RAPIRA RS3

Руководство пользователя

ООО «НПО РАПИРА», 2024г.

Оглавление

Введение

Версия документа: **2.1.99** (2024-04-09 13:52:31 +0300)

Настоящее Руководство по эксплуатации распространяется на радиомаршрутизатор, соответствующий ТУ № 464-002-41540932-2023. Руководство содержит сведения о конструкции разработанного радиомаршрутизатора, его принципах действия, технических характеристиках, его модификациях, а также указания, необходимые для правильной и безопасной эксплуатации, оценки его технического состояния, а также сведения по утилизации радиомаршрутизатора.

Для обеспечения эксплуатации радиомаршрутизатора необходим следующий обслуживающий персонал:

- системный программист, требуемое образование – высшее по специальности: Вычислительная математика
- инженер-электронщик, требуемое образование – высшее, по специальности: Радиотехника

Радиомаршрутизатор монтируется на улице на высотных объектах, таких как крыши, вышки, мачты и т.п, которые очень часто подвержены действию атмосферного статического электричества, поэтому обязательно должны быть приняты меры по заземлению устройства, а также по защите оборудования и людей, имеющих контакт с корпусом радиомаршрутизатора, креплением маршрутизатора, мачтой и кронштейнами, приемо-передающей антенной и любыми кабелями, присоединенными к радиомаршрутизатору.

Руководство распространяется на все модификации радиомаршрутизатора, поскольку все модификации радиомаршрутизатора унифицированы в части аппаратной платформы, а также в части программного обеспечения.

Глоссарий

Ниже представлен список сокращений и терминов, наиболее часто встречающихся в документе:

- ACL - списки контроля доступа
- ARP - протокол разрешения адресов
- AP - базовая станция
- CPE - клиентская станция
- CLI - интерфейс командной строки
- DHCP - протокол динамической конфигурации хоста
- DNS - служба доменных имён
- LAN - локальная сеть
- MTU - максимальный размер блока данных одного пакета в байтах, который может быть передан на канальном уровне протокола TCP/IP
- NAT - преобразование сетевых адресов
- POE - (Power Over Ethernet) технология, позволяющая запитать радиомаршрутизатор через кабель снижения
- PTP - система «Точка-точка»
- PTMP - система «Точка-многоточка»
- PuTTY - утилита для подключения к радиомаршрутизатору по протоколу SSH
- SSID - идентификатор сети
- SSH - протокол безопасного доступа к консоли на основе системы кодирования с открытыми ключами.
- TFTP - протокол, использующийся для передачи данных при обновлении ПО и настройке радиомаршрутизатора
- VLAN - виртуальная локальная компьютерная сеть
- WPA - протокол шифрования данных, передаваемых по беспроводной сети
- WDS - параметр, включающий режим беспроводного (прозрачного) моста
- АФТ - антенно-фидерный тракт
- кабельная сборка - высокочастотный кабель (фидер) для передачи СВЧ-сигнала с малыми потерями
- кабель снижения (FTP cat.5e) - кабель для передачи данных и питания, соединяющий радиомаршрутизатор с инжектором POE
- поллинг - алгоритм опроса базой клиентских станций, позволяющий распределять передаваемый трафик между станциями по заданным правилам
- РЭС - радиоэлектронное средство

Описание и работа изделия

Назначение изделия

Радиомаршрутизатор спроектирован для работы в сетях связи общего пользования и предназначен для передачи и приема цифровых данных со скоростью от 1 до 866[1] Мбит/с на расстояния от 100 м до 100 км и более (при условии обеспечения приемлемой энергетики канала).

Радиомаршрутизатор применяется для построения территориально – распределенных широкополосных сетей беспроводного абонентского доступа к ресурсам Интернет, телефонии и других сетей связи общего пользования, а также создания корпоративных и ведомственных сетей с интеграцией голоса, видео, телеметрии и т.д.

Радиомаршрутизатор может быть использован для создания магистральных скоростных каналов "точка – точка", протяженных линий связи с ