраивают режим безопасности на своих беспроводных клиентах. Список «Available Networks» (Доступные сети) будет меняться в зависимости от местоположения клиента и от того, какие точки доступа находятся в сети и обнаруживаются в этом месте.¹ Когда клиент обнаруживает точку доступа с соответствующим режимом безопасности, она остается в списке сетей клиента, но в зависимости от ситуации отображается как доступная или недоступная. Для каждой сети, к которой вы хотите подключиться, настройте параметры безопасности на клиенте таким образом, чтобы они совпадали с режимом безопасности, используемым в этой сети.

Здесь описана настройка режима безопасности на клиенте, использующим клиентское ПО Microsoft® Windows® для подключения к беспроводной сети. В примере используется клиентское ПО Windows как наиболее распространенное и доступное для компьютеров и ноутбуков с установленной системой Windows. Процедура будет немного отличаться, если вы используете другое клиентское ПО (например, Funk Odyssey®), но конфигурационная информация, которую вам нужно предоставить, будет той же.



Примечание. Рекомендованная последовательность настройки системы безопасности: 1) настройка режима безопасности на точке доступа; 2) настройка режима безопасности на каждом беспроводном клиенте. Предполагается, что сначала вы подключитесь к точке доступа с неустановленным режимом безопасности (значение «None» (Нет)) с незащищенного беспроводного клиента. После первоначального подключения вы можете перейти на веб-страницы администрирования точки доступа и настроить режим безопасности.

*После повторной настройки режима безопасности на точке доступа нажмите на кнопку **Update** (Обновить), и ваш беспроводной клиент будет диссоциирован. При этом соединение с веб-страницами администрирования точки доступа будет потеряно. В некоторых случаях может потребоваться ввести дополнительные изменения в параметры безопасности точки доступа до настройки клиента. Поэтому необходимо иметь резервное подключение Ethernet (проводное).*

В следующих разделах описан процесс настройки каждого из поддерживаемых режимов безопасности на беспроводных клиентах сети, обслуживаемой беспроводным шлюзом 9160 G2 Wireless Gateway.

¹Исключением является ситуация, когда на точке доступа запрещена трансляция собственного сетевого имени. В этом случае идентификатор SSID не отображается в списке «Available Networks» (Доступные сети) на клиенте. Поэтому для подключения к сети в свойствах сетевого соединения клиента необходимо указать точное сетевое имя.

В.1 Сетевая инфраструктура; выбор между встроенным и внешним сервером аутентификации

Конфигурации сетевой безопасности, которые включают в себя *инфраструктуры открытого ключа* (PKI), серверы *службы идентификации удаленных пользователей* (RADIUS) и *центры сертификации* (CA), могут сильно меняться от одной организации к другой в отношении предоставления функций *аутентификации*, *авторизации* и *учета* (AAA). В конечном итоге, способ настройки режима безопасности на клиентских устройствах для доступа к беспроводной сети определяется особенностями инфраструктуры. В настоящем документе приводятся только общие сведения о каждом типе клиентских конфигураций, поддерживаемых беспроводным шлюзом 9160 G2 Wireless Gateway; в нем не содержатся подробные сведения о каждом возможном сценарии работы.

В.1.1 Использование встроенного сервера аутентификации (EAP-PEAP)

Если у вас нет RADIUS-сервера или инфраструктуры PKI или вы не знакомы большинством этих понятий, рекомендуем настроить режим безопасности беспроводных шлюзов 9160 G2 Wireless Gateway, использующий *встроенный сервер аутентификации* на точке доступа. Это значит, что на точке доступа нужно выбрать режим безопасности «IEEE 802.1x» или «WPA/WPA2 Enterprise (RADIUS)». (Встроенный сервер аутентификации использует протокол аутентификации EAP-PEAP.)

- Если на беспроводном шлюзе 9160 G2 Wireless Gateway настроен режим безопасности IEEE 802.1x и используется встроенный сервер аутентификации, настройка беспроводных клиентов выполняется в соответствии с описанием, приведенным в «Клиенты с режимом безопасности IEEE 802.1x и протоколом EAP/PEAP» на стр. В-17.
- Если на беспроводном шлюзе 9160 G2 Wireless Gateway настроен режим безопасности WPA/WPA2 Enterprise (RADIUS) и используется встроенный сервер аутентификации, настройка беспроводных клиентов выполняется в соответствии с описанием, приведенным в «Клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) с использованием протокола EAP/PEAP» на стр. В-25.

В.1.2 Использование внешнего RADIUS-сервера с сертификатами EAP-TLS или EAP-PEAP

Мы исходим из того, что если у вас настроен внешний RADIUS-сервер и PKI/CA, вы знаете, как настроить параметры безопасности клиента в соответствии с особенностями инфраструктуры вашей системы безопасности, помимо фундаментальных знаний, которые приводятся в данном документе. Здесь рассматриваются следующие вопросы, связанные с конфигурацией системы безопасности клиентов в среде RADIUS-PKI:

- «Клиенты с режимом безопасности IEEE 802.1x, использующим сертификат EAP/TLS» на стр. В-21.
- «Клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) с использованием сертификата EAP-TLS» на стр. В-30.
- «Настройка внешнего RADIUS-сервера для распознавания 9160 G2» на стр. В-37.
- «Получение сертификата TLS-EAP для клиента» на стр. В-41.

В данном документе не содержатся подробные сведения о настройке клиента EAP-PEAP с внешним RADIUS-сервером.

В.2 Убедитесь, что у вас установлена последняя версия беспроводного клиентского ПО

Перед настройкой не забудьте о том, что пакеты обновления, обновления, новые версии драйверов и другие поддерживающие технологии для беспроводных клиентов выпускаются довольно часто. Общей проблемой, с которой сталкиваются пользователи при настройке системы безопасности клиентов, является отсутствие нужного драйвера или обновления на клиентском устройстве. Например, если вы настраиваете на клиенте режим WPA, убедитесь, что на нем установлен драйвер, поддерживающий протокол WPA, который является относительно новой технологией. В настоящее время многие карты клиентских устройств поступают в продажу без последних версий драйверов.

В.3 Доступ к параметрам безопасности беспроводных клиентов Microsoft Windows

Доступ к параметрам безопасности беспроводных клиентов под управлением Windows XP осуществляется одним из двух способов:

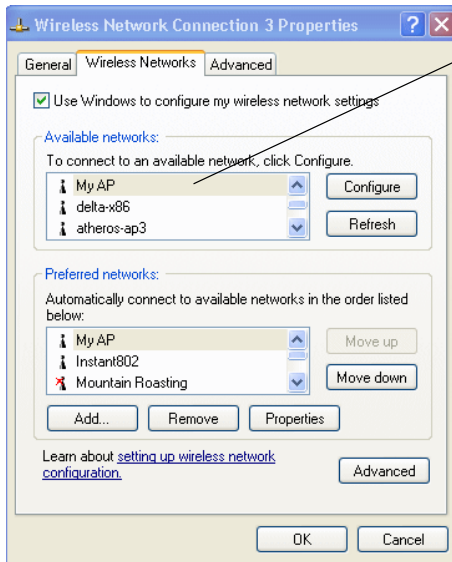
1. С помощью значка *Wireless Connection (Беспроводное соединение)* на панели задач Windows:

- Щелкните правой кнопкой мыши на значке беспроводного соединения, который находится на панели задач Windows, и выберите пункт **View available wireless networks** (Просмотреть доступные беспроводные сети).
- Выберите идентификатор SSID сети, к которой вы хотите подключиться, и нажмите **Advanced** (Дополнительно), чтобы открыть диалоговое окно *Wireless Network Connection Properties* (Свойства беспроводного сетевого подключения).

ИЛИ

1. С помощью меню *Start* (Пуск) в левой части панели задач:
 - В меню *Start* (Пуск) на панели задач выберите **Start** (Пуск), **My Network Places** (Сетевое окружение), чтобы открыть окно «Network Connections» (Сетевые подключения).
 - В меню *Network Tasks* (Сетевые задачи) слева нажмите **View Network Connections** (Просмотреть сетевые подключения), чтобы открыть окно *Network Connections* (Сетевые подключения).
 - Выберите *Wireless Network Connection* (Беспроводное сетевое подключение), которое вы хотите настроить, щелкните правой кнопкой мыши и выберите **View available wireless networks** (Просмотреть доступные беспроводные сети).
 - Выберите идентификатор SSID сети, к которой вы хотите подключиться, и нажмите **Advanced** (Дополнительно), чтобы открыть диалоговое окно *Wireless Network Connection Properties* (Свойства беспроводного сетевого подключения).

На вкладке *Wireless Networks* (Беспроводные сети), которая должна отображаться автоматически, содержатся два списка: *Available networks* (Доступные сети) и *Preferred networks* (Предпочтительные сети).



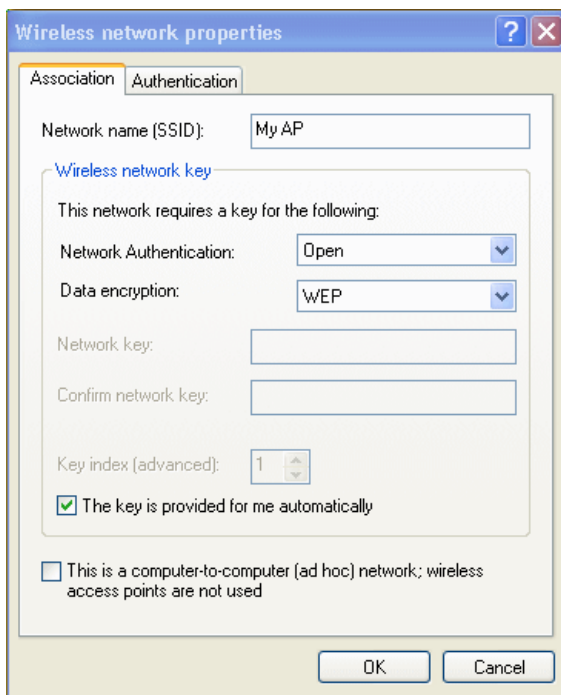
Список доступных сетей будет меняться в зависимости от местоположения клиента. Каждая сеть (или точка доступа), определяемая клиентом, отображается в списке. Кнопка «Refresh» (Обновить) обновляет список с текущей информацией.

Для каждой сети, к которой вы хотите подключиться, настройте параметры безопасности на клиенте таким образом, чтобы они совпадали с режимом безопасности, используемым в этой сети.

Примечание. Исключением является ситуация, когда на точке доступа запрещена трансляция собственного сетевого имени. В этом случае имя не будет отображаться в списке. Поэтому для подключения к такой точке доступа необходимо указать ее точное сетевое имя.

2. В списке *Available networks* (Доступные сети) выберите идентификатор SSID сети, к которой вы хотите подключиться, и нажмите **Configure** (Настроить).

Откроется диалоговое окно *Wireless Network Connection Properties* (Свойства беспроводного сетевого соединения) с вкладками *Association* (Ассоциация) и *Authentication* (Аутентификация) для выбранной сети.



Используйте это диалоговое окно для настройки всех типов режимов безопасности клиентских устройств, описанных в следующих разделах. Убедитесь, что диалоговое окно *Wireless Network Properties* (*Свойства беспроводной сети*), в котором вы работаете, относится к сети с сетевым именем (SSID), к которой вы хотите подключить настраиваемый беспроводной клиент.

В.4 Настройка доступа клиента к незащищенной сети (с отключенным режимом безопасности)

Если точка доступа или беспроводная сеть, к которой вы хотите подключиться, имеет настройку режима безопасности «None» (Нет), т.е. режим безопасности на ней отключен, необходимо настроить клиент соответствующим образом. Для настройки подключения клиента с отключенным режимом безопасности необходимо выбрать для параметра *Network Authentication* (*Аутентификация сети*) в данной сети значение **Open** (Открытая система), а для параметра *Data Encryption* (*Шифрование данных*) — значение **Disabled** (Отключено), как описано ниже.

Если режим безопасности клиента настроен на работу с незащищенной сетью, подключение к сети может стать невозможным по причине несоответствия конфигураций систем безопасности клиента и точки доступа.

Чтобы отключить режим безопасности клиента, откройте диалоговое окно клиента *Network Properties (Свойства сети)* и настройте следующие параметры.

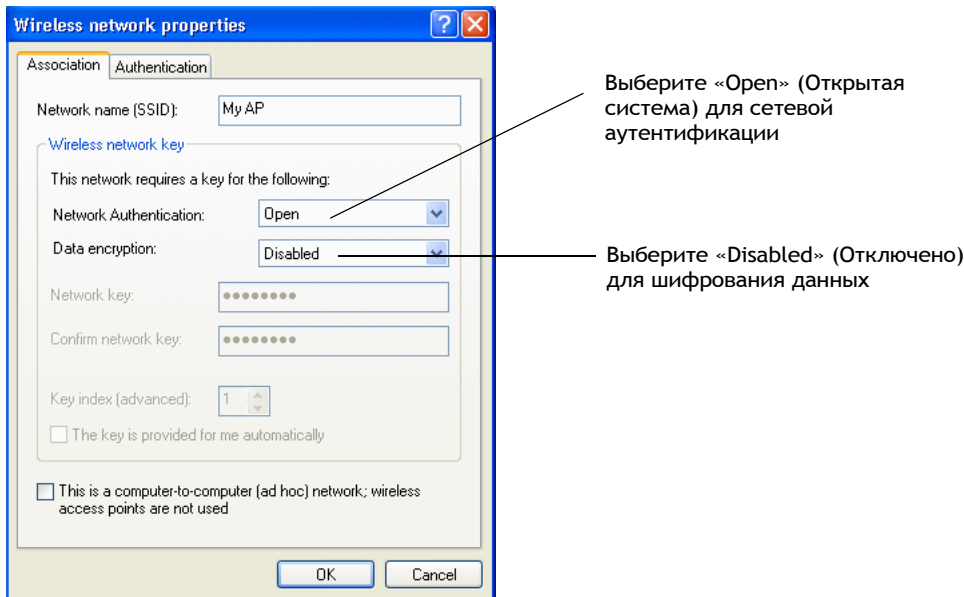


Табл. В.1 Параметры ассоциации

| | |
|---|-------------------------|
| <i>Network Authentication (Аутентификация сети)</i> | Open (Открытая система) |
| <i>Data Encryption (Шифрование данных)</i> | Disabled (Отключено) |

В.5 Настройка статического WEP-шифрования на клиенте

Статический эквивалент конфиденциальности проводных сетей (WEP) зашифровывает данные, передаваемые по беспроводной сети, с помощью статического (не изменяющегося) ключа. Используется поточный алгоритм шифрования, также называемый RC4. Точка доступа передает данные клиентским станциям, используя ключ. Каждый клиент должен использовать аналогичный ключ для декодирования данных, которые он получает от точки доступа. Разные клиенты могут использовать разные ключи для передачи данных точке доступа. (Также они могут использовать один ключ, но это менее безопасно, так как означает, что одна станция может дешифровать данные, передаваемые другой станцией.)

Если вы настроили режим статического WEP-шифрования на беспроводном шлюзе 9160 G2 Wireless Gateway. . .

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Modify Internal Network security settings

☒ Broadcast SSID

☐ Station Isolation

Mode:

Static WEP

Transfer key index:

1

Key Length:

☐ 64 bits

☒ 128 bits

☐ 152 bits

Key Type:

☐ ASCII

☒ Hex

WEP Keys:

(Characters required: 26)

1:

012345678901234567890123

2:

012345678901234567890123

3:

4:

Authentication :

☒ Open system

☐ Shared key

Update

... настройте режим безопасности WEP на каждом клиенте следующим образом.

Выберите «Open» (Открытая система) или «Shared» (Общая система)

Выберите WEP в качестве режима шифрования данных

Введите сетевой ключ, соответствующий ключу WEP на точке доступа в положении, установленном индексом передаточного ключа (и введите повторно для подтверждения)

(Необязательно) укажите другой индекс передаточного ключа для отправки данных от клиента к точке доступа

Отключите настройку автоматического ключа

Табл. В.2 Параметры ассоциации

| | |
|--|--|
| <i>Network Authentication</i> (Аутентификация сети) | <p>Open (Открытая система) или Shared (Общая система), в зависимости от того, как вы настроили этот параметр на точке доступа.</p> <p>Примечание. Если на точке доступа установлено значение алгоритма аутентификации Both (Все), клиенты, на которых установлено значение Shared (Общая система) или Open (Открытая система) могут ассоциироваться с этой точкой доступа. Клиенты, настроенные на использование протокола WEP в режиме общего ключа, должны иметь действительный ключ WEP для установки связи с точкой доступа. Клиенты, на которых режим WEP настроен на использование в качестве открытой системы, могут ассоциироваться с точкой доступа даже без корректного ключа WEP (однако ключ потребуется для просмотра и обмена данными). Для получения дополнительной информации обратитесь к интерактивной справке на точке доступа.</p> |
| <i>Data Encryption</i> (Шифрование данных) | WEP |

Табл. В.2 Параметры ассоциации (Продолжение)

| | |
|---|---|
| <i>Network Key</i> (Сетевой ключ) | Укажите ключ WEP , который вы задали как позицию «Transfer Key Index» (Индекс передаточного ключа) в разделе <i>Security settings</i> (Параметры безопасности) точки доступа. Например, если на точке доступа установлено значение «Transfer Key Index» (Индекс передаточного ключа), равное 1 , на клиенте необходимо установить значение «Network Key» (Сетевой ключ), равное значению ключа WEP, установленному как WEP Key 1 (Ключ WEP 1) на точке доступа. |
| <i>Key Index</i> (Индекс ключа) | Установите индекс ключа, чтобы указать, какой из ключей WEP, заданных на экране <i>Security</i> (Безопасность) точки доступа будет использоваться для передачи данных от клиента точке доступа. Например, вы можете установить значения 1, 2, 3, или 4 , если на точке доступа настроены все четыре ключа WEP. |
| <i>The key is provided for me automatically</i> (Ключ предоставляется автоматически) | Отключите этот параметр (снимите флажок). |
| <i>Enable IEEE 802.1x authentication for this network</i> (Включить аутентификацию IEEE 802.1x для этой сети) | Убедитесь, что аутентификация IEEE 802.1x отключена (флажок должен быть снят). При выборе режима WEP-шифрования аутентификация отключается автоматически. |

Табл. В.3 Параметры аутентификации

| | |
|---|---|
| <i>Enable IEEE 802.1x authentication for this network</i> (Включить аутентификацию IEEE 802.1x для этой сети) | Убедитесь, что аутентификация IEEE 802.1x отключена (флажок должен быть снят). При выборе режима WEP-шифрования аутентификация отключается автоматически. |
|---|---|

Нажмите **ОК**, чтобы закрыть диалоговое окно *Wireless Network Properties* (Свойства беспроводной сети) и сохранить изменения.

Подключение к беспроводной сети клиента с режимом статического WEP-шифрования

Теперь клиенты с установленным режимом статического WEP-шифрования могут ассоциироваться с точкой доступа и проходить процесс аутентификации. На клиенте не требуется вводить ключ WEP. Ключ WEP, установленный в параметрах безопасности клиента, будет использоваться при подключении автоматически.

В.6 Настройка режима безопасности IEEE 802.1x на клиенте

IEEE 802.1x — это стандарт, определяющий протокол аутентификации и доступ к инфраструктуре для управления ключами с использованием портов. Сообщения *расширяемого протокола аутентификации* (EAP), отправляемые по беспроводной сети IEEE 802.11 по протоколу передачи EAP-сообщений в стандарте 802.1x (EAP Encapsulation Over LANs, EAPOL). В режиме безопасности IEEE 802.1x используются динамически генерируемые ключи, которые периодически обновляются. Поточное шифрование RC4 используется для шифрования тела кадра и периодической проверки резервирования (CRC) каждого кадра 802.11.

В.6.1 Клиенты с режимом безопасности IEEE 802.1x и протоколом EAP/PEAP

Встроенный сервер аутентификации на беспроводном шлюзе 9160 G2 Wireless Gateway использует защищенный расширяемый протокол аутентификации (*Protected Extensible Authentication Protocol*), именуемый здесь «EAP/PEAP».

- Если на беспроводном шлюзе 9160 G2 Wireless Gateway вы используете встроенный сервер аутентификации с режимом безопасности «IEEE 802.1x», необходимо настроить беспроводные клиенты на использование протокола PEAP.
 - Кроме того, можно использовать внешний RADIUS-сервер, который работает по протоколу EAP/PEAP. В этом случае вам необходимо выполнить следующие действия:
 1. Добавить беспроводной шлюз 9160 G2 Wireless Gateway в список клиентов RADIUS-сервера.
- И
2. Настроить использование протокола PEAP на беспроводных клиентах, работающих в режиме безопасности IEEE 802.1x.



Примечание. В следующем примере используется встроенный сервер аутентификации, поставляемый с беспроводным шлюзом 9160 G2 Wireless Gateway. Если вы настраиваете использование протокола EAP/PEAP на клиенте точки доступа, которая использует внешний RADIUS-сервер, процесс настройки клиента будет несколько отличаться от данного примера, особенно в отношении проверки сертификатов.

Если вы настроили на беспроводном шлюзе 9160 G2 Wireless Gateway режим безопасности IEEE 802.1x. . .

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: IEEE802.1x

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☐ Enable radius accounting

Update

. . . настройте режим безопасности IEEE 802.1x с использованием аутентификации PEAP на каждом клиенте следующим образом:

Включите (установите флажок) аутентификацию IEEE 8021x

Выберите «Open» (Открытая система)

Выберите WEP в качестве режима шифрования данных

Выберите «Protected EAP (PEAP)» (Защищенный EAP (PEAP))

. . . затем нажмите Properties (Свойства)

Включите настройку автоматического ключа

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

1 OK Cancel

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks:

☒ Enable IEEE 802.1x authentication for this network:

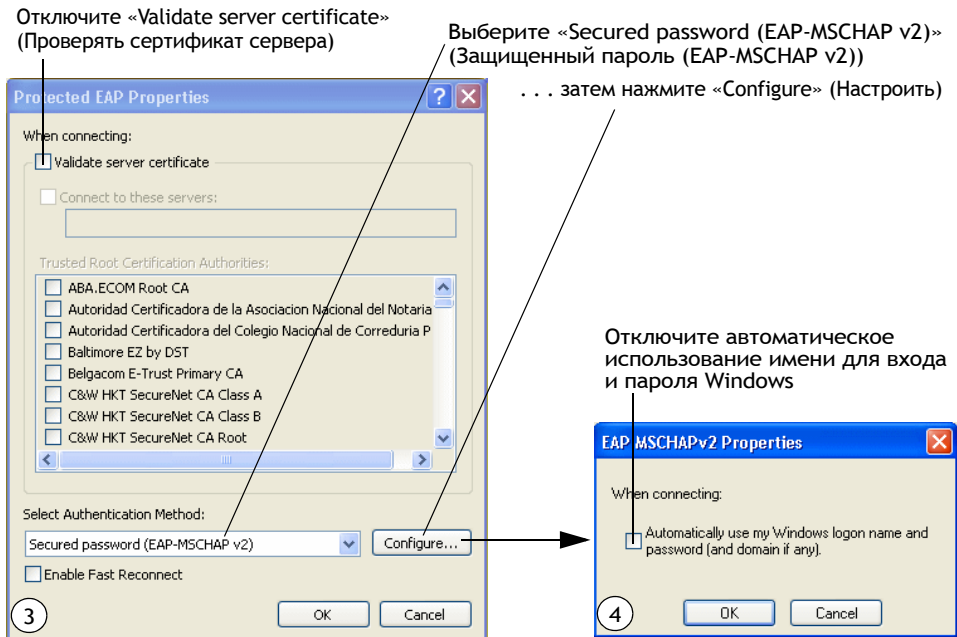
EAP type: Protected EAP (PEAP)

Properties

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

2 OK Cancel



1. Настройте следующие параметры на вкладке *Association* (Ассоциация) диалогового окна *Network Properties* (Свойства сети).

Табл. В.4 Параметры ассоциации

| | |
|--|--|
| <i>Network Authentication</i> (Аутентификация сети) | Оpen (Открытая система) |
| <i>Data Encryption</i> (Шифрование данных) | WEP Примечание. Поточное шифрование RC4 используется для шифрования тела кадра и периодической проверки резервирования (CRC) каждого кадра IEEE 802.11. Аналогичный алгоритм шифрования используется при статическом WEP-шифровании, поэтому для этого режима безопасности методом шифрования данных на клиенте является WEP-шифрование. |
| <i>The key is provided for me automatically</i> (Ключ предоставляется автоматически) | Включите (установите флажок) этот параметр. |

2. Настройте этот параметр на вкладке *Authentication* (Аутентификация).

Табл. В.5 Параметры аутентификации

| | |
|--------------------|---|
| EAP Type (Тип EAP) | Выберите Protected EAP (PEAP) (Защищенный EAP (PEAP)). |
|--------------------|---|

3. Нажмите **Properties** (Свойства) для открытия диалогового окна *Protected EAP Properties* (Свойства протокола PEAP) и настройте следующие параметры.

Табл. В.6 Параметры «Protected EAP Properties» (Свойства протокола PEAP)

| | |
|--|---|
| Validate Server Certificate (Проверять сертификат сервера) | Отключите этот параметр (снимите флажок). Примечание. Пример предполагает использование на точке доступа встроенного сервера аутентификации. Если вы настраиваете протокол EAP/PEAP на клиенте точки доступа, которая использует внешний RADIUS-сервер, для проверки сертификата выберите сертификат, соответствующий вашей инфраструктуре. |
| Select Authentication Method (Выбрать метод аутентификации) | Выберите Secured password (EAP-MSCHAP v2) (Защищенный пароль (EAP-MSCHAP v2)). |

4. Нажмите **Configure** (Настроить) для открытия диалогового окна *EAP MSCHAP v2 Properties* (Свойства протокола EAP MSCHAP v2).

В диалоговом окне **отключите** (снимите флажок) параметр *Automatically use my Windows logon name* (Автоматически использовать имя для входа в Windows). . . и т.д.

Нажмите **ОК** во всех диалоговых окнах (начиная с окна *EAP MSCHAP v2 Properties* (Свойства протокола EAP MSCHAP v2)), чтобы закрыть их и сохранить изменения.

Вход в беспроводную сеть с клиента с режимом безопасности IEEE 802.1x PEAP

Теперь клиенты с режимом безопасности IEEE 802.1x PEAP смогут ассоциироваться с точкой доступа. Пользователям клиентских устройств будет предложено ввести имя пользователя и пароль для аутентификации в сети.

В.6.2 Клиенты с режимом безопасности IEEE 802.1х, использующим сертификат EAP/TLS

Расширяемый протокол аутентификации с защитой транспортного уровня (Extensible Authentication Protocol (EAP) Transport Layer Security (TLS)), или протокол EAP-TLS, — протокол аутентификации, поддерживающий использование смарт-карт и сертификатов. При наличии внешнего RADIUS-сервера, поддерживающего протокол EAP-TLS, вы можете использовать этот протокол в режимах WPA/WPA2 Enterprise (RADIUS) и IEEE 802.1х.



Примечание. Для использования режима IEEE 802.1х с сертификатами EAP-TLS для аутентификации и авторизации клиентских устройств необходимо наличие внешнего RADIUS-сервера и настроенного в сети сервера инфраструктуры для аутентификации с использованием открытого ключа (Public Key Authority Infrastructure, PKI), включая центр сертификации (CA). Описание настройки RADIUS-сервера, PKI и сервера центра сертификации не приводится в данном документе. Ознакомьтесь с соответствующей документацией к этим продуктам. Информацию об инфраструктуре открытого ключа Microsoft Windows PKI можно найти в этих статьях:

«How to Install/Uninstall a Public Key Certificate Authority for Windows 2000» (<http://support.microsoft.com/default.aspx?scid=kb:en-us:231881>) и

«How to Configure a Certificate Server»

(<http://support.microsoft.com/default.aspx?scid=kb:en-us:318710#3>).

Чтобы использовать этот режим безопасности, выполните следующие действия.

1. Добавить беспроводной шлюз 9160 G2 Wireless Gateway в список клиентов RADIUS-сервера. (См. «Настройка внешнего RADIUS-сервера для распознавания 9160 G2» на стр. В-37.)
2. Настройте беспроводной шлюз 9160 G2 Wireless Gateway для использования RADIUS-сервера (указав IP-адрес RADIUS-сервера при настройке параметров безопасности «IEEE 802.1х»).
3. На беспроводных клиентах настройте режим безопасности «IEEE 802.1х» и выберите значение «Smart Card or other Certificate» (Смарт-карта или другой сертификат), следуя инструкциям, приведенным в данном разделе.
4. Получите сертификат для клиента, выполнив действия, описанные в «Получение сертификата TLS-EAP для клиента» на стр. В-41.

Если вы настроили режим безопасности IEEE 802.1x с использованием внешнего RADIUS-сервера на беспроводном шлюзе 9160 G2 Wireless Gateway. . .

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: IEEE802.1x

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☒ Enable radius accounting

Update

. . . настройте режим безопасности IEEE 802.1x с использованием аутентификации по сертификату на каждом клиенте следующим образом:

Выберите «Open» (Открытая система)

Выберите WEP в качестве режима шифрования данных

Включите (установите флажок) аутентификацию IEEE 8021x

Выберите «Smart Card/Certificate» (Смарт-карта/сертификат)

. . . затем нажмите «Properties» (Свойства)

Включите настройку автоматического ключа

1

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK Cancel

2

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks:

☒ Enable IEEE 802.1x authentication for this network

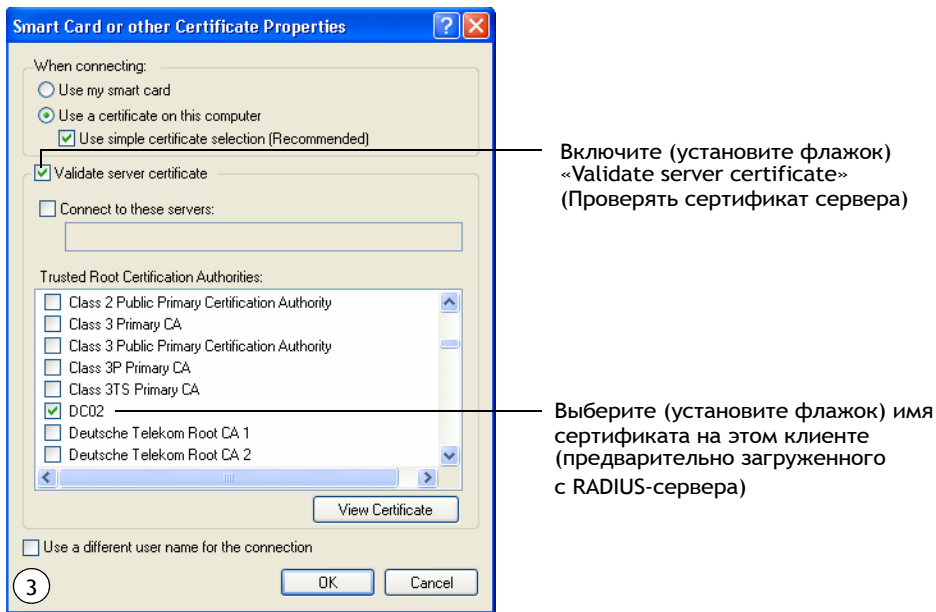
EAP type: Smart Card or other Certificate

Properties

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

OK Cancel



1. Настройте следующие параметры на вкладке *Association* (Ассоциация) диалогового окна *Network Properties* (Свойства сети).

Табл. В.7 Параметры ассоциации

| | |
|--|--|
| <i>Network Authentication</i> (Аутентификация сети) | Открытая система |
| <i>Data Encryption</i> (Шифрование данных) | WEP Примечание. Поточное шифрование RC4 используется для шифрования тела кадра и периодической проверки резервирования (CRC) каждого кадра IEEE 802.11. Аналогичный алгоритм шифрования используется при статическом WEP-шифровании, поэтому для этого режима безопасности методом шифрования данных на клиенте является WEP-шифрование. |
| <i>The key is provided for me automatically</i> (Ключ предоставляется автоматически) | Включите (установите флажок) этот параметр. |

2. Настройте эти параметры на вкладке *Authentication* (Аутентификация).

Табл. В.8 Параметры аутентификации

| | |
|--|---|
| <i>Enable IEEE 802.1x authentication for this network</i> (Включить аутентификацию IEEE 802.1x для этой сети) | Включите (установите флажок) этот параметр. |
| <i>EAP Type (Tun EAP)</i> | Выберите Smart Card or other Certificate (Смарт-карта или другой сертификат). |

3. Нажмите **Properties** (Свойства), чтобы открыть диалоговое окно *Smart Card or other Certificate Properties* (Свойства смарт-карты или другого сертификата), и включите параметр **Validate server certificate** (Проверить сертификат сервера).

Табл. В.9 Параметры «Smart Card Or Other Certificate Properties» (Свойства смарт-карты или другого сертификата)

| | |
|---|---|
| <i>Validate Server Certificate</i> (Проверить сертификат сервера) | Включите этот параметр (установите флажок). |
| <i>Certificates</i> (Сертификаты) | В списке сертификатов выберите сертификат для данного клиента. |

Нажмите **ОК** во всех диалоговых окнах для их закрытия и сохранения изменений.

4. Для завершения настройки клиента теперь необходимо получить сертификат от RADIUS-сервера и установить его на клиентское устройство. Для получения информации о необходимых для этого действиях см. «Получение сертификата TLS-EAP для клиента» на стр. В-41.

Подключение к сети клиента с режимом безопасности IEEE 802.1x и использованием сертификата

Теперь клиенты с режимом безопасности IEEE 802.1x могут подключаться к точке доступа, используя свои сертификаты TLS. Для подключения используется установленный сертификат, поэтому вводить данные о входе в систему не нужно. Сертификат автоматически отсылается RADIUS-серверу для аутентификации и авторизации.

В.7 Настройка режима безопасности WPA/WPA2 Enterprise (RADIUS) на клиенте

Режим безопасности WPA 2 (WPA2) с использованием службы идентификации удаленных пользователей (RADIUS) является реализацией стандарта Wi-Fi Alliance IEEE 802.11h, который включает в себя усовершенствованный стандарт шифрования (AES), режим гаммирования/протокол CBC-MAC (CCMP) и протокол шифрования с использованием временных ключей (TKIP). Этот режим требует использования RADIUS-сервера для аутентификации пользователей.

Также данный режим безопасности имеет обратную совместимость для беспроводных клиентов, которые поддерживают только оригинальный WPA.

При настройке режима безопасности WPA/WPA2 Enterprise (RADIUS) на точке доступа вы можете выбрать, какой сервер вы будете использовать — встроенный сервер аутентификации или внешний RADIUS-сервер.

Встроенный сервер аутентификации беспроводного шлюза 9160 G2 Wireless Gateway поддерживает защищенный расширяемый протокол аутентификации (*Protected Extensible Authentication Protocol*, EAP), или протокол EAP/PEAP, и протокол аутентификации по квитированию вызова компании, версия 2 (*Microsoft Challenge Handshake Authentication Protocol Version 2*, MSCHAP V2), обеспечивающий аутентификацию для двухточечных соединений (PPP) между компьютером под управлением Windows и сетевыми устройствами, например точками доступа.

Таким образом, при настройке режима безопасности сети (точки доступа) с использованием встроенного сервера аутентификации необходимо настроить режим безопасности WPA/WPA2 Enterprise (RADIUS) с использованием протокола EAP/PEAP на клиентских станциях.

При настройке этого режима безопасности сети (точки доступа) с использованием внешнего RADIUS-сервера необходимо настроить режим безопасности WPA/WPA2 Enterprise (RADIUS) на клиентских станциях с использованием протокола безопасности, с которым работает RADIUS-сервер.

В.7.1 Клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) с использованием протокола EAP/PEAP

Встроенный сервер аутентификации на беспроводном шлюзе 9160 G2 Wireless Gateway использует защищенный расширяемый протокол аутентификации (*Protected Extensible Authentication Protocol*), именуемый здесь «EAP/PEAP».

- Если на беспроводном шлюзе 9160 G2 Wireless Gateway вы используете встроенный сервер аутентификации с режимом безопасности «WPA/WPA2 Enterprise (RADIUS)», необходимо настроить беспроводные клиенты на использование протокола PEAP.
 - Кроме того, можно использовать внешний RADIUS-сервер, который работает по протоколу EAP/PEAP. В этом случае вам необходимо выполнить следующие действия:
 1. Добавить беспроводной шлюз 9160 G2 Wireless Gateway в список клиентов RADIUS-сервера.
- И
2. Настройте использование протокола PEAP на беспроводных клиентах, работающих в режиме безопасности «WPA/WPA2 Enterprise (RADIUS)».



Примечание. В следующем примере используется встроенный сервер аутентификации, поставляемый с беспроводным шлюзом 9160 G2 Wireless Gateway. Если вы настраиваете использование протокола EAP/PEAP на клиенте точки доступа, которая использует внешний RADIUS-сервер, процесс настройки клиента будет несколько отличаться от данного примера, особенно в отношении проверки сертификатов.

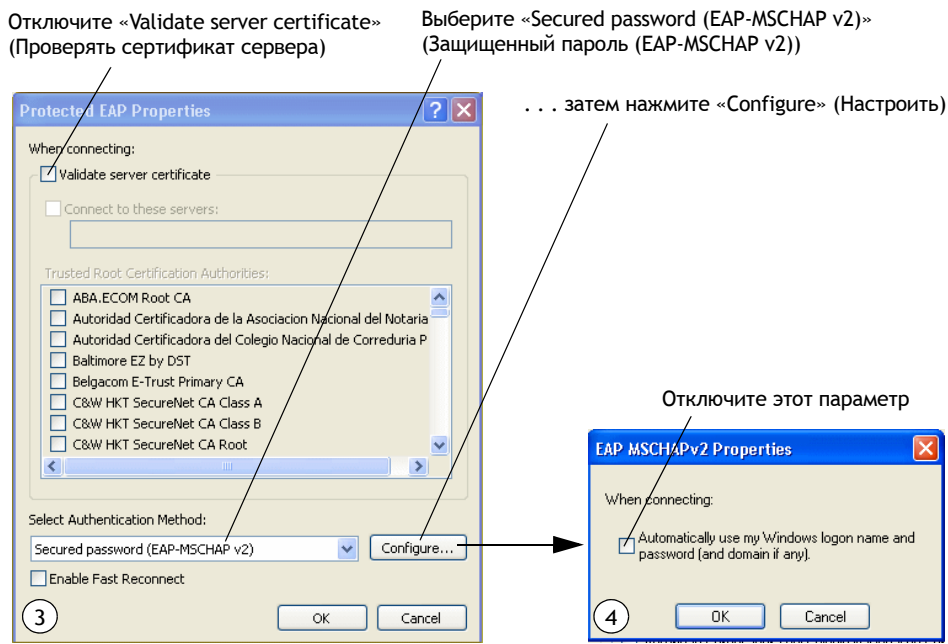
Если на беспроводном шлюзе 9160 G2 Wireless Gateway вы настроили режим безопасности WPA/WPA2 Enterprise (RADIUS) с использованием встроенного сервера аутентификации или внешнего RADIUS-сервера, работающего с протоколом EAP/PEAP. . .

| | |
|---|---|
| <ul style="list-style-type: none"> Basic Settings User Management Cluster Access Points Sessions Channel Management Wireless Neighborhood Security Status Interfaces Events Transmit/Receive Client Associations | <h3 style="text-align: center;">Modify Internal Network security settings</h3> <p> <input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation </p> <p> Mode: WPA Enterprise </p> <p> WPAVersions: <input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2 <input type="checkbox"/> Enable pre-authentication </p> <p> Cipher Suites: <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES) </p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <input checked="" type="checkbox"/> Use internal radius server </div> <p> Radius IP: 10.128.14.14 </p> <p> Radius Key: ●●●●●●●● </p> <p> <input checked="" type="checkbox"/> Enable radius accounting </p> <p style="text-align: right;"> Update </p> |
|---|---|

... сначала настройте учетные записи пользователей на точке доступа (перейдите на вкладку *User Management (Управление пользователями)*). ...

| Edit | Username | Real name | Status |
|------------------------|----------|------------------|---------|
| [Edit] | Darren | Darren Stevens | enabled |
| [Edit] | Samantha | Samantha Stevens | enabled |

... а затем настройте режим безопасности WPA с использованием аутентификации PEAP на каждом клиенте следующим образом.



1. Настройте следующие параметры на вкладках *Association* (Ассоциация) и *Authentication* (Аутентификация) диалогового окна *Network Properties* (Свойства сети).

Табл. В.10 Параметры ассоциации

| | |
|--|---|
| <i>Network Authentication</i> (Аутентификация сети) | WPA |
| <i>Data Encryption</i> (Шифрование данных) | <p>TKIP или AES, в зависимости от того, как этот параметр настроен на точке доступа.</p> <p>Примечание. Если на точке доступа значение «Cipher Suite» (Набор шифров) имеет значение Both (Все), клиенты с параметром шифрования TKIP и корректным ключом TKIP, а также клиенты с параметром шифрования AES и корректным ключом CCMP (AES), могут ассоциироваться с точкой доступа. Для получения дополнительной информации обратитесь к интерактивной справке на точке доступа.</p> |

2. Настройте этот параметр на вкладке *Authentication (Аутентификация)*.

Табл. В.11 Параметры аутентификации

| | |
|---------------------------|---|
| <i>EAP Type (Тип EAP)</i> | Выберите Protected EAP (PEAP) (Защищенный EAP (PEAP)). |
|---------------------------|---|

3. Нажмите **Properties** (Свойства) для открытия диалогового окна *Protected EAP Properties (Свойства протокола PEAP)* и настройте следующие параметры.

Табл. В.12 Параметры «Protected EAP Properties» (Свойства протокола PEAP)

| | |
|--|--|
| <i>Validate Server Certificate (Проверять сертификат сервера)</i> | Отключите этот параметр (снимите флажок). Примечание. Пример предполагает использование на точке доступа встроенного сервера аутентификации. Если вы настраиваете протокол EAP/PEAP на клиенте точки доступа, которая использует внешний RADIUS-сервер, для проверки сертификата выберите сертификат, соответствующий вашей инфраструктуре. |
| <i>Select Authentication Method (Выбрать метод аутентификации)</i> | Выберите Secured password (EAP-MSCHAP v2) (Защищенный пароль (EAP-MSCHAP v2)). |

4. Нажмите **Configure** (Настроить) для открытия диалогового окна *EAP MSCHAP v2 Properties (Свойства протокола EAP MSCHAP v2)*.

В диалоговом окне **отключите** (снимите флажок) параметр *Automatically use my Windows logon name (Автоматически использовать имя для входа в Windows)*. . . и так далее, чтобы при входе в систему требовался ввод имени пользователя и пароля.

Нажмите **ОК** во всех диалоговых окнах (начиная с окна *EAP MSCHAP v2 Properties (Свойства протокола EAP MSCHAP v2)*), чтобы закрыть их и сохранить изменения.

Вход в беспроводную сеть с клиента с режимом безопасности WPA/WPA2 Enterprise (RADIUS) PEAP

Теперь клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) PEAP смогут ассоциироваться с точкой доступа. Пользователям клиентских устройств будет предложено ввести имя пользователя и пароль для аутентификации в сети.

В.7.2 Клиенты с режимом безопасности WPA/WPA2 Enterprise (RADIUS) с использованием сертификата EAP-TLS

Расширяемый протокол аутентификации с защитой транспортного уровня (*Extensible Authentication Protocol (EAP) Transport Layer Security (TLS)*), или протокол EAP-TLS, — протокол аутентификации, поддерживающий использование смарт-карт и сертификатов. При наличии внешнего RADIUS-сервера, поддерживающего протокол EAP-TLS, вы можете использовать этот протокол в режимах WPA/WPA2 Enterprise (RADIUS) и IEEE 802.1x.



Примечание. Для использования режима IEEE 802.1x с сертификатами EAP-TLS для аутентификации и авторизации клиентских устройств необходимо наличие внешнего RADIUS-сервера и настроенного в сети сервера инфраструктуры для аутентификации с использованием открытого ключа (Public Key Authority Infrastructure, PKI), включая центр сертификации (CA). Описание настройки RADIUS-сервера, PKI и сервера центра сертификации не приводится в данном документе. Ознакомьтесь с соответствующей документацией к этим продуктам. Информацию об инфраструктуре открытого ключа Microsoft Windows PKI можно найти в этих статьях:

«How to Install/Uninstall a Public Key Certificate Authority for Windows 2000» (<http://support.microsoft.com/default.aspx?scid=kb;en-us:231881>) и

«How to Configure a Certificate Server»

(<http://support.microsoft.com/default.aspx?scid=kb;en-us:318710#3>).

Чтобы использовать этот режим безопасности, выполните следующие действия.

1. Добавить беспроводной шлюз 9160 G2 Wireless Gateway в список клиентов RADIUS-сервера. (См. «Настройка внешнего RADIUS-сервера для распознавания 9160 G2» на стр. В-37.)
2. Настройте беспроводной шлюз 9160 G2 Wireless Gateway для использования RADIUS-сервера (указав IP-адрес RADIUS-сервера при настройке параметров безопасности «WPA/WPA2 Enterprise [RADIUS]»).
3. На беспроводных клиентах настройте режим безопасности «WPA» и выберите значение «Smart Card or other Certificate» (Смарт-карта или другой сертификат), следуя инструкциям, приведенным в данном разделе.
4. Получите сертификат для клиента, выполнив действия, описанные в «Получение сертификата TLS-EAP для клиента» на стр. В-41.

Если вы настроили режим безопасности WPA/WPA2 Enterprise (RADIUS) с использованием внешнего RADIUS-сервера на беспроводном шлюзе 9160 G2 Wireless Gateway. . .

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: WPA Enterprise

WPA Versions: ☒ WPA ☒ WPA2

☐ Enable pre-authentication

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☒ Enable radius accounting

Update

. . . а затем настройте режим безопасности WPA с использованием аутентификации по сертификату на каждом клиенте следующим образом.

Выберите WPA

Выберите TKIP или AES в качестве режима шифрования данных

Выберите «Smart Card or other Certificate» (Смарт-карта или другой сертификат) и включите «Authenticate as computer ...» (Аутентификация в качестве компьютера...)

. . . затем нажмите Properties (Свойства)

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

1 OK Cancel

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☒ Enable IEEE 802.1x authentication for this network

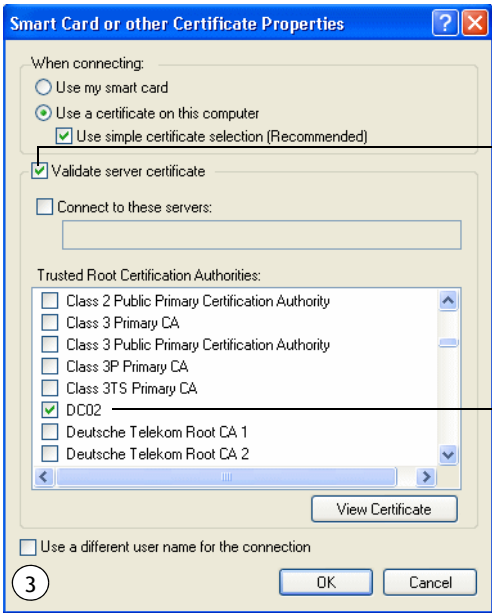
EAP type: Smart Card or other Certificate

Properties

☒ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

2 OK Cancel



Включите (установите флажок) «Validate server certificate» (Проверять сертификат сервера)

Выберите (установите флажок) имя сертификата на этом клиенте (предварительно загруженного с RADIUS-сервера)

1. Настройте следующие параметры на вкладке *Association (Ассоциация)* диалогового окна *Network Properties (Свойства сети)*.

Табл. В.13 Параметры ассоциации

| | |
|---|---|
| <i>Network Authentication (Аутентификация сети)</i> | WPA |
| <i>Data Encryption (Шифрование данных)</i> | TKIP или AES , в зависимости от того, как этот параметр настроен на точке доступа. Примечание. Если на точке доступа значение «Cipher Suite» (Набор шифров) имеет значение «Both» (Все), клиенты с параметром шифрования TKIP и корректным ключом TKIP, а также клиенты с параметром шифрования AES и корректным ключом CCMP (AES), могут ассоциироваться с точкой доступа. Для получения дополнительной информации обратитесь к интерактивной справке на точке доступа. |

2. Настройте эти параметры на вкладке *Authentication* (Аутентификация).

Табл. В.14 Параметры аутентификации

| | |
|--|---|
| <i>Enable IEEE 802.1x authentication for this network</i> (Включить аутентификацию IEEE 802.1x для этой сети) | Включите (установите флажок) этот параметр. |
| <i>EAP Type (Tun EAP)</i> | Выберите Smart Card or other Certificate (Смарт-карта или другой сертификат). |

3. Нажмите **Properties** (Свойства), чтобы открыть диалоговое окно *Smart Card or other Certificate Properties* (Свойства смарт-карты или другого сертификата), и включите параметр **Validate server certificate** (Проверить сертификат сервера).

Табл. В.15 Параметры «Smart Card Or Other Certificate Properties»
(Свойства смарт-карты или другого сертификата)

| | |
|--|---|
| <i>Validate Server Certificate</i> (Проверять сертификат сервера) | Включите этот параметр (установите флажок). |
| <i>Certificates (Сертификаты)</i> | В списке сертификатов выберите сертификат для данного клиента. |

Нажмите **ОК** во всех диалоговых окнах для их закрытия и сохранения изменений.

4. Для завершения настройки клиента теперь необходимо получить сертификат от RADIUS-сервера и установить его на клиентское устройство. Для получения информации о необходимых для этого действиях см. «Получение сертификата TLS-EAP для клиента» на стр. В-41.

Вход в беспроводную сеть на клиентском устройстве с режимом безопасности WPA с использованием сертификата

Теперь клиенты с режимом безопасности WPA могут подключаться к точке доступа, используя свои сертификаты TLS. Для подключения используется установленный сертификат, поэтому вводить данные о входе в систему не нужно. Сертификат автоматически отсылается RADIUS-серверу для аутентификации и авторизации.

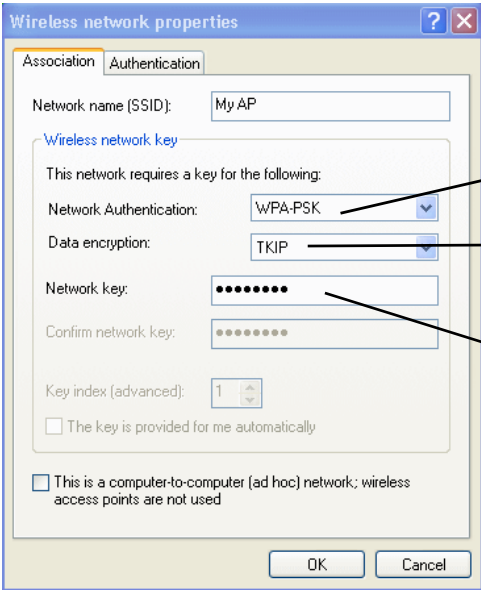
В.8 Настройка режима безопасности WPA/WPA2 Personal (PSK) на клиенте

Защищенный доступ к Wi-Fi (WPA) с предварительным ключом (PSK) входит в стандарт Wi-Fi Alliance IEEE 802.11i, который включает в себя *протокол шифрования с использованием временных ключей (TKIP)*, *улучшенный алгоритм шифрования (Advanced Encryption Algorithm, AES)* и *режим гаммирования/протокол CBC-MAC (CCMP)*. PSK использует предварительный ключ для начальной проверки учетных данных клиента.

Если вы настроили на беспроводном шлюзе 9160 G2 Wireless Gateway режим безопасности WPA/WPA2 Personal (PSK). . .

| | |
|-----------------------|--|
| Basic Settings | <div>Modify Internal Network security settings</div> <div><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</div> <div>Mode: WPA Personal ▾</div> <div>WPAVersions: <input checked="" type="checkbox"/> WPA <input type="checkbox"/> WPA2</div> <div>Cipher Suites: <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES)</div> <div>Key: reoreore</div> <div>Update</div> |
| User Management | |
| Cluster | |
| Access Points | |
| Sessions | |
| Channel Management | |
| Wireless Neighborhood | |
| Security | |
| Status | |

... настройте режим безопасности WPA/WPA2 Personal (PSK) на каждом клиенте следующим образом.



Выберите WPA-PSK.

Выберите TKIP или AES в качестве режима шифрования данных.

Введите сетевой ключ, соответствующий указанному на точке доступа (введите повторно для подтверждения).

Табл. В.16 Параметры ассоциации

| | |
|---|---|
| Network Authentication (Аутентификация сети) | WPA-PSK |
| Data Encryption (Шифрование данных) | <p>TKIP или AES, в зависимости от того, как этот параметр настроен на точке доступа.</p> <p>Примечание. Если на точке доступа значение «Cipher Suite» (Набор шифров) имеет значение Both (Все), клиенты с параметром шифрования TKIP и корректным ключом TKIP, а также клиенты с параметром шифрования AES и корректным ключом CCMP (AES), могут ассоциироваться с точкой доступа. Для получения дополнительной информации обратитесь к интерактивной справке на точке доступа.</p> |

Табл. В.16 Параметры ассоциации (Продолжение)

| | |
|--|---|
| <i>Network Key</i> (Сетевой ключ) | Укажите ключ, который вы установили при настройке параметров безопасности точки доступа для используемого набора шифров. Например, если на точке доступа установлено значение TKIP-ключа «012345678», введите это значение для сетевого ключа на клиенте с шифрованием TKIP. |
| <i>The key is provided for me automatically</i> (Ключ предоставляется автоматически) | Этот параметр должен быть отключен автоматически при настройке других параметров. |

Табл. В.17 Параметры аутентификации

| | |
|--|---|
| <i>Enable IEEE 802.1x authentication for this network</i> (Включить аутентификацию IEEE 802.1x для этой сети) | Убедитесь, что аутентификация IEEE 802.1x отключена (флажок должен быть снят). При выборе режима WEP-шифрования аутентификация отключается автоматически. |
|--|---|

Нажмите **ОК**, чтобы закрыть диалоговое окно Wireless Network Properties (Свойства беспроводной сети) и сохранить изменения.

Подключение к беспроводной сети клиента с режимом WPA-PSK

Теперь клиенты с установленным режимом WPA-PSK могут ассоциироваться с точкой доступа и проходить процесс аутентификации. На клиенте не требуется вводить ключ. При подключении автоматически используется ключ TKIP или AES, указанный в параметрах безопасности.

В.9 Настройка внешнего RADIUS-сервера для распознавания 9160 G2

Работающий в сети внешний *сервер службы идентификации удаленных пользователей* (RADIUS) может выдавать клиентам в *инфраструктуре открытых ключей* (PKI) смарт-карты и сертификаты EAP-TLS, а также выполнять настройку и аутентификацию учетных записей пользователей EAP-PEAP. Под *внешним RADIUS-сервером* подразумевается сервер аутентификации, внешний по отношению к точке доступа. Сетевой RADIUS-сервер и *встроенный сервер аутентификации* используются на беспроводном шлюзе 9160 G2 Wireless Gateway в разных сценариях.

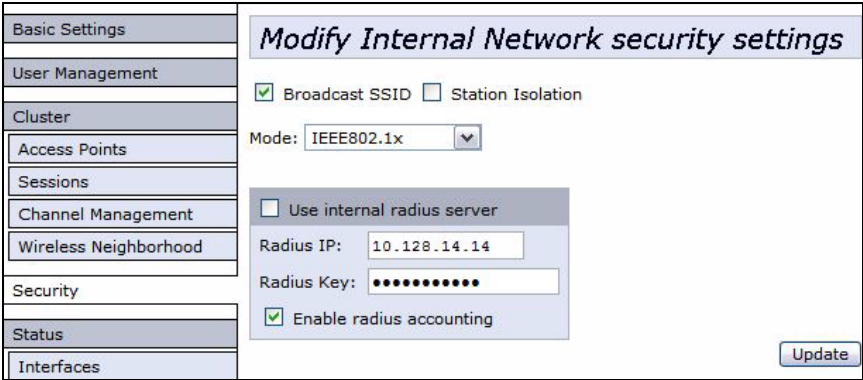
В данном разделе приводится пример настройки внешнего RADIUS-сервера для аутентификации и авторизации сертификатов TLS-EAP беспроводных клиентов беспроводного шлюза 9160 G2 Wireless Gateway, на котором настроен режим безопасности «WPA/WPA2 Enterprise (RADIUS)» или «IEEE 802.1x». Данный раздел содержит только общую информацию о процессе настройки, который будет отличаться в зависимости от того, какой RADIUS-сервер вы используете и как он настроен. В данном примере используется служба аутентификации в сети Интернет, входящая в сервер Microsoft Windows 2003.



Примечание. Этот документ не содержит описания настроек пользователя с правами администратора на RADIUS-сервере. В примере предполагается, что учетные записи пользователей RADIUS-сервера уже настроены. Вам понадобится имя пользователя и пароль для доступа к RADIUS-серверу для выполнения этих действий, а также для следующей процедуры — получения и установки сертификата на беспроводном клиенте. Чтобы настроить учетные записи пользователей, следуйте инструкциям, приведенным в документации к RADIUS-серверу.

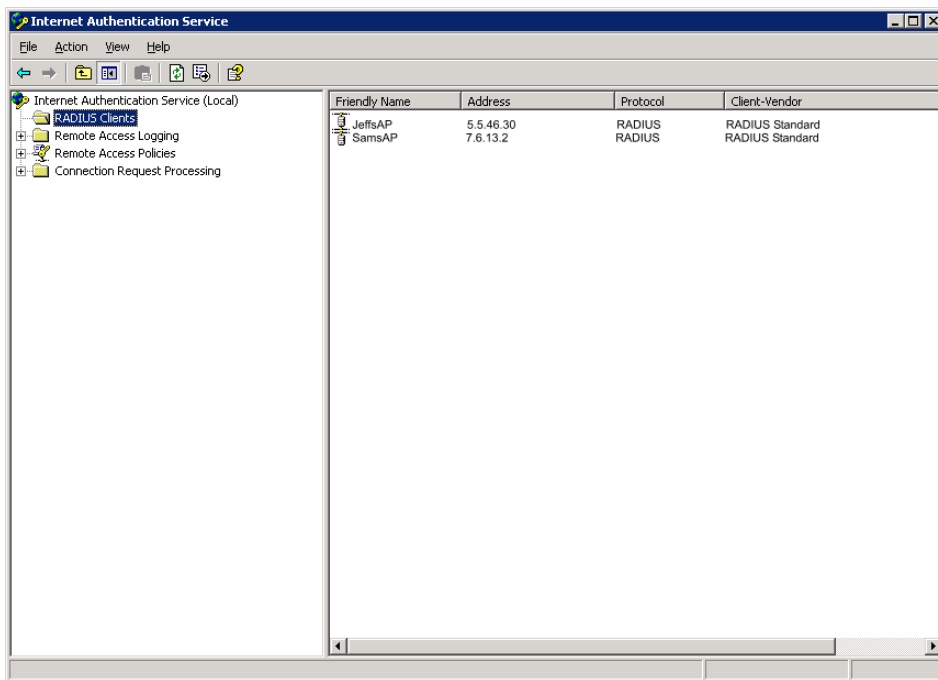
Целью этой процедуры является определение вашего беспроводного шлюза 9160 G2 Wireless Gateway как «клиента» RADIUS-сервера. После этого RADIUS-сервер может выполнять аутентификацию и авторизацию беспроводных клиентов для точки доступа. Необходимо выполнить эту процедуру настройки *на каждой точке доступа*. Если у вас есть несколько точек доступа, с которыми вы планируете использовать внешний RADIUS-сервер, необходимо выполнить эту процедуру для каждой точки доступа.

Помните, что информация о точке доступа, которую вам необходимо предоставить RADIUS-серверу, должна соответствовать параметрам на точке доступа (*Security (Безопасность)*) и наоборот. После того, как вы предоставили IP-адрес RADIUS-сервера точке доступа, предоставьте IP-адрес точки доступа RADIUS-серверу. Ключ RADIUS, указанный на точке доступа, является общим секретным ключом, который вы передадите RADIUS-серверу.



Примечание. RADIUS-сервер определяется по IP-адресу и номерам портов UDP для каждой предоставляемой им службы. В текущей версии беспроводного шлюза 9160 G2 Wireless Gateway порты протокола пользовательских датаграмм (UDP) RADIUS-сервера, используемые точкой доступа, являются ненастраиваемыми. В беспроводном шлюзе 9160 G2 Wireless Gateway порт UDP 1812 RADIUS-сервера жестко запрограммирован для использования в целях аутентификации, а порт 1813 — для ведения учета.

1. Войдите в систему, на которой размещен RADIUS-сервер, и вызовите службу аутентификации в сети Интернет.



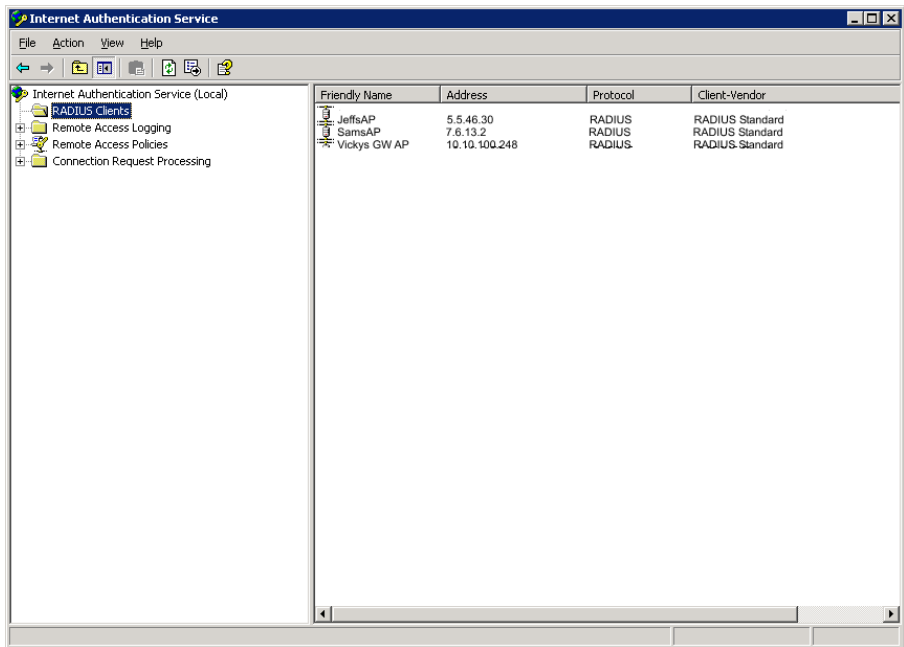
2. В левой панели щелкните правой кнопкой мыши на узле **RADIUS Clients** (Клиенты RADIUS) и выберите пункты всплывающего меню **New (Новый) > Radius Client** (Клиент Radius).
3. На первом экране мастера создания клиента *New RADIUS Client (Новый клиент RADIUS)* введите информацию о беспроводном шлюзе 9160 G2 Wireless Gateway, к которому должны подключиться клиенты:
 - Логическое (понятное) имя для точки доступа. (Можно использовать имя DNS или местоположение.)
 - IP-адрес для точки доступа. Нажмите «Next» (Далее).

The screenshot shows the 'New RADIUS Client' dialog box with the 'Name and Address' tab selected. The dialog has a title bar with a close button. Below the title bar is a section labeled 'Name and Address'. It contains a text box for 'Friendly name' with the value 'Vickys GW AP' and a text box for 'Client address (IP or DNS):' with the value '10.10.100.248'. There is a 'Verify...' button next to the client address field. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

4. В поле *Shared secret* (*Общий секретный ключ*) введите значение **RADIUS Key** (Ключ RADIUS), указанное на точке доступа (на экране *Security* (*Безопасность*)). Повторно введите ключ для подтверждения.

The screenshot shows the 'New RADIUS Client' dialog box with the 'Additional Information' tab selected. The dialog has a title bar with a close button. Below the title bar is a section labeled 'Additional Information'. It contains a text box for 'Client-Vendor:' with a dropdown menu showing 'RADIUS Standard'. Below this are two text boxes for 'Shared secret:' and 'Confirm shared secret:', both containing masked text (asterisks). At the bottom of the dialog is a checkbox labeled 'Request must contain the Message Authenticator attribute' which is unchecked. At the bottom of the dialog are three buttons: '< Back', 'Finish', and 'Cancel'.

5. Нажмите «**Finish**» (Готово). Теперь точка доступа отображается как клиент сервера аутентификации.



В.10 Получение сертификата TLS-EAP для клиента



Примечание. Для использования режима IEEE 802.1x с сертификатами EAP-TLS для аутентификации и авторизации клиентских устройств необходимо наличие внешнего RADIUS-сервера и настроенного в сети сервера инфраструктуры для аутентификации с использованием открытого ключа (Public Key Authority Infrastructure, PKI), включая центр сертификации (CA). Описание настройки RADIUS-сервера, PKI и сервера центра сертификации не приводится в данном документе. Ознакомьтесь с соответствующей документацией к этим продуктам. Информацию об инфраструктуре открытого ключа Microsoft Windows PKI можно найти в этих статьях:

«How to Install/Uninstall a Public Key Certificate Authority for Windows 2000» <http://support.microsoft.com/default.aspx?scid=kb:EN-US:231881> и

«How to Configure a Certificate Server»

(<http://support.microsoft.com/default.aspx?scid=kb:en-us:318710#3>).

Беспроводные клиенты, которые работают в режиме безопасности «WPA/WPA2 Enterprise (RADIUS)» или «IEEE 802.1x» с использованием внешнего RADIUS-сервера, поддерживающего сертификаты TLS-EAP, должны получить сертификат TLS от RADIUS-сервера.

Это однократное действие, которое необходимо выполнить на каждом клиенте, работающем в одном из этих режимов безопасности с использованием сертификатов. В данном примере используется сервер сертификатов Microsoft Certificate Server.

Чтобы получить сертификат для клиента, выполните следующие действия.

1. В веб-браузере перейдите по следующему URL-адресу:

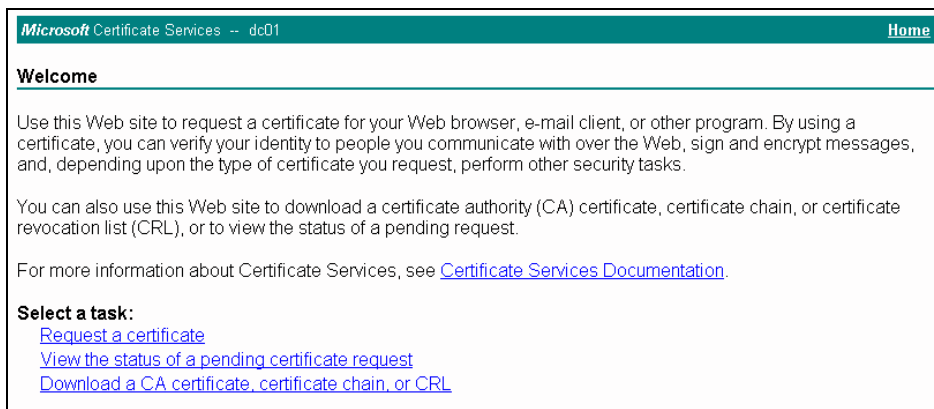
<https://IPAddressOfServer/certsrv/>

Где *IPAddressOfServer* — это IP-адрес внешнего RADIUS-сервера или *центра сертификации (CA)*, в зависимости от конфигурации инфраструктуры.

2. Нажмите **Yes** (Да) для перехода на защищенную веб-страницу сервера.



В браузере отобразится экран приветствия сервера сертификатов.



3. Нажмите **Request a certificate** (Запросить сертификат) для получения приглашения на вход в систему RADIUS-сервера.
4. Укажите корректные значения **имени пользователя** и **пароля** для получения доступа к RADIUS-серверу.

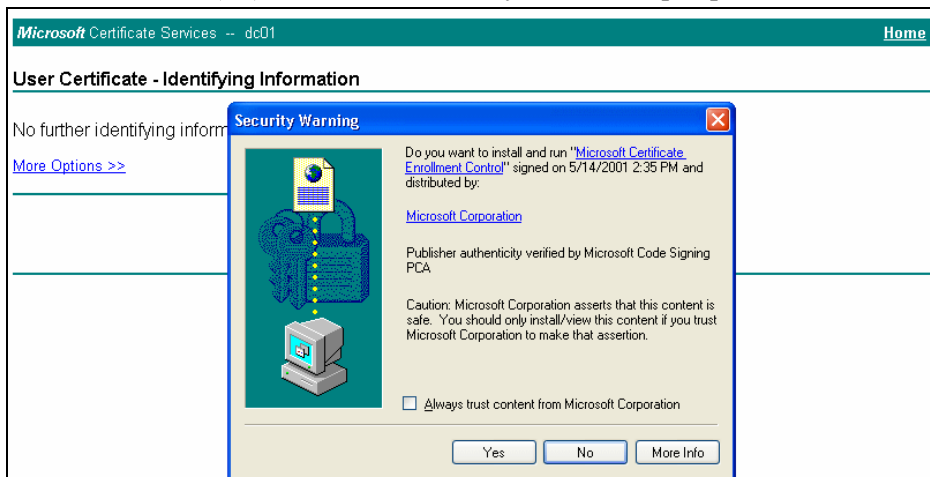


Примечание. Имя пользователя и пароль, которые необходимо здесь указать, предназначены для получения доступа к RADIUS-серверу, для которого вы уже настроили учетные записи пользователей. Этот документ не содержит описания настроек учетных записей пользователей с правами администратора на RADIUS-сервере. Для выполнения этих действий ознакомьтесь с соответствующей документацией о RADIUS-сервере.

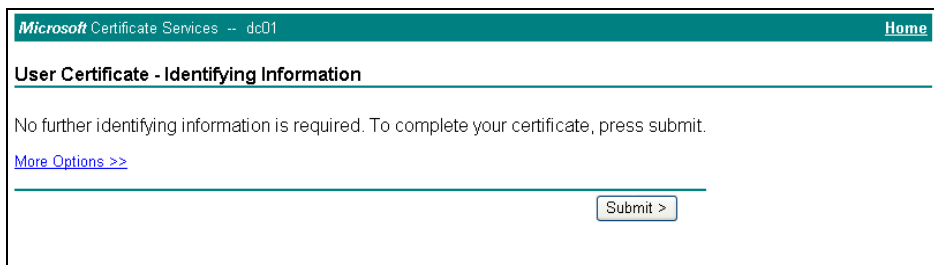
5. Нажмите **User Certificate** (Пользовательский сертификат) на следующей странице.



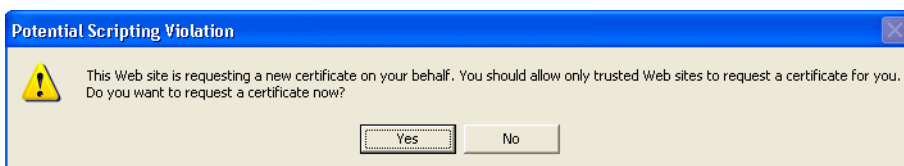
6. Нажмите **Yes (Да)** в диалоговом окне установки сертификата.



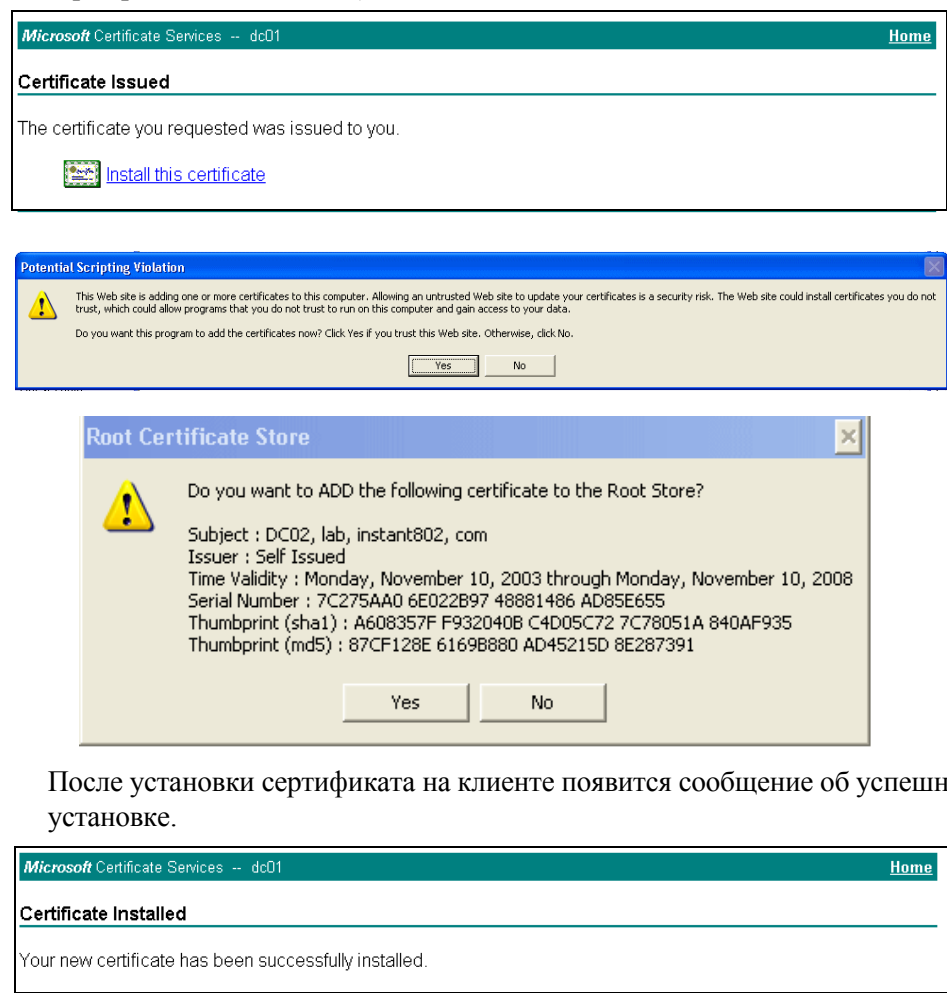
7. Нажмите **Submit** (Отправить) для завершения процедуры, а затем нажмите **Yes** (Да) для подтверждения отправки в появившемся диалоговом окне.



The screenshot shows a web browser window with the title bar "Microsoft Certificate Services -- dc01" and a "Home" link in the top right corner. The main content area is titled "User Certificate - Identifying Information". Below the title, it states: "No further identifying information is required. To complete your certificate, press submit." There is a blue hyperlink "More Options >>" and a "Submit >" button at the bottom right of the form area.



8. Нажмите **Install this certificate** (Установить этот сертификат) для установки нового сертификата на клиентскую станцию. (Также нажмите **Yes** (Да) в появившихся диалоговых окнах для подтверждения установки и добавления сертификата в Root Store.)



После установки сертификата на клиенте появится сообщение об успешной установке.

В.11 Настройка RADIUS-сервера для тегов VLAN

Виртуальная локальная сеть (VLAN) — это группировка портов на одном или нескольких коммутаторах. С помощью динамических VLAN вы можете назначить пользователя VLAN, и коммутаторы динамически используют эту информацию для автоматической настройки портов на коммутаторе.

Выбор VLAN обычно зависит от идентификации пользователя. RADIUS-сервер сообщает NAS (например, точке доступа) о выбранном VLAN в процессе аутентификации. При такой настройке пользователи динамических VLAN могут менять свое местоположение без вмешательства и необходимости внесения изменений на коммутаторах.

При использовании беспроводного шлюза 9160 G2 Wireless Gateway, если пользователь использует внешний RADIUS-сервер (настроенный на экране *Security (Безопасность)*), аутентификация пользователя будет выполняться с помощью внешнего RADIUS-сервера. Учетные данные пользователя для аутентификации передаются RADIUS-серверу. Если учетные данные после проверки найдены корректными, NAS настраивает порт для VLAN, указанного сервером аутентификации RADIUS.

В.11.1 Настройка RADIUS-сервера

На RADIUS-сервере необходимо настроить атрибуты туннеля («Tunnel») в сообщениях разрешения доступа («Access-Accept»), для того чтобы сообщать точке доступа о выбранном VLAN. Эти атрибуты определяются в RFC 2868, а их использование в динамических VLAN — в RFC 3580.

При использовании сервера FreeRADIUS для добавления необходимых атрибутов можно указать следующие параметры в файле пользователя.

```
example-user  Auth-Type :=EAP, User-Password == "password"  
              Tunnel-Type = 13,  
              Tunnel-Medium-Type = 6,  
              Tunnel-Private-Group-ID = 7
```

«Tunnel-Type» и «Tunnel-Medium-Type» имеют одинаковые значения для всех станций. Tunnel-Private-Group-ID — это идентификатор выбранной VLAN, который может отличаться для каждого пользователя.

ПРИЛОЖЕНИЕ С

ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

| | |
|---|----|
| С.1 Устранение проблем, связанных с распределенной беспроводной системой (WDS). | 51 |
| С.2 Восстановление кластера | 52 |
| С.2.1 Перезагрузка или сброс настроек точки доступа | 52 |

В этом разделе приведена информация о решении основных проблем, которые могут возникать при обновлении конфигураций в сетях, обслуживаемых несколькими точками доступа, объединенными в кластеры.

С.1 Устранение проблем, связанных с распределенной беспроводной системой (WDS)

Если у вас возникли проблемы с настройкой соединения WDS, внимательно прочтите примечания и предостережения в разделе «Настройка параметров WDS» на стр. 235. Для удобства эти примечания также приведены здесь. Основная проблема, с которой сталкиваются администраторы при настройке WDS, заключается в том, что они забывают настроить обе точки доступа, между которыми устанавливается соединение, на один радиоканал и режим IEEE 802.11. Эти и другие предварительные настройки описаны в примечаниях ниже.



Примечания.

*При использовании WDS необходимо настроить параметры WDS на **обеих** точках доступа, участвующих в соединении WDS.*

Между любой парой точек доступа можно установить только одно соединение WDS. Это означает, что удаленный MAC-адрес указывается в настройках WDS конкретной точки доступа только один раз.

Обе точки доступа, участвующие в соединении WDS, должны работать на одном и том же радиоканале и в одном и том же режиме IEEE 802.11. Информацию о настройке режима радиомодуля и канала см. в разделе «Настройка параметров радиомодуля» на стр. 187. Дополнительную информацию о стандарте IEEE 802.11h см. в разделе «Управление регулятивным доменом 802.11h» на стр. 163.

Убедитесь, что включен протокол связующего дерева (Spanning Tree Protocol, STP). Это позволит предотвратить бесконечные циклы и избыточность путей при использовании мостовых соединений WDS либо комбинаций проводных соединений (Ethernet) и мостов WDS. Если протокол STP включен, WDS можно использовать для создания резервных соединений. Если протокол STP отключен, обратите внимание на следующие правила.

- Любые две точки доступа могут быть соединены одним каналом; это может быть либо мост WDS (беспроводное соединение) либо подключение Ethernet (проводное), но не оба этих соединения одновременно.
- Не создавайте «резервные» соединения.
- Если возможна трассировка нескольких путей между любой парой точек доступа в любой комбинации соединений Ethernet или WDS, это указывает на наличие петли.
- Расширить или соединить мостом можно либо внутреннюю, либо гостевую сеть, но не обе эти сети одновременно.

С.2 Восстановление кластера

В случаях, когда возникает рассинхронизация точек доступа в кластере либо становится невозможным присоединение точек доступа к кластеру или их удаление из кластера, рекомендуется выполнить восстановление кластера одним из следующих способов.

С.2.1 Перезагрузка или сброс настроек точки доступа

Способы восстановления приведены в порядке их рекомендуемого использования. Во всех случаях, кроме последнего (остановка кластера), достаточно выполнить сброс настроек или перезагрузку точки доступа, конфигурация которой не синхронизирована с другими устройствами в кластере. То же самое относится к случаям, когда точку доступа невозможно присоединить к кластеру или удалить из него.

- Выполните физическую перезагрузку точки доступа, отключив и снова включив питание (нажмите на кнопку питания, чтобы выключить устройство, затем нажмите кнопку питания еще раз, чтобы включить его).
- Сбросьте настройки точки доступа с помощью интерфейса администрирования. Для этого перейдите по адресу <http://IPAddressOfAccessPoint>, затем перейдите в раздел **Reset Configuration** (Сброс конфигурации) и нажмите кнопку **Reset** (Сброс). IP-адреса точек доступа указаны на экране **Cluster** (Кластер) > **Access Points** (Точки доступа) для всех устройств в кластере.

ПРИЛОЖЕНИЕ D

ГЛОССАРИЙ

*0-9 A B C D E H I L M N O P Q R S T U V W X Б Д З И К М
О П Р С Т Ш*

0-9

802

IEEE 802 (IEEE Std. 802-2001) — семейство стандартов одноранговой связи по *LAN*. Эти технологии используют общую среду для широковещательной передачи информации всем станциям. Основной принцип передачи информации — на основе пакетов. Основная единица передачи данных — последовательность октетов данных (8-битных), размер которых может быть любым в зависимости от типа *LAN*.

В семейство стандартов *IEEE 802* входят определения протоколов преобразования данных, управления и безопасности.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) — это стандарт для пакетов *EAP* по беспроводной сети *802,11* с использованием протокола *передачи EAP-сообщений в стандарте 802.1x* (EAP Encapsulation Over LANs, EAPOL). Он создает инфраструктуру, поддерживающую несколько методов аутентификации.

IEEE 802.1x выполняет аутентификацию пользователей, а не компьютеров.

802.2

IEEE 802.2 (*IEEE Std. 802.2.1998*) определяет уровень *LLC* для семейства стандартов *802*.

802,3

IEEE 802,3 (IEEE Std. 802.3-2002) определяет уровень **MAC** для сетей, использующих **CSMA/CA**. **Ethernet** — пример такой сети.

802,11

IEEE 802,11 (IEEE Std. 802.11-1999) — спецификация управления доступом к среде передачи (**MAC**) и физического уровня (**PHY**) для беспроводных подключений для фиксированных, переносных и перемещающихся станций в границах зоны покрытия. Стандарт использует расширенный спектр с перестройкой частоты с применением прямой последовательности (DSSS) в промышленном, научном и медицинском диапазоне (ISM) на частоте 2,4 ГГц и поддерживает максимальные физические скорости передачи данных — 1 и 2 Мбит/с. Формально он был принят в 1997 году, но большей частью был вытеснен стандартом **802.11b**.

Стандарт IEEE 802.11 также используется главным образом для обозначения семейства стандартов **IEEE** для беспроводных локальных сетей.

802.11a

IEEE 802.11a (IEEE Std. 802.11a-1999) — стандарт физического уровня (**PHY**), определяющий работу на диапазоне частот U-NII 5 ГГц с использованием мультиплексирования с ортогональным делением частот (OFDM). Поддерживает скорости передачи данных от 6 до 54 Мбит/с.

802.11a Turbo

IEEE 802.11a Turbo — проприетарный вариант стандарта **802.11a** от компании Atheros Communications. Поддерживает увеличенные скорости передачи данных от 6 до 108 Мбит/с. Atheros Turbo 5 ГГц — режим IEEE 802.11a Turbo. Atheros Turbo 2,4 ГГц — режим IEEE 802.11g Turbo.

802.11b

IEEE 802.11b (*IEEE Std. 802.11b-1999*) — улучшенный первоначальный стандарт **802,11 PHY**, включающий скорости передачи данных 5,5 Мбит/с и 11 Мбит/с. Он использует расширенный спектр с перестройкой частоты с применением прямой последовательности (DSSS) или расширенный спектр со скачкообразной перестройкой частоты (FHSS) в промышленном, научном и медицинском диапазоне (ISM) на частоте 2,4 ГГц, а также кодирование с использованием дополняющих кодов (ССК) для обеспечения высоких скоростей передачи данных. Он поддерживает скорости передачи данных от 1 до 11 Мбит/с.

802.11d

IEEE 802.11d позволяет применять стандартные правила функционирования беспроводных сетей IEEE 802.11 в любой стране без необходимости изменения конфигурации. Описаны следующие требования к физическому уровню (PHY): таблицы скачкообразной перестройки частоты, допустимые каналы и уровни мощности для каждой страны. При включении поддержки стандарта IEEE 802.11d на точке доступа в маячки точки доступа будет добавляться информация о стране, в которой она находится. Эта информация используется клиентскими станциями. Это особенно важно для работы точки доступа IEEE 802.11a на частоте 5 ГГц, так как использование этих частот сильно отличается в разных странах.

802.11e

IEEE 802.11e — разрабатываемый стандарт *IEEE* для улучшенной работы *MAC* и поддержки *QoS*. Использует механизм приоритизации трафика в **802,11**. Стандарт описывает разрешенные изменения в межкадровом пространстве арбитража, минимальный и максимальный размер окна коллизий и максимальную длину (в μsec) пакета данных.

IEEE 802.11e является проектом стандарта *IEEE* (последняя версия по состоянию на июль 2003 г. — D5.0). Доступная в настоящее время разновидность 802.11e — стандарт *Wireless Multimedia Enhancements (WMM)*.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) — стандарт, определяющий протокол обмена данными между точками доступа (**IAPP**) для точек доступа (беспроводных концентраторов) в режиме расширенного набора служб (**ESS**). Стандарт определяет, как точки доступа обмениваются информацией об ассоциациях и реассоциациях своих мобильных станций.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) — высокоскоростное (до 54 Мбит/с) расширение стандарта **802.11b PHY** для диапазона частот 2,4 ГГц. Использует мультиплексирование с ортогональным делением частот (OFDM). Поддерживает скорости передачи данных от 1 до 54 Мбит/с.

802.11h

IEEE 802.11h — стандарт, используемый для разрешения проблемы возникновения помех, присущей стандарту 802.11a. Для снижения уровня помех в стандарте 802.11h используются две схемы: регулировка уровня передачи (TPC) и динамический выбор частоты (DFS). DFS обнаруживает другие точки доступа, работающие на одной частоте, и перенаправляет их на другой канал. TPC снижает выходную мощность частоты сети точки доступа, устраняя возможность помех. Этот стандарт является рекомендованным для использования в Европе, Японии и США.

802.11i

IEEE 802.11i — универсальный стандарт *IEEE* для обеспечения безопасности в беспроводной локальной сети (**WLAN**), описывающий защищенный доступ Wi-Fi (**Wi-Fi Protected Access 2, WPA2**). Он содержит улучшения уровня **MAC**, компенсируя слабые стороны **WEP**. Стандарт включает более надежные алгоритмы шифрования по сравнению с оригинальным стандартом **Wi-Fi Protected Access (WPA)**, такие как улучшенный стандарт шифрования (**AES**).

Оригинальный **WPA**, который может считаться разновидностью стандарта 802.11i, для шифрования использует *протокол целостности временного ключа (TKIP)*. WPA2 имеет обратную совместимость с продуктами, которые поддерживают оригинальный WPA.

IEEE 802.11i / WPA2 был завершен и ратифицирован в июне 2004 г.

802.11j

IEEE 802.11j устанавливает стандарты процессоров, которые могут использовать диапазоны радиочастот 4,9 и 5 ГГц в соответствии с правилами, установленными правительством Японии для открытия этих радиочастот для использования в приложениях внутренних, внешних и мобильных беспроводных локальных сетей. В соответствии с правилами, компании должны регулировать ширину этих каналов. Благодаря стандарту IEEE 802.11j беспроводные устройства могут работать на некоторых ранее недоступных каналах, пользуясь преимуществами новых частот и режимов работы. Отчасти это попытка снизить нагрузку на радиоволны, что имеет косвенное отношение к стандарту IEEE 802.11h.

802.11k

IEEE 802.11k — разрабатываемый стандарт *IEEE* для беспроводных сетей (*WLAN*), с помощью которого выполняется автоматическое управление выбором сетевого канала (*Канал*), роумингом клиента (*Роуминг*) и использованием точки доступа (*Точка доступа*). В сетях с возможностью использования стандарта 802.11k выполняется автоматическая балансировка нагрузки сетевого трафика между точками доступа для улучшения производительности сети и предотвращения неполного или чрезмерного использования точек доступа. В перспективе стандарт 802.11k дополнит стандарт *802.11e* и качество обслуживания (*QoS*), обеспечив QoS для передачи мультимедиа по радиоканалу.

802.1p

802.1p является расширением стандарта IEEE 802 и регулирует обеспечение QoS. Основная задача стандарта 802.1p — приоритизация сетевого трафика на канальном уровне/уровне MAC. 802.1p предоставляет возможность отфильтровывать многоадресный трафик, чтобы он не выходил за пределы коммутируемых сетей уровня 2. В качестве схемы приоритизации используются кадры тегов.

Для обеспечения соответствия этому стандарту коммутаторы уровня 2 должны иметь возможность группировать входящие пакеты LAN в отдельные классы данных.

802.1Q

IEEE 802.1Q — стандарт *IEEE* для виртуальных локальных сетей (*VLAN*), предназначенный для беспроводных технологий.
(См. <http://www.ieee802.org/1/pages/802.1Q.html>.)

Стандарт описывает проблему разделения больших сетей на меньшие части в целях предотвращения использования широковещательным и многоадресным трафиком данных большей полосы пропускания, чем это необходимо. Кроме того, стандарт 802.11Q обеспечивает лучшую защиту сегментов внутренних сетей. Спецификация 802.1Q предусматривает использование стандартного метода для добавления информации о членах VLAN в кадры Ethernet.

A

AES

Усовершенствованный стандарт шифрования (AES) — симметричный 128-разрядный алгоритм блочного шифрования, разработанный для использования вместо шифрования DES. AES одновременно работает на нескольких уровнях сети.

Дополнительная информация доступна на [веб-сайте NIST](#).

Atheros XR (расширенный диапазон)

Расширенный диапазон Atheros (XR) — это коммерческая реализация метода низкоскоростной передачи трафика на большие расстояния. Этот метод доступен для клиентов и точек доступа с поддержкой XR, а также совместим со стандартом 802.11 в режимах 802.11g и 802.11a. Поддержка Atheros XR, Atheros Turbo 5 ГГц и Atheros Dynamic Turbo 5 ГГц, в режиме 802.11b не реализована.

B

BSS

Базовый набор служб (BSS) — *Инфраструктура беспроводной сети* в режиме инфраструктуры (см. *Режим инфраструктуры*) с одной точкой доступа. См. также расширенный набор служб (*ESS*) и независимый базовый набор служб (*IBSS*).

BSSID

В режиме инфраструктуры (см. *Режим инфраструктуры*) идентификатор базового набора служб (BSSID) — это 48-разрядный *MAC*-адрес беспроводного интерфейса точки доступа (см. *Точка доступа*).

С

CCMP

Режим гаммирования/протокол CBC-MAC (CCMP) — метод шифрования для стандарта **802.11h**, использующий *AES*. Он использует режим *CCM*, объединяя блочную передачу зашифрованного текста/режим гаммирования (CBC-CTR) и блочную передачу зашифрованного текста/код аутентификации сообщения (CBC-MAC) для шифрования данных и сохранения целостности сообщений.

Для работы AES-CCMP необходимо наличие специализированного процессора.

CGI

Общий интерфейс шлюза (CGI) — стандарт запуска внешних программ с сервера *HTTP*. Определяет процесс передачи аргументов выполняющей программе как часть запроса *HTTP*. Также может определять набор переменных среды.

Программа CGI — обычный способ динамического взаимодействия сервера *HTTP* с пользователями. Например, страница HTML, содержащая форму, может использовать программу CGI для обработки данных формы после ее отправки.

CSMA/CA

Многостанционный доступ с контролем несущей и предотвращением конфликтов (CSMA/CA) — сетевой протокол разрешения конфликтов нижнего уровня. Станция прослушивает канал и начинает передачу пакета, если канал свободен. Когда станция определяет, что канал не занят, она передает пакет. Если обнаруживается, что канал занят, станция приостанавливает передачу на произвольный период времени и затем снова пытается получить доступ к каналу.

Протокол CSMA/CA является основным в работе функции распределенного управления (*DCF*) стандарта IEEE 802.11e. См. также *RTS* и *CTS*.

Протокол CSMA/CA, используемый в сетях **802.11**, является разновидностью протокола CSMA/CD (используемого в сетях *Ethernet*). Протокол CSMA/CD сосредоточен на *обнаружении* коллизий, в то время как протокол CSMA/CA — на их *предотвращении*.

CTS

Сообщение разрешения на передачу данных (*clear to send*, CTS) — это сигнал, отправляемый клиентской станцией **IEEE 802.11** в ответ на сообщение запроса на передачу данных (*request to send*, **RTS**). Сообщение CTS означает, что канал свободен для того, чтобы отправитель сообщения RTS смог начать передачу данных. Другие станции будут ожидать окончания передачи. Сообщение является частью протокола **CSMA/CA** стандарта IEEE 802.11. См. также **RTS**.

D

DCF

Функция распределенного управления является компонентом технологии качества обслуживания (QoS) стандарта IEEE 802.11e. Функция DCF координирует доступ к каналу для станций беспроводной сети, управляя временем ожидания для доступа к каналу. Время ожидания определяется таймером случайной задержки, который настраивается путем определения минимального и максимального окна коллизии. См. также **EDCF**.

DHCP

Протокол динамического конфигурирования хоста (DHCP) определяет способ, используемый центральным сервером для динамического предоставления данных о сетевой конфигурации клиентам. Сервер DHCP «предлагает аренду» клиентским системам (на определенный период времени, см. **Срок аренды**). Предоставляемые данные включают в себя IP-адреса и маски сети, а также адреса серверов **DNS** и шлюза (см. **Шлюз**).

DNS

Служба доменных имен (DNS) — это универсальная служба запросов, используемая для перевода *полных квалификационных имен* в адреса Интернет. Полное квалификационное имя состоит из имени хоста системы и ее доменного имени. Например, **www** — имя хоста веб-сервера, а **www.pSIONteklogix.com** — полное квалификационное имя этого сервера. DNS переводит доменное имя **www.pSIONteklogix.com** в IP-адрес, например 66.93.138.219.

Доменное имя может иметь один или несколько IP-адресов. В свою очередь, IP-адрес может быть сопоставлен с несколькими доменными именами.

Доменное имя имеет суффикс, который показывает, какому *домену верхнего уровня* (TLD) он принадлежит. У каждой страны есть свой домен верхнего уровня, например, .de — Германия, .fr — Франция, .jp — Япония, .tw — Тайвань, .uk — Великобритания, .us — США и т.д. Существует также домен .com для коммерческих организаций, .edu для образовательных учреждений, .net для сетевых операторов, .org для прочих организаций, а также .gov для правительства США и .mil для вооруженных сил США.

DOM

Объектная модель документов (DOM) — это интерфейс, предоставляющий программам и сценариям динамический доступ к содержимому, структуре и стилю документов и возможность их обновления. DOM позволяет моделировать объекты в документах HTML и XML (текст, ссылки, изображения, таблицы), определяя атрибуты каждого объекта и способ управления ими.

Для получения дополнительной информации об объектной модели документов перейдите на веб-сайт [W3C](#).

DTIM

Схема данных о доставке трафика (DTIM) — сообщение, являющееся элементом некоторых кадров маячка (см. *Маячок*). Эта схема определяет, для каких станций, находящихся в данный момент в режиме пониженного энергопотребления, на точке доступа (см. *Точка доступа*) имеются буферизированные данные, ожидающие приема. Часть DTIM-сообщения указывает, как часто станции должны проверять наличие буферизованных данных.

E

EAP

Расширяемый протокол аутентификации (EAP) — протокол аутентификации, поддерживающий несколько методов: маркер-карты, Kerberos, одноразовые пароли, сертификаты, аутентификация с использованием открытого ключа и смарт-карты.

Разновидности EAP включают следующие протоколы: EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS и EAP Tunnelled TLS (EAP-TTLS).

EDCF

Функция расширенного распределенного управления — это расширение **DCF**. В качестве компонента стандарта IEEE Wireless Multimedia (WMM) EDCF обеспечивает приоритетный доступ к беспроводной среде.

ERP

Протокол Extended Rate Protocol используется станциями **IEEE 802.11g** (со скоростью передачи данных более 20 Мбит/с на частоте 2,4 ГГц) совместно с мультиплексированием с ортогональным частотным разделением каналов (OFDM). В протоколе ERP и стандарте IEEE **802.11g** используется схема эффективного взаимодействия станций IEEE 802.11g с узлами IEEE 802.11b на одном канале.

Устаревшие устройства с режимом IEEE 802.11b не могут обнаружить сигналы ERP-OFDM, используемые станциями IEEE 802.11g, что может привести к коллизии кадров данных станций IEEE 802.11b и IEEE 802.11g.

Если на одном канале присутствуют узлы 802.11b и 802.11g, станции IEEE 802.11g обнаруживают это посредством флага ERP на точке доступа и включают защиту с помощью *запросов на передачу (RTS)* и *разрешений на передачу (CTS)* перед отправлением данных.

См. также протокол **CSMA/CA**.

ESS

Расширенный набор служб (ESS) — **Инфраструктура беспроводной сети** в режиме инфраструктуры (см. *Режим инфраструктуры*) с несколькими точками доступа, формирующими единую подсеть, которая может поддерживать большее количество клиентов, чем базовый набор служб (**BSS**). Каждая точка доступа поддерживает некоторое количество беспроводных станций, предоставляя расширенную зону покрытия, например для офиса.

Ethernet

Ethernet — архитектура локальной сети (*LAN*), поддерживающая скорости передачи данных от 10 Мбит/с до 1 Гбит/с. Спецификация Ethernet является основой стандарта **IEEE 802,3**, определяющей физический уровень и нижний уровень программного обеспечения. Для обработки совмещенной нагрузки используется способ доступа **CSMA/CA**.

Ethernet поддерживает скорость 10 Мбит/с, *Fast Ethernet* — 100 Мбит/с, а *Gigabit Ethernet* — 1 Гбит/с. Кабели классифицируются как «*XbaseY*», где *X* — это скорость передачи данных в Мбит/с, а *Y* — категория кабеля. Оригинальный кабель: *10base5* (толстый коаксиальный или «желтый» кабель). Другие кабели — *10base2* (тонкий кабель), *10baseT* (витая пара) и *100baseT* (Fast Ethernet). Два последних варианта обычно поставляются с кабелем *CAT5* с разъемами *RJ-45*. Также существует кабель *1000baseT* (Gigabit Ethernet).

H

HTML

Язык гипертекстовой разметки (HTML) определяет структуру документа в Интернете. В этом языке используются теги и атрибуты для создания макета документа.

Документ HTML начинается с тега <html> и заканчивается тегом </html>. Правильно оформленный документ также имеет раздел <head> ... </head>, в котором содержатся метаданные документа, и раздел <body> ... </body> с содержимым документа. Разметка HTML основана на *стандартном языке обобщенной разметки документов (SGML)*.

Документы HTML отправляются сервером браузеру по протоколу **HTTP**. См. также **XML**.

HTTP

Протокол передачи гипертекстовых файлов (HTTP) определяет формат и передачу сообщений по Интернету. Сообщение HTTP состоит из **URL**-адреса и команды (GET, HEAD, POST и т.д.), за запросом следует ответ.

HTTPS

Протокол защищенной пересылки гипертекста (HTTPS) — защищенная версия протокола HTTP, протокол связи по Интернету. Протокол HTTPS встроен в браузер. При использовании протокола HTTPS в нижнем углу страницы браузера появляется значок закрытого замка.

Данные, передаваемые по протоколу HTTPS, зашифровываются, что обеспечивает их безопасную передачу.

I

IAPP

Протокол обмена служебной информацией между точками доступа (IAPP) — это стандарт IEEE (802.11f), определяющий тип связи между точками доступа в «системе распределения». Сюда относится обмен информацией о мобильных станциях и обслуживание таблиц переадресации моста, а также защита каналов связи между точками доступа.

IBSS

*Независимый базовый набор служб (IBSS) — Инфраструктура беспроводной сети в режиме прямого подключения (см. *Режим прямого подключения*), в котором станции взаимодействуют друг с другом напрямую.*

IEEE

Институт инженеров по электротехнике и электронике (IEEE) — международная организация по разработке и созданию отраслевых стандартов для широкого ряда технологий, в том числе семейства стандартов беспроводной связи 802. См. *802, 802.1x, 802.11, 802.11a, 802.11b, 802.11e, 802.11f, 802.11g и 802.11h.*

Для получения дополнительной информации о рабочих группах и стандартах IEEE см. <http://standards.ieee.org/>.

IP

Протокол Internet Protocol (IP) определяет формат пакетов, называемых датаграммами, и схему адресации. Протокол IP — это протокол коммутации пакетов, не требующий соединения и негарантированный по скорости. Он обеспечивает маршрутизацию, фрагментацию и повторную сборку пакетов. Протокол работает совместно с протоколами более высокого уровня, такими как *TCP* или *UDP*, для установки виртуального соединения между получателем и отправителем.

Текущая версия протокола — *IPv4*. В разработке находится новая версия, называемая *IPv6* или *IPng*. *IPv6* призван разрешить проблему нехватки IP-адресов.

IPSec

Безопасность IP (IPSec) — набор протоколов для обеспечения безопасного обмена пакетами на уровне протокола *IP*. Здесь используются общие открытые ключи. Применяются два режима шифрования: транспортный и туннельный.

- В *транспортном* режиме зашифровываются только часть данных (полезная нагрузка) каждого пакета, а заголовки остаются незашифрованными.
- В более безопасном *туннельном* режиме зашифровываются и заголовок, и полезная нагрузка.

IP-адрес

Системы определяются по *IP-адресу*, 4-битовому (октетному) номеру — уникальному идентификатору каждого хоста в сети Интернет. Обычно IP-адрес имеет следующий формат: 192.168.2.254. Это называется десятичным представлением адреса с точками.

IP-адрес состоит из двух частей: сетевого префикса и номера хоста в сети. *Маска подсети* используется для определения этих частей данных. Существуют два специальных номера хоста:

- *Сетевой адрес* состоит из номера хоста, включающего все нули (например, 192.168.2.0).
- *Широковещательный адрес* состоит из номера хоста, включающего все единицы (например, 192.168.2.255).

Количество IP-адресов ограничено. Поэтому обычно локальная сеть использует один из диапазонов адресов, назначенных IANA для использования в частных сетях. Это следующие диапазоны 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

Динамический IP-адрес — это IP-адрес, который автоматически назначается хосту сервером **DHCP** или похожим механизмом. Он называется динамическим, потому что меняется с каждым новым подключением.

Статический IP-адрес — это IP-адрес, который запрограммирован для определенного хоста. Обычно статический адрес требуется для хоста, на котором работает сервер, например веб-сервер.

ISP

Интернет-оператор (ISP) — компания, предоставляющая доступ к Интернету физическим лицам и организациям. Он также может предоставлять связанные услуги, например, виртуальный хостинг, консультирование, веб-дизайн и т.д.

L

LAN

Локальная сеть (LAN) — это сеть связи с зоной покрытия ограниченной области, например домашние компьютеры, которые вы хотите объединить в сеть, или два этажа здания. LAN соединяет множество компьютеров и других сетевых устройств, таких как системы хранения данных и принтеры. **Ethernet** — наиболее распространенная технология реализации LAN.

Другой популярной технологией LAN является беспроводной Ethernet (**802.11**) (также см. **WLAN**).

LDAP

Облегченный протокол доступа к каталогам (LDAP) — протокол, использующийся для доступа к сетевой службе каталогов. Он используется для обеспечения механизма аутентификации. Он основан на стандарте X.500, но является менее сложным.

LLC

Уровень *управления логическими связями (LLC)* управляет синхронизацией кадра, управлением потоками данных и проверкой ошибок. Это протокол более высокого уровня, чем физический (*PHY*), работающий совместно с *MAC*-уровнем.

M

MAC

Уровень *управления доступом к среде передачи (MAC)* управляет передвижением пакетов данных между *NIC* по общему каналу. Это протокол более высокого уровня, чем физический (*PHY*). Он предоставляет механизм разрешения конфликтов для устранения коллизий сигналов.

Данный протокол использует аппаратный адрес, также известный как *MAC-адрес* — уникальный идентификатор каждого узла в сети. Сетевые устройства стандарта *IEEE 802* используют распространенный 48-разрядный формат *MAC*-адреса, который отображается в виде строки из двенадцати (12) шестнадцатеричных цифр, разделенных двоеточиями, например FE:DC:BA:09:87:65.

MDI и MDI-X

Интерфейс, зависящий от передающей среды (MDI) и *интерфейс, зависящий от передающей среды с перекрестным соединением (MDIX)*, — порты Ethernet аппаратных устройств, для соединения которых используется витая пара. Встроенная витая пара и механизм автоматического распознавания позволяют подключить похожие устройства с использованием стандартного кабеля Ethernet. Например, если беспроводная точка доступа поддерживает интерфейсы MDI/MDIX, можно подключить компьютер к этой точке доступа по кабелю Ethernet, а не кроссоверному кабелю.

MIB

Информационная база управления (MIB) — виртуальная база данных объектов, используемых для сетевого управления. *SNMP*-агенты, а также другие инструменты SNMP, могут использоваться для мониторинга любого сетевого устройства, определенного в MIB.

MSCHAP V2

Протокол аутентификации по квитированию вызова корпорации Microsoft, версия 2 (MSCHAP V2) обеспечивает аутентификацию для соединений *PPP* между компьютером под управлением Windows и точкой доступа (см. *Точка доступа*) или другим устройством доступа к сети.

MTU

Максимальный размер пакета — самый большой физический размер пакета, измеряемый в байтах, который может быть передан по сети. Сообщение размером больше значения MTU перед отправкой фрагментируется на более мелкие пакеты.

N

NAT

Преобразование сетевых адресов — стандарт сети Интернет, маскирующий внутренние IP-адреса, используемые в *LAN*. Работающий на шлюзе сервер NAT обслуживает таблицу преобразований, которая сопоставляет все внутренние IP-адреса в исходящих запросах со своими собственными адресами и конвертирует все входящие запросы к корректному внутреннему хосту.

NAT служит трем главным целям: обеспечивает безопасность маскировкой, скрывая внутренний IP-адрес, позволяет использовать широкий диапазон внутренних IP-адресов без риска возникновения конфликта с адресами, используемыми другими организациями, и позволяет использовать одно Интернет-соединение.

NIC

Сетевая плата — это адаптер или расширительная плата, вставляемая в компьютер для обеспечения физического подключения к сети. Большинство сетевых плат разрабатывается для определенного типа сети, протокола или носителя, например для сети *Ethernet* или беспроводной сети.

NTP

Сетевой протокол синхронизации времени обеспечивает точную синхронизацию системных часов в сети компьютеров. Серверы NTP передают *всемирное координированное время* (UTC, также известное как *среднее время по Гринвичу*) своим клиентским системам. Клиент NTP отправляет серверам периодические запросы о времени, используя возвращаемую метку времени для синхронизации времени.

O

OSI

Базовая модель *открытого взаимодействия систем* (OSI) — инфраструктура для проектирования сети. Модель OSI состоит из семи уровней:

- Уровень 1, физический уровень, определяет физический носитель, используемый для установки связи между узлами. В беспроводных сетях физическим носителем является воздух, а волны радиочастоты являются компонентами физического уровня.
- Уровень 2, уровень канала передачи данных, определяет структуру и формат передаваемых данных, а также протокол нижнего уровня для связи и адресации. Например, такие протоколы, как *CSMA/CA*, и такие компоненты, как *MAC*-адреса и кадры (см. *Кадр*), определяются и используются как часть канального уровня.
- Уровень 3, сетевой уровень, указывает, как определить лучший путь для передачи информации по сети. *Пакеты* и логические *IP-адреса* работают на уровне сети.
- Уровень 4, транспортный уровень, определяет протоколы с установлением соединения, такие как *TCP* и *UDP*.

- Уровень 5, уровень сеанса, определяет протоколы для инициализации, обслуживания и завершения связи и операций в сети. Примерами распространенных протоколов, работающих на этом уровне, являются сетевая файловая система (NFS) и язык структурированных запросов (SQL). Также частью этого уровня являются следующие режимы отправки потоков данных: единый режим (устройство отправляет информационный массив), полудуплексный режим (устройства передают массивы информации по очереди) и полнодуплексный режим (интерактивный, в котором устройства передают и получают данные одновременно).
- Уровень 6, уровень презентации, определяет, как информация представлена для приложения. Он включает мета-информацию о шифровании/дешифровании и сжатии/развертывании данных. Примерами протоколов этого уровня могут служить форматы файлов JPEG и TIFF.
- Уровень 7, уровень приложений, включает такие протоколы как протокол передачи гипертекстовых файлов (**HTTP**), простой протокол передачи почты (SMTP) и протокол передачи файлов (FTP).

P

PHY

Физический уровень (PHY) — самый нижний уровень в модели сетевых уровней (см. **OSI**). Физический уровень передает поток двоичных сигналов — электрический импульс, световой или радиосигнал — по сети на электрическом и механическом уровне. Это предоставляет аппаратное средство отправки и получения данных на носителе, включая определение кабелей, **NIC** и физических аспектов.

Ethernet и семейство **802,11** — протоколы с компонентами физического уровня.

PID

Идентификатор процесса (PID) — целое число, которое Linux использует для уникальной идентификации процесса. PID возвращается после системного вызова `fork()`. Он может использоваться процессами `wait()` или `kill()` для выполнения соответствующих действий.

PPP

Протокол двухточечной связи — стандарт для передачи датаграмм сетевого уровня (**IP**-пакеты) по последовательной двухточечной линии связи. Протокол PPP разработан для работы как через асинхронные подключения, так и бит-ориентированные синхронные системы.

PPPoE

Протокол двухточечной связи по сети Ethernet (PPPoE) — спецификация для подключения пользователей в **LAN** к Интернету через широкополосную среду передачи данных, например, DSL или кабельный модем.

PPtP

Туннельный протокол двухточечной связи (PPtP) — технология создания виртуальной частной сети (**VPN**) в рамках протокола двухточечной связи (**PPP**). Используется для безопасной передачи данных от одного узла VPN к другому.

PSK

Предварительный ключ (PSK), см. **Общий ключ**.

Q

QoS

Уровень качества обслуживания (**QoS**) определяет эксплуатационные свойства сетевой службы, включая гарантированную пропускную способность, задержка передачи и приоритизированные очереди. **QoS** разработан для снижения вероятности таких эффектов как *Запаздывание*, *Искажения*, *Потеря пакетов* и перегрузка сети. Он также обеспечивает способ предоставления выделенной полосы пропускания для сетевого трафика с высоким приоритетом.

В настоящее время стандарт **IEEE** для реализации **QoS** в беспроводных сетях находится на стадии разработки рабочей группой **802.11e**. Набор функций **802.11e** описан в спецификации **WMM**.

R

RADIUS

Служба идентификации удаленных пользователей (RADIUS) предоставляет систему аутентификации и учета. Это популярный механизм аутентификации для многих *ISP*.

RC4

Симметричное потоковое шифрование, предоставляемое *RSA Security*. Это потоковое шифрование, построенное на основе параметризованного ключом генератора псевдослучайных битов с равномерным распределением. Длина ключа не должна превышать 2048 битов.

RSSI

Индикация уровня принимаемого сигнала (RSSI) — значение *802.1x*, измеряющее уровень мощности принимаемого сигнала. RSSI — это один из нескольких способов измерения и индикации мощности *радиочастотного* сигнала. Мощность сигнала также может измеряться в милливаттах (мВт), децибелах на милливатт (дБм) и процентах.

RTP

Транспортный протокол реального времени (RTP) — интернет-протокол для передачи аудио- и видеоданных в реальном времени. Он не гарантирует доставку, но обеспечивает поддержку механизмов отправки и получения приложений для использования потоков данных. Как правило, протокол RTP работает вместе с протоколом *UDP*, но может поддерживать и другие транспортные протоколы.

RTS

Сообщение запроса на передачу данных (RTS) — это сигнал, отправляемый клиентской станцией точке доступа для запроса разрешения на отправку пакета данных во избежание занятия канала другими беспроводными клиентскими станциями. Сообщение является частью протокола *CSMA/CA* стандарта IEEE 802.11. См. также *Порог RTS* и *CTS*.

S

SNMP

Простой протокол сетевого управления (SNMP) был разработан для управления и мониторинга узлов в сети. Он является частью набора протоколов *TCP/IP*.

Протокол SNMP состоит из управляемых устройств, их агентов и системы управления. Агенты сохраняют данные о соответствующих устройствах в *информационных базах управления (MIB)* и возвращают эти данные в систему управления SNMP по запросу.

SNMP-ловушки

SNMP-ловушки обеспечивают асинхронную связь между сетевыми устройствами и управляемыми агентами. Настройка SNMP-ловушек позволяет сэкономить сетевые ресурсы и устраняет избыточные запросы SNMP.

SSID

Идентификатор набора служб (SSID) — это буквенно-цифровой ключ длиной не более 32 символов, который является уникальным идентификатором беспроводной локальной сети. Он также называется «*Network Name*» (*Сетевое имя*). В идентификаторе SSID можно использовать любые символы без ограничений.

STP

Протокол связующего дерева (STP) — это протокол стандарта IEEE 802.1 (связанный с управлением сетью) для мостов *MAC*, управляющий избыточностью сетевого пути и устраняющий петли в сети, создаваемые несколькими активными путями между клиентскими станциями. Петли возникают при наличии нескольких маршрутов между точками доступа. Протокол STP создает дерево, связывающее все коммутаторы в расширенной сети, и блокирует избыточные пути или переводит их в состояние ожидания. Протокол STP позволяет одновременно использовать только один активный путь между двумя сетевыми устройствами (тем самым устраняя петли), но создает резервную ссылку, которая используется при сбое первой ссылки. При изменении стоимости STP или в ситуации, когда сетевой сегмент становится недоступным, алгоритм связующего дерева переопределяет топологию связующего дерева и восстанавливает ссылку, активируя резервный путь. Без использования протокола STP существует вероятность, что оба соединения одновременно будут активными, что может привести к возникновению бесконечной петли трафика в локальной сети.

SVP

Определение приоритетов голосовых данных SpectraLink (SVP) — это одна из методик QoS для развертывания сетей Wi-Fi. SVP является открытой спецификацией, соответствующей стандарту IEEE 802.11b. SVP сокращает время задержки передачи голосовых пакетов, повышая их приоритет по сравнению с пакетами данных в беспроводной сети, тем самым увеличивая потенциальную производительность сети.

T

TCP

Протокол управления передачей (TCP) построен на основе протокола Internet Protocol (*IP*). Он обеспечивает надежную связь (гарантирует доставку данных), управление потоками данных, мультиплексирование (несколько одновременных подключений) и передачу данных на основе соединений (получатель пакета должен отправить подтверждение получения отправителю). Он также гарантирует, что пакеты будут доставлены в том же порядке, в каком они были отправлены.

TCP/IP

Интернет и большинство локальных сетей определяются группой протоколов. Основные из них — это *протокол управления передачей и межсетевой протокол* (TCP/IP), которые фактически являются стандартными протоколами. Протокол TCP/IP был разработан Агентством передовых оборонных исследовательских проектов (DARPA, или ARPA — агентство Министерства обороны США).

Хотя *TCP* и *IP* — это два отдельных протокола, TCP/IP часто используется для определения набора сетевых протоколов, среди которых также используются ICMP, ARP, *UDP* и другие, а также приложений, работающих с этими протоколами, таких как telnet, FTP и т.д.

TKIP

Протокол шифрования с использованием временных ключей (TKIP) предоставляет расширенный 48-разрядный вектор инициализации, конструирование и распространение ключа для каждого пакета, код проверки целостности сообщения (MIC, также называемый «Michael») и механизм изменения ключа. Поточное шифрование **RC4** используется для шифрования тела кадра и периодической проверки резервирования (CRC) каждого кадра **802.11** перед передачей. Это важный компонент режимов безопасности **WPA** и **802.11h**.

ToS

Пакеты **TCP/IP** содержат заголовки с 3-5-битным полем «*Type of Service*» (ToS), настроенным разработчиком приложения. Это поле определяет тип обслуживания, соответствующий данным в пакете. Способ настройки битов определяет, нужно ли добавлять пакет в очередь на отправку с параметрами минимальной задержки, максимальной пропускной способности, низкой стоимости или максимально возможного доступа, в зависимости от требований к данным. Поле ToS используется беспроводным шлюзом 9160 G2 Wireless Gateway для обеспечения контроля конфигурации над очередями *Quality of Service (QoS)* для данных, передаваемых от точки доступа клиентским станциям.

U

UDP

Протокол пользовательских датаграмм (UDP) — это протокол транспортного уровня, предоставляющий простые, хотя и ненадежные, услуги отправки датаграмм. Он добавляет информацию об адресе порта и контрольную сумму в пакет **IP**.

Протокол UDP не гарантирует доставку и не требует подключения. Он не занимает много места и эффективно работает. Обработка ошибок и повторная передача должны осуществляться специальным приложением.

URL

Унифицированный указатель ресурса (URL) — это стандарт для определения местоположения объектов (файлов, групп новостей и т.д.) в Интернете. URL-адреса широко используются в HTML-документах для указания адреса гиперссылки, который часто является другим HTML-документом (возможно, сохраненным на другом компьютере). Первая часть URL-адреса указывает на используемый протокол, а вторая содержит IP-адрес или имя домена, на котором размещен ресурс.

Например, URL-адрес `ftp://ftp.devicescape.com/downloads/myfile.tar.gz` указывает на файл, который можно получить по протоколу FTP; URL-адрес <http://www.devicescape.com/index.html> указывает на веб-страницу, на которую можно перейти, используя протокол *HTTP*.

UTC

Всемирное координированное время (UTC), называемое также «среднее время по Гринвичу».

V

VLAN

Виртуальная LAN (VLAN) — это программно реализованная логическая группа сетевых устройств, позволяющая им работать так, как будто они подключены к одной физической сети. Узлы VLAN изолированы в сети, но имеют общие ресурсы и полосу пропускания. Беспроводной шлюз 9160 G2 Wireless Gateway поддерживает конфигурацию беспроводного VLAN. Эта технология используется на точке доступа для «виртуальной» гостевой сети.

VPN

Виртуальная частная сеть (VPN) — это сеть, которая для подключения своих узлов использует Интернет. В ней используется шифрование и другие механизмы, позволяющие обеспечить доступ к узлам только для авторизованных пользователей и предотвращающие перехват данных.

W

WAN

Глобальная сеть (WAN) — это сеть связи, охватывающая большие территории и действующая на расстоянии более одного километра. Зачастую WAN использует для подключения общедоступные сети, например системы телефонной связи. Также могут использоваться арендованные или спутниковые каналы.

Интернет, по сути, является очень большой WAN.

WDS

С помощью *распределенной беспроводной системы (WDS)* можно создать полностью беспроводную инфраструктуру. Обычно *Точка доступа* подключается к проводной *LAN*. Благодаря WDS возможно беспроводное подключение точек доступа. Точки доступа могут функционировать в режиме беспроводных ретрансляторов или мостов.

WEP

Эквивалент конфиденциальности проводных сетей (WEP) — это протокол шифрования данных в беспроводных сетях **802,11**. Все беспроводные станции и точки доступа в сети настраиваются с помощью статического 64-разрядного общего ключа (40-разрядный секретный ключ + 24-разрядный вектор инициализации (IV)) или 128-разрядного общего ключа (104-разрядный секретный ключ + 24-разрядный вектор инициализации) (см. *Общий ключ*) для шифрования данных. Поточное шифрование *RC4* используется для шифрования тела кадра и периодической проверки резервирования (CRC) каждого кадра **802,11** перед передачей.

Wi-Fi

Тестирование и сертификация взаимодействия продуктов *WLAN* на основе стандарта **IEEE 802,11**, распространяемого *Wi-Fi Alliance*, некоммерческой торговой организацией.

WINS

Служба интернет-имен для Windows (WINS) — серверный процесс для сопоставления имен компьютеров под управлением Windows с IP-адресами. Предоставляет информацию, с помощью которой эти системы могут выполнять поиск сетей, используя функцию *сетевого окружения*.

WLAN

Беспроводная локальная сеть (WLAN) — это *LAN*, использующая для связи между узлами высокочастотные радиоволны, а не кабели.

WMM

Беспроводные мультимедиа (WMM) — стандарт технологии *IEEE*, разработанный для улучшения качества аудио-, видео- и мультимедийных приложений в беспроводной сети. WMM можно использовать как на точке доступа, так и на беспроводных клиентах (ноутбуках, бытовой электронике). Функции WMM являются подгруппой проекта спецификации *WLAN IEEE 802.11e*. Беспроводные продукты, созданные в соответствии со стандартом и прошедшие ряд испытаний качества, могут носить метку «Wi-Fi certified for WMM» (Сертификат Wi-Fi для WMM), обозначающую возможность взаимодействия с другими подобными продуктами. Для получения дополнительной информации см. страницу WMM на веб-сайте Wi-Fi Alliance: <http://www.wi-fi.org/OpenSection/wmm.asp>.

WPA

Защищенный доступ Wi-Fi (WPA) — версия *Wi-Fi Alliance* проекта стандарта *IEEE 802.11h*. Обеспечивает более сложный механизм шифрования данных по сравнению с шифрованием *WEP* и использует аутентификацию пользователей. WPA включает алгоритмы *TKIP* и *802.1x*.

WPA2

Защищенный доступ Wi-Fi (WPA2) — это улучшенный стандарт безопасности, описанный в *IEEE 802.11h*, в котором для шифрования данных используется усовершенствованный стандарт шифрования (*AES*).

Оригинальный стандарт **WPA** для шифрования данных использует протокол шифрования с использованием временных ключей (**TKIP**). WPA2 имеет обратную совместимость с продуктами, которые поддерживают оригинальный **WPA**.

Стандарт WPA2, как и оригинальный **WPA**, имеет две версии — *Enterprise* и *Personal*. Версия Enterprise требует использования функций безопасности IEEE **802.1x** и *расширяемого протокола аутентификации (EAP)* с **RADIUS**-сервером.

Версия Personal не требует использования IEEE **802.1x** и **EAP**. В ней используется *предварительный ключ (PSK)* для генерирования ключей, необходимых для аутентификации.

WRAP

Протокол WRAP (Wireless Robust Authentication Protocol) — это метод шифрования для стандарта **802.11h**, который использует **AES**, но для шифрования и проверки целостности применяет другой режим шифрования (**OCB**).

X

XML

Расширяемый язык разметки (XML) — это спецификация, разработанная консорциумом **W3C**. XML — это простой и гибкий текстовый формат, созданный на основе *стандартного языка обобщенной разметки (SGML)*, разработанного специально для электронного редактирования и оформления документов.

Б

Базовый диапазон скорости

Базовый диапазон скорости определяет скорость передачи данных, обязательную для любой станции, которая хочет присоединиться к данной беспроводной сети. Все станции должны иметь возможность получать данные на скоростях, входящих в этот диапазон.

Д

Динамический IP-адрес

См. *IP-адрес*.

З

Запаздывание

Запаздывание, или *задержка*, — период времени, необходимый для передачи пакета (см. *Пакет*) от отправителя получателю. Запаздывание может произойти при передаче данных от точки доступа клиенту и наоборот. Оно также может возникнуть при передаче данных от точки доступа в Интернет и наоборот. Запаздывание возникает из-за *фиксированных факторов сети*, таких как время кодирования и декодирования пакета, а также из-за *переменных факторов сети*, таких как занятость и перегрузка сети. Функции *QoS* разработаны, чтобы устранить запаздывание для высокоприоритетного сетевого трафика.

И

Инфраструктура беспроводной сети

Существует два способа организации беспроводной сети:

- Станции взаимодействуют непосредственно друг с другом в сети, работающей в режиме прямого подключения (см. *Режим прямого подключения*), называемого также независимым базовым набором служб (*IBSS*).
- Станции взаимодействуют через точку доступа (см. *Точка доступа*) в сети, работающей в режиме инфраструктуры (см. *Режим инфраструктуры*). Одна точка доступа создает базовый набор служб инфраструктуры (*BSS*), а несколько точек доступа организуются в расширенный набор служб (*ESS*).

Искажения

Искажения — это разница между запаздыванием (или задержкой) при передаче пакета от одного узла по сети. Если пакеты не передаются с постоянной скоростью (включая *Запаздывание*), это может повлиять на уровень *QoS* для некоторых типов данных. Например, непостоянная скорость передачи данных может стать причиной искажений при использовании IP-телефонии и передаче мультимедийных потоков. Стандарт *QoS* разработан для устранения искажений, а также других факторов, влияющих на производительность сети.

К

Кадр

Кадр состоит из разрозненных фрагментов данных и описательной мета-информации, упакованных для передачи по беспроводной сети. Каждый кадр включает *MAC*-адрес отправителя и получателя, контрольное поле с версией протокола, тип кадра, номер последовательности кадров, тело кадра (с актуальной информацией для передачи) и контрольную сумму проверки кадров для обнаружения ошибок. Понятие кадра близко к понятию пакета (см. *Пакет*), с той разницей, что пакеты обрабатываются на сетевом уровне (уровень 3 в модели OSI), а кадры — на канальном уровне (уровень 2 в модели *OSI*).

Канал

Канал определяет часть радиочастотного спектра, который будет использоваться радиомодулем для передачи и приема сигнала. Каждый стандарт *802.11* предлагает некоторое количество каналов, в зависимости от того, как лицензируется диапазон радиочастот государственными и межгосударственными органами власти, такими как Федеральное агентство по связи США (FCC), Европейский институт по стандартизации в области телекоммуникаций (ETSI), Корейская комиссия по связи и Технический центр связи (TELEC).

М

Маршрутизатор

Маршрутизатор — сетевое устройство, перенаправляющее пакеты данных между сетями. Он подключен по крайней мере к двум сетям; обычно это две локальные сети (*LAN*) или *LAN* и глобальная сеть (*WAN*), например Интернет. Маршрутизаторы расположены на шлюзах — местах, где соединяются две или несколько сетей.

Маршрутизатор использует содержимое заголовков и свои таблицы для определения лучшего пути для передачи пакета. Для взаимодействия с другими маршрутизаторами для настройки лучшего маршрута между двумя узлами он использует следующие протоколы: протокол межсетевых управляющих сообщений (ICMP), протокол маршрутной информации (RIP) и протокол обнаружения маршрутизаторов (IRDP). Маршрутизатор практически не фильтрует передаваемые данные.

Маска подсети

Маска подсети — это номер, который определяет, какая часть IP-адреса является сетевым адресом, а какая — адресом хоста в сети. Имеет десятичное представление адреса с точками (например, 24-битовая маска представлена в виде 255.255.255.0) или номера, добавляемого к IP-адресу (например, 192.168.2.0/24).

С помощью маски подсети маршрутизатор быстро определяет, является ли IP-адрес локальным или его необходимо перенаправить, выполнив побитовую операцию AND на маске и IP-адресе. Например, для IP-адреса 192.168.2.128 и маски подсети 255.255.255.0 результирующим сетевым адресом будет 192.168.2.0.

Побитовый оператор AND сравнивает два бита и добавляет 1 к результату, только если оба бита равны 1. В таблице ниже представлена подробная информация о маске подсети:

| | | |
|------------------------------|---------------|-------------------------------------|
| IP-адрес | 192.168.2.128 | 11000000 10101000 00000010 10000000 |
| Маска сети | 255.255.255.0 | 11111111 11111111 11111111 00000000 |
| Результирующий сетевой адрес | 192.168.2.0 | 11000000 10101000 00000010 00000000 |

Маячок

Кадры маячка представляют собой периодический сигнал **WLAN**, сообщающий о существовании сети и позволяющий станциям устанавливать и поддерживать связь упорядоченным способом. Маячок несет следующую информацию (часть ее является необязательной):

- *Метка времени* используется станциями для обновления часов местного времени, способствуя процессу синхронизации всех ассоциированных станций.
- *Интервал маячка* определяет период времени между передачей кадров маячка. Перед переключением в режим экономии электроэнергии станции необходимо получить интервал маячка, чтобы установить время включения для получения маячка.
- *Данные о емкости* — список требований к станциям, которые хотят присоединиться к **WLAN**. Например, все станции должны использовать стандарт **WEP**.
- *Идентификатор набора служб (SSID)*.
- *Базовый диапазон скорости* отображает список скоростей передачи данных, поддерживаемых в сети **WLAN**.
- Необязательные *наборы параметров* обозначают функции определенных используемых способов сигнализации (например, расширенный спектр сигнала со скачкообразной перестройкой частоты, расширенный спектр с перестройкой частоты с применением прямой последовательности и т.д.).
- Необязательная *карта указателей трафика (TIM)* обозначает станции, использующие режим экономии электроэнергии, для которых имеется очередь кадров данных.

Многоадресная передача

При *многоадресной передаче* одно сообщение отправляется выбранной группе получателей. Примером многоадресной передачи может служить отправка сообщения списку получателей. В беспроводных сетях многоадресной передачей обычно называется взаимодействие, при котором точка доступа отправляет трафик данных в форме кадров **IEEE 802.1x** (см. *Кадр*) определенному количеству клиентских станций (**MAC**-адресов) в сети.

В некоторых режимах безопасности беспроводной сети различается необходимость и способ шифрования одноадресных, многоадресных и широковещательных кадров.

См. также *Одноадресная передача* и *Широковещательная передача*.

Мост

Подключение между двумя локальными сетями (*LAN*) по одному протоколу, например Ethernet или *IEEE 802.1x*.

0

Обнаружение вторжения

Система обнаружения вторжения (IDS) проверяет сетевую активность на входе и сообщает о подозрительных сценариях, которые могут означать, что сеть или система подвергается внешней атаке. Она сообщает о попытках входа, при которых используются неподдерживаемые или неизвестные небезопасные протоколы.

Общий ключ

Общий ключ используется в традиционном шифровании, где один ключ применяется для шифрования и дешифрования. Он также называется *секретным* или *симметричным ключом*.

См. также *Открытый ключ*.

Одноадресная передача

При *одноадресной передаче* сообщение отправляется одному указанному получателю. В беспроводных сетях одноадресной передачей обычно называется взаимодействие, при котором точка доступа отправляет трафик данных в форме кадров *IEEE 802.1x* (см. *Кадр*) непосредственно на *MAC*-адрес одной клиентской станции сети.

В некоторых режимах безопасности беспроводной сети различается необходимость и способ шифрования одноадресных, многоадресных и широковещательных кадров.

См. также *Многоадресная передача* и *Широковещательная передача*.

Открытый ключ

Открытый ключ используется в криптографии открытого ключа для шифрования сообщения, которое может быть расшифровано только с помощью частного или секретного ключа получателя. Шифрование открытого ключа также называется асимметричным шифрованием, потому что использует два ключа, или шифрованием по методу Диффи-Хеллмана. См. также *Общий ключ*.

П

Пакет

Данные передаются по узлам сети в форме *пакетов*. Данные и мультимедийное содержимое разбиваются и упаковываются в *пакеты*. В пакете содержится небольшая часть содержимого, которое необходимо отправить, а также адрес назначения и адрес отправителя. Пакеты отправляются в сеть и проверяются каждым узлом. Конечным получателем выступает узел, которому адресован пакет.

Переадресация портов

При *переадресации портов* создается «туннель» через межсетевой экран, позволяющий пользователям Интернета получать доступ к службам, запущенным на одном из компьютеров в *LAN*, например к веб-серверу, серверу FTP или SSH и другим службам. С точки зрения внешнего пользователя это будет выглядеть так, как будто служба запущена на межсетевом экране.

Поддерживаемые диапазоны скорости

Поддерживаемый диапазон скорости определяет скорость передачи данных, доступную в данной беспроводной сети. Станция может иметь возможность получать данные на любой из скоростей, входящих в этот диапазон. Все станции должны иметь возможность получать данные на скоростях, входящих в *Базовый диапазон скорости*.

Порог RTS

Порог RTS определяет размер пакета запроса на передачу (*RTS*). Это значение помогает контролировать поток трафика через точку доступа, что особенно полезно для настройки параметров производительности на точке доступа с множеством клиентов.

Потеря пакетов

Потеря пакетов — процент переданных по сети пакетов, которые не достигли адреса назначения. Нулевой процент потери пакетов означает, что при передаче данных пакеты потеряны не были. Функции **QoS** предназначены для минимизации потери пакетов.

Прокси-сервер

Прокси-сервер находится между клиентским приложением и реальным сервером. Он перехватывает запросы, пытаясь выполнить их самостоятельно. Если он не может этого сделать, он передает их реальному серверу. Прокси-серверы выполняют две основные цели: повышение производительности путем распределения запросов среди нескольких машин и фильтрация запросов для предотвращения доступа к определенным серверам или службам.

Р

Режим инфраструктуры

Режим инфраструктуры — это **Инфраструктура беспроводной сети**, в которой беспроводные станции взаимодействуют друг с другом через точку доступа (см. **Точка доступа**). В этом режиме беспроводные станции могут взаимодействовать друг с другом или с главными устройствами в проводной сети. Точка доступа подключается к проводной сети и поддерживает несколько беспроводных станций.

Режим инфраструктуры может обеспечиваться одной точкой доступа (**BSS**) или несколькими точками доступа (**ESS**).

Режим прямого подключения

Режим прямого подключения — это **Инфраструктура беспроводной сети**, в которой станции взаимодействуют друг с другом напрямую. Этот режим используется для быстрого создания сети в ситуациях, когда формальная инфраструктура не требуется.

Режим прямого подключения также называется *одноранговым режимом* или независимым базовым набором служб (**IBSS**).

Роуминг

В терминологии *IEEE 802.11*, клиенты роуминга — это мобильные клиентские станции или устройства в беспроводной сети (*WLAN*), которым необходимо более одной точки доступа (см. *Точка доступа*) при нахождении в зонах обслуживания разных базовых станций. Стандарт *IEEE 802.11f* определяет способ, с помощью которого точки доступа могут передавать информацию об ассоциациях и диссоциациях клиентов для поддержки клиентов в роуминге.

С

Сетевой адрес

См. *IP-адрес*.

Срок аренды

Срок аренды определяет период времени, на который сервер *DHCP* предоставляет своим клиентам *IP-адрес* и другую необходимую информацию. Когда срок аренды истекает, клиент должен запросить новый период аренды. Если установлен краткий срок аренды, вы можете обновить сетевую информацию и своевременно распространить предоставленную информацию среди клиентов.

Статический IP-адрес

См. *IP-адрес*.

Т

Точка доступа

Точка доступа — узел связи для устройств в *WLAN*, обеспечивающий подключение или мост между беспроводными и проводными сетевыми устройствами. Она поддерживает инфраструктуру беспроводной сети (*Инфраструктура беспроводной сети*), называемую режимом инфраструктуры (*Режим инфраструктуры*).

Когда одна точка доступа подключена к проводной сети и поддерживает набор беспроводных станций, она называется базовым набором служб (*BSS*). Расширенный набор служб (*ESS*) создается при соединении двух или более *BSS*.

Ш

Широковещательная передача

При *широковещательной передаче* одно сообщение отправляется одновременно всем получателям. В беспроводных сетях широковещательной передачей называется взаимодействие, при котором точка доступа отправляет трафик данных в форме кадров *IEEE 802.1x* (см. *Кадр*) всем клиентским станциям в сети.

В некоторых режимах безопасности беспроводной сети различается необходимость и способ шифрования одноадресных, многоадресных и широковещательных кадров.

См. также *Одноадресная передача* и *Многоадресная передача*.

Широковещательный адрес

См. *IP-адрес*.

Шлюз

Шлюз — это сетевой узел, который служит входом в другую сеть. Часто шлюз также предоставляет прокси-сервер и межсетевой экран. Он связан с маршрутизатором, который использует заголовки и таблицы переадресации для определения конечного пункта доставки пакетов, и с коммутатором или мостом, позволяющим пакету войти и выйти из шлюза.

Чтобы главное устройство в *LAN* могло получить доступ к Интернету, оно должно знать адрес *шлюза по умолчанию*.

УКАЗАТЕЛЬ

Номер

100BaseT Ethernet 24, B-3

10BaseT Ethernet 24, B-3

3274/Telnet 292–310

Протокол 308

802.IQ

802.IQv1

**Идентификатор типа
протокола** 346

Интерфейсы маячка 347

**Начальное время на передачу и
подтверждение** 346

описание 343

Только передача пакетов

802.IQ 347

Функции Меню 347

802.IQv2

описание 343

Порт UDP маячка 347

Функции Меню 347

Автозапуск 343

**Время ожидания терминала в
автономном режиме** 344

Интервал маячка 344

обзор протокола 343

9010 / TCP/IP, конфигурация базовой
станции 283, 290

A

Actively Negotiate with Host

Протокол Telnet/3274 306

Протокол Telnet/5250 324

AIAG

Эмуляция 3274 299

Эмуляция 5250 317

ANSI, подключение терминалов 26

Auto-telnet, ANSI/Telnet

Главное устройство 336

Auto-telnet Host

Протокол Telnet/3274 308

Протокол Telnet/5250 325

C

Close Host Sessions on Terminal Reset

Протокол Telnet/ANSI 334

D

DCF

по отношению к QoS 215

таймер случайной задержки 216

DEC VT220, подключение 26

DHCP, общие сведения о

самоуправляемых точках доступа 36

DSCP

Приоритет 219

теги 217

E

EAP-PEAP

настройка на клиенте

IEEE 802.1x C-17

настройка на клиенте WPA/WPA2

Enterprise (RADIUS) C-25

Ethernet

100BaseT 24

выводы B-3

10BaseT 24

выводы B-3

базовая станция 267

волоконно-оптический

100Base-FX 25

длина кабеля 24

карты адаптера 366

параметры 147, 177

подключения 24, 42

светодиодный индикатор

состояния 25

F

Firefox 26

I

IEEE 802.11

диапазон скорости, настройка 187
поддержка стандартов 11
режим радиомодуля, настройка 187
IEEE 802.11a
настройка 187
IEEE 802.11b
настройка 187
IEEE 802.11g
настройка 187
IEEE 802.1x
режим безопасности
использование 103
конфигурация клиента C-17
настройка 116
Internet Explorer 26
IP-адрес (базовая станция) 268
IP-адреса
9160 G2 24
общие сведения о политиках для
самоуправляемых точек
доступа 36
переход 66
просмотр точек доступа 59, 67, 91

Is Host Fujitsu

Эмуляция 3274 293

M

mapRF

802.IQv2 343

MIB См. Информационные базы
управления 243

Microsoft Internet Explorer 26

P

PEAP

настройка на клиенте

IEEE 802.1x C-17

настройка на клиенте WPA/WPA2

Enterprise (RADIUS) C-25

Q

QoS См. качество
обслуживания 209

R

RADIUS-сервер

См. также сервер аутентификации
настройка для обнаружения точек
доступа C-37

S

SDRAM 366

SNMP См. Простой протокол
сетевого управления 243

T

TekTerm, Функции радиоканала 278

TLS-EAP

настройка на клиенте

IEEE 802.1x C-21

настройка на клиенте WPA/WPA2

Enterprise (RADIUS) C-30

получение сертификата
для клиента C-41

ToS по отношению к QoS 213

V

VLAN

для внутреннего и гостевого
интерфейсов 172

Приоритет 219

VWN (виртуальные беспроводные сети),
Параметры Ethernet 153

W

WDS

настройка 235

описание 231

правила 236

пример 239

A

Автозапуск

(базовая станция) 268

802.IQ 343

группа RRM 271

Автозапуск, режим базовой
станции 259

Автоматические сеансы telnet

Протокол Telnet/3274 308

Протокол Telnet/5250 324

Автоматические сеансы telnet,

ANSI/Telnet

Включить автоматические сеансы
telnet/логин для входа 335

Запрос терминала 336

Пароль 337

Автоматические сеансы telnet без действий пользователя*Протокол Telnet/3274 309**Протокол Telnet/5250 325**Протокол Telnet/ANSI 339***Автоматический вход, ANSI/Telnet**

Включить автоматические сеансы telnet/логин для входа 335

Идентификатор пользователя 337

неправильный логин 338

Пароль 338

администратор

пароль

в разделе «Basic Settings»

(Базовые параметры) 53

Активный канал

Группа RRM 274

Параметры RA1001A 264

аппаратные линии связи 42

ассоциированные беспроводные

клиенты 140

аутентификация для режимов

безопасности 100

Б

базовая станция

IP-адрес 268

Автозапуск 259, 268

Главные устройства 281–284

Имя 268

конфигурация 251–284

Меню подключений 265–284

меню узкополосного

радиомодуля 255–264

Не уведомлять об изменении**сетевого статуса**, хост

9010/TCP/IP 284

Номер базовой станции 267

Номер главного устройства 283, 290

обзор 253

Опрос монитора, хост

9010/TCP/IP 284

Первый терминал 291**Первый терминал**, хост

9010/TCP/IP 283

Последний терминал, хост

9010/TCP/IP 283

Последний терминал главное

устройство 291

Размер сообщения 268**Режим работы** 259**Совместно используемый канал** 260

хост 9010/TCP/IP 283, 290

базовые параметры, просмотр 45

балансировка нагрузки, настройка 205

безопасность

IEEE 802.1x 116

WPA/WPA2 Enterprise (RADIUS) 122

WPA/WPA2 Personal (PSK) 119

гостевая сеть 110

инструкции xvii

настройка 97–127

настройка на беспроводных

клиентах C-5

настройка на точке доступа 107

обзор функций 13

преимущества и недостатки разных

режимов 99

простой текст

(настройка «none») 110

сервер аутентификации C-37

сертификаты на клиентских

устройствах C-41

сравнение режимов 100

статическое WEP-шифрование 111

утверждения xvi

безопасность гостевой сети 110

беспроводная сеть

обзор функций точки доступа 8

параметры 159

соседние сети 89

В

веб-браузер 26

видеотерминал, подключение 26

Видимый совпадающий символ*Эмуляция 3274 301**Эмуляция 5250 319*

Включение и отключение режима

Persistence (Непрерывный), Журналы

регистрации событий 133

Включение удаленного передатчика

группа RRM 274

узкополосный радиомодуль 263

внешние устройства 23

волоконно-оптический порт

100Base-FX 25

волоконно-оптический порт Ethernet 25
Временная задержка автоматических сеансов telnet без действий пользователя
Протокол Telnet/ANSI 339
 временное мультиплексирование 253
 время, настройка точки доступа для использования сервера NTP 352
 время ожидания автосинхронизации кластера 63
Время ожидания терминала протокола опроса, Функции радиоканала 277
Время ожидания терминала протокола опроса в процентах, Функции радиоканала 278
Время ожидания управляющей команды, *Эмуляция ANSI* 329
 вход на веб-страницы администрирования 45
 входное напряжение (требования к источнику питания) 21, 366
 выводы разъема RJ-45 (10BaseT Ethernet) B-3
 выводы *См. выводы портов*

Г

Главное устройство

Время ожидания

Эмуляция ANSI 328

Печать

Эмуляция 3274 297

Эмуляция 5250 314

Порт

Протокол Telnet/3274 306

Протокол Telnet/5250 323

Протокол Telnet/ANSI 333

ГЛАВНЫЕ УСТРОЙСТВА

конфигурация

мини-контроллера 288

Главные устройства (конфигурация базовой станции) 281–284

Глубина, Журналы регистрации событий 135

Гостевой доступ,

Параметры Ethernet 151

гостевой интерфейс

VLAN 172

настройка 172

обзор функций 14

определение 171

Группа RRM

Автозапуск 271

Активный канал 274

Включение удаленного передатчика 274

Задержка синхронизации 274

Количество окон опроса 272

Количество повторов 272

Комбинация 274

Лимит режима сообщений 272

Максимальный размер сегмента сообщения 272

Номер группы RRM 270

Параметры протокола опроса 271

Период позывного 273

Размер коллизии 272

Размер окон опроса 272

Совместно используемый канал 271

Строка позывного 273

Удаленные радиомодули 275

Фактор свободного окна 272

Групповое кодирование, *Эмуляция ANSI* 332

Группы RRM параметры настройки 268

Д

Данные инициализации главного устройства, *Эмуляция ANSI* 332

Данные инициализации терминала, *Эмуляция ANSI* 332

Диапазон автоматического назначения адресов радиомодулям, Функции радиоканала 278

диапазон терминала, *Главные устройства* меню 291

диапазон терминала, *Главные устройства* меню (эмуляция 9010) 283

Длина формы печати

Эмуляция 3274 304

Эмуляция 5250 321

З

Задержка синхронизации группа RRM 274

узкополосный радиомодуль 263
Запись кода ошибки,
Эмуляция 5250 310
 запуск сети 54
 значки в пользовательском
 интерфейсе 54

И

Идентификатор опроса, Функции
 радиоканала 277

Изменений значений клавиш
управления курсором, Эмуляция
ANSI 330

Изменить выделение поля
Эмуляция 5250 312

Изоляция станции 108

Имя хоста DNS, Параметры
 Ethernet 151

индикатор выполнения
 автосинхронизации кластера 63
 индикаторы состояния (светодиодные
 индикаторы) 25

интервал маячка, настройка 187

интерфейсы, сеть 366

информационные базы управления
 (MIB) 243

Информация о выбросах загрязняющих
 веществ, Канада xv

Использовать международный
EVCDIC

Эмуляция 3274 293

Эмуляция 5250 310

К

кабели

№ консольного порта 19387 B-2

коаксиальный 22

описание последовательных B-1

канал, настройка радиомодуля 187

каптивный портал 173

качество обслуживания 209

кластер

автосинхронизация 63

безопасность 63

добавление точки доступа 65

общие сведения 60

определение 60

остановка кластеризации 66

поддерживаемые типы точек
 доступа 60

размер 60

размер и состав 63

соседние сети 89, 91

управление каналами 79

устранение неисправностей D-52

формирование 62

клиент

См. также *станции 187*

безопасность C-5

мониторинг целостности
 соединений 141

платформа 35

сеанс, определение 68

сеансы 67

клиенты

ассоциации 140

Ключ запроса сеанса TCP, Протокол
Telnet/ANSI 334

Ключ последнего активного сеанса,
Протокол Telnet/ANSI 335

Ключ цикла сеанса, Протокол
Telnet/ANSI 334

Количество

Окна опроса

группа RRM 272

Окна опроса, узкополосный
 радиомодуль 260

Повторы

группа RRM 272

Повторы, узкополосный
 радиомодуль 261

Коллизия

Размер

группа RRM 272

узкополосный радиомодуль 261

Комбинация, Группа RRM 274

компактный приемопередатчик 25

компьютер администратора
 платформа 33

Конвертировать 7-битовые
последовательности в 8-битовые
Эмуляция ANSI 332

консоль

подключение к 26

порт

№ кабеля 19387 B-2

выводы B-1

конфигурация
 мини-контроллер 285–340
Конфигурация 9010 284
конфигурация базовой станции 284
конфигурация клиента для режима
 безопасности WPA/WPA2 Enterprise
 (RADIUS) C-25
конфигурация по умолчанию,
 восстановление 284, 292
Критичность, Журналы регистрации
 событий 134

Л

Лимит размера поля

 Эмуляция 3274 304

 Эмуляция 5250 322

Линия передачи

 Эмуляция 3274 299

 Эмуляция 5250 316

Локальные процедуры

 Эмуляция 3274 296

 Эмуляция 5250 313

Локальный IP-адрес для связывания

 Протокол Telnet/3274 306

 Протокол Telnet/5250 324

 Протокол Telnet/ANSI 334

М

Максимальное число попыток

 автоматических сеансов telnet

 Протокол Telnet/ANSI 339

Максимальный

 Размер экрана,

 Эмуляция ANSI 328

Максимум

 Размер сегмента сообщения

 группа RRM 272

 Размер сегмента сообщения,

 узкополосный радиомодуль 261

 Сеансов на терминал

 Протокол Telnet/3274 306

 Протокол Telnet/5250 323

 Протокол Telnet/ANSI 333

Маячок

 Интервал

 802.IQ 344

 Интерфейсы, 802.IQv1 347

 Порт UDP, 802.IQv2 347

 межкадровые интервалы по

 отношению к QoS 215

МЕНЮ «HOST» (ГЛАВНОЕ УСТРОЙСТВО)

 мини-контроллер 292

 Меню подключений 281, 284

 местоположение, описание 65

 мини-контроллер

 конфигурация 285–340

 сети 287

 эмуляции 287

 мониторинг сеансов

 навигация 67

 обзор 68

 обновление информации 70

 просмотр информации о сеансе 69

 мониторинг целостности

 соединений 141

 мосты, WDS 231

 мошеннические точки доступа 141

 мощность передачи, настройка 187

Н

Набор символов верхнего регистра

 (GR), Эмуляция ANSI 332

Набор символов нижнего регистра

 (GL), Эмуляция ANSI 332

 направленная антенна 21

 напряжение, входное 21, 366

Настройка имен LU

 Протокол Telnet/3274 307

Настройка имен устройств

 Протокол Telnet/3274 326

Начальное время на передачу и

 подтверждение, 802.IQv1 346

 ненаправленная антенна 21

Не уведомлять об изменении сетевого

 статуса, эмуляция 9010/TCP/IP 284

Номер автоматического терминала,

 Функции радиоканала 280

 Номер главного устройства,

 конфигурация базовой

 станции 283, 290

О

 обзор функций 11

 обзор функций оркестровки 14

Область команд

 Эмуляция 3274 304

Эмуляция 5250 322
 обновление ПО
 802.IQv2 343
 Обновление прошивки 10
Общие параметры, узкополосный
 радиомодуль 258
 описание заводских настроек 29
Опрос монитора, эмуляция
 9010/TCP/IP 284
**Отправить запрос на прерывание
 программы IAS как ключ
 прерывания**, *Протокол
 Telnet/3274* 308
**Отправить запрос на прерывание
 процесса IAS как системный
 запрос** 308
 очереди, настройка для QoS 221

П

пакетная передача данных
 по отношению к QoS 217
 память 366
 параметры
 изменение в веб-браузере 26
 Параметры 802.11 (экран «Wireless
 Settings» (Параметры беспроводной
 сети)) 161, 167
 Параметры внутреннего интерфейса,
 Параметры Ethernet 154
 Параметры времени 351
 Параметры гостевого интерфейса,
 Параметры Ethernet 157
Параметры групп, Группа RRM 274
Параметры подключений
 Режим RRM 264
 Режим базовой станции 258
 параметры по умолчанию, для 9160 G2
 Wireless Gateway 29
 параметры проводной сети 177
Параметры протокола опроса
 RA1001A 260
 Группа RRM 271
Параметры радиомодуля
 RA1001A 263
 Группа RRM 273
Параметры радиомодуля
 RA1001A 257

пароль
 в разделе «Basic Settings»
 (Базовые параметры) 53
 сетевые параметры для
 администратора 53
Первый локальный порт терминала
 Протокол Telnet/3274 306
 Протокол Telnet/5250 324
 Протокол Telnet/ANSI 334
**Первый порт прослушивания
 терминала**
 Протокол Telnet/3274 306
 Протокол Telnet/5250 324
 Протокол Telnet/ANSI 334
Первый терминал 283, 291
 передача/получение информации 139
 Передача голоса по протоколу IP
 высокое качество обслуживания с
 QoS 209
 период DTIM, настройка 187
 петли, WDS 233
Печать строки
 Эмуляция 3274 303
 Эмуляция 5250 321
 питание
 подключения 42
 требования 21, 366
 платформа
 требования к клиенту 35
 требования к компьютеру
 администратора 33
Повторы, Количество 261
 поддерживаемые платформы
 клиент 35
 компьютер администратора 33
 подключение
 Ethernet 24
 видеотерминал 26
 консоль 26
 терминалы ANSI 26
Позывной
Период
 группа RRM 273
Период, узкополосный
 радиомодуль 262
Строка
 группа RRM 273
Строка, узкополосный
 радиомодуль 263

пользователь
 аутентификация
 настройка на клиенте
 IEEE 802.1x C-17
 настройка на клиенте WPA/WPA2
 Enterprise (RADIUS) C-25
 учетные записи
 для встроенного сервера
 аутентификации 71
 резервное копирование и
 восстановление 77
 порог RTS, настройка 187
Пороговое значение
 Эмуляция ANSI 329
 порог фрагментации, настройка 187
Порт, параметры RA1001A 264
 порты
 выводы
 консольный порт B-1
 разъем RJ-45 (10BaseT) B-3
 местонахождение 23
 оборудование 41
 последовательный
 светодиодные индикаторы
 состояния 25
 скорость передачи данных 26
 последовательный порт
 Последовательный порт
 ввода/вывода
 Эмуляция 3274 303
 Эмуляция 5250 320
Префикс имени LU
 Протокол Telnet/3274 307
Префикс имени устройства
 Протокол Telnet/5250 326
Проверка дублирования номера
терминала при прямом
TCP-подключении, Функции
 радиоканала 278
 Простой протокол сетевого управления
 (SNMP) 243
Протокол
 Идентификатор типа, 802.IQv1 346
 протокол
 адаптивный опрос/коллизия 254
 радиомодуль
 адаптивный опрос/коллизия 254
 временное
 мультиплексирование 253

переключение сотового канала
 связи 253
 Протокол адаптивного
 опроса/коллизии 254
Процедуры
 Эмуляция 3274 296
 Эмуляция 5250 313
 процессор 366
Прямая отправка
 Эмуляция 3274 295
 Эмуляция 5250 312
Прямые TCP-подключения для
TekTerm, Функции радиоканала 278
Пустое поле
 Эмуляция 3274 295
 Эмуляция 5250 312

Р

Работа в режиме сотовой связи,
 Функции радиоканала 277
 радиомодули
 протоколы (адаптивный опрос,
 IEEE 802.11) 254
 радиомодуль
 SuperAG 187
 включение и выключение 187
Время ожидания терминала
протокола опроса 277
Время ожидания терминала
протокола опроса в
процентах 278
Диапазон автоматического
назначения адресов
радиомодулям 278
 диапазоны скорости 187
Идентификатор опроса 277
 интервал маячка 187
 максимальное количество
 станций 187
 мощность передачи 187
 настройка параметров 187
 настройка точек доступа с одним или
 двумя радиомодулями 187
Номер автоматического
терминала 280
 период DTIM 187
 порог RTS 187
 порог фрагментации 187
 радиомодуль 802.11A/G 366

- радиомодуль 802.11G 366
 - режим IEEE 802.11 187
 - светодиодные индикаторы
 - состояния 25
 - спецификации 366
 - Срок годности** 279
 - узкополосный RA1001A 367
 - управление каналами объединенных в
 - кластер точек доступа 79
 - установка и антенны 20
 - установленная конфигурация 10
 - широковещательный режим Turbo, не
 - рекомендуется 9, 185
 - радиомодуль 802.11A/G 366
 - радиомодуль 802.11G 366
 - Размер окон опроса**
 - группа RRM 272
 - узкополосный радиомодуль 261
 - Разрешить**
 - Сеансы TCP, ANSI/Telnet** 339
 - Разрешить имена виртуальных устройств, Протокол Telnet/5250** 325
 - Разрешить нулевой символ**
 - Эмуляция* 3274 293
 - Эмуляция* 5250 311
 - разъемы
 - RJ-45 B-3
 - Расширенные параметры 802.11 (экран «Radio Settings» (Параметры радиомодуля)) 185, 194
 - расширенный набор служб с мостом WDS 231
 - режим RRM 264
 - режим безопасности «простой текст»
 - использование 101
 - конфигурация клиента C-12
 - настройка 110
 - режим безопасности «Статическое WEP-шифрование»
 - использование 101
 - на ссылках WDS 233
 - настройка 111
 - режим безопасности WEP
 - использование 101
 - конфигурация клиента C-14
 - настройка 111
 - режим безопасности WPA/WPA2 Personal (PSK)
 - конфигурация клиента C-34
 - режим безопасности WPA Enterprise
 - использование 105
 - настройка 122
 - режим безопасности WPA Personal
 - использование 104
 - настройка 119
 - режим работы
 - относительная влажность воздуха 365
 - температура 365
 - Режим работы, базовая станция** 259
 - режимы Atheros Turbo 9, 185
 - резервное копирование
 - база данных учетных данных пользователей 77
 - ссылки, WDS 233
- С**
- светодиодные индикаторы 25
 - Свободное окно**
 - Фактор окна**
 - группа RRM 272
 - Фактор окна, узкополосный радиомодуль** 262
 - Сеансы 67
 - сервер NTP
 - настройка точки доступа для использования 352
 - сервер аутентификации
 - для режима безопасности IEEE 802.1x 116
 - для режима безопасности WPA Enterprise 122
 - сервер связи 9500, режим сотовой связи 277
 - сертификат
 - безопасность для клиента IEEE 802.1x C-21
 - безопасность для клиента WPA/WPA2 Enterprise (RADIUS) C-30
 - получение сертификата TLS-EAP для клиента C-41
 - сетевые интерфейсы 366
 - сеть, обзор функций 15
 - Сигнал**
 - Эмуляция* 3274 294

Эмуляция 5250 312
синхронизация кластера 63
скорость передачи данных,
последовательный 26
Скрытый совпадающий символ
Эмуляция 3274 303
Эмуляция 5250 320
События 132
события
журнал 132
мониторинг 132
Совместно используемый канал
группа RRM 271
Совместно используемый канал,
базовая станция 260
Сообщение
Лимит режима
группа RRM 272
Лимит режима, узкополосный
радиомодуль 262
Размер (базовая станция) 268
сообщения об изменении сетевого
статуса 284
соответствие требованиям Wi-Fi 11
соседние точки доступа 141
Соседний офис 91
сотовый канал связи
база 255, 277
переключение 253
Сохранение страниц
Эмуляция ANSI 330
Сохранение страниц с учетом
двухбайтовых символов, Эмуляция
ANSI 331
спецификации
радиомодуль 802.11A/G 366
радиомодуль 802.11G 366
узкополосный радиомодуль
RA1001A 367
физические свойства 365
Спецификации питания через Ethernet
(POE) 366
Список функциональных клавиш,
Эмуляция ANSI 330
Срок годности, Функции
радиоканала 279
стандарты 11

станции
См. также клиент
настройка максимально допустимого
количества 187
Статус радиокарты
меню настройки узкополосного
радиомодуля 256
Страницы
Эмуляция 3274 298
Эмуляция 5250 316
Строка ввода
Эмуляция 3274 304
Эмуляция 5250 321
Т
теги 802.1p 217
Терминал
Время ожидания в автономном
режиме
802.IQ 344
Тип
Протокол Telnet 5250 323
Протокол Telnet/3274 305
Протокол Telnet/ANSI 333
терминал
подключение монитора 26
Тип обслуживания См. ToS 213
Только передача пакетов 802.IQ,
802.IQ 347
точка доступа
QoS 209
балансировка нагрузки 201
безопасность 97
гостевая сеть 169
кластеризация 60
мониторинг 129
мост WDS 229
параметры Ethernet
(проводной сети) 147
параметры беспроводной сети 159
радиомодуль 183
управление пользователем 71
фильтрация MAC-адресов 195
требования к антеннам 21, 22
требования к охране окружающей среды
относительная влажность воздуха при
работе 365
температура хранения 365
температурный режим работы 365

требования к техническому обслуживанию 20
 требования по охране окружающей среды 19
 обзор 19

У

Удаленная печать

Эмуляция 3274 298

Эмуляция 5250 315

Удаленные радиомодули, Группа RRM 275

Узел ретрансляции журнала событий для сообщений ядра системы, Журналы регистрации событий 135

узкополосный радиомодуль

Активный канал параметр 264

двухуровневая модуляция 263

параметры настройки 255, 264

Параметры подключений, Режим RRM 264

Параметры подключений, Режим базовой станции 258

Параметры протокола опроса 260

Параметры радиомодуля 263

Порт параметр 264

четырёхуровневая модуляция 263

узкополосный радиомодуль RA1001A

конфигурация 255

спецификации 367

управление каналами объединенных в кластер точек доступа
 навигация 81

общие сведения 81

пример 82

просмотр/настройка блокировки 85

расширенные параметры 86

рекомендуемые назначения каналов 86

управление ключами, безопасность 100

уровни модуляции, узкополосный радиомодуль 263

условные обозначения в тексте 7

установка

LAN 24

антенны 24

безопасность xvii

кабель питания 24

требования к охране окружающей среды 365

требования по охране окружающей среды 19

установка LAN 24

устранение проблем при запуске 47

утверждения xvi

утверждения требований к электробезопасности xvi

Ф

физические свойства

описание 365

спецификации 365

фильтрация MAC-адресов, настройка 198

флэш-память 366

Функции радиоканала, параметры настройки 275–281

Функциональная клавиша n

Список функциональных клавиш 3274 310

5250 327

ANSI 340

Ц

цвета и стиль пользовательского интерфейса 55

Ч

Часовой пояс 353

Ш

Широковещательный идентификатор SSID 108

широковещательный режим Turbo, не рекомендуется 9, 185

шифрование в различных режимах безопасности 100

Штрихкод

Эмуляция 3274 304

Эмуляция 5250 321

Э

эмуляции

3274/Telnet 292–310

5250 310–327

9010/TCP/IP 284

ANSI 328–340

Указатель

обзор 287

Эмуляция

конфигурация

мини-контроллера 291

Эмуляция 5250 310–327

Эмуляция 9010 284

Эмуляция ANSI 328–340

Эхо, Эмуляция ANSI 329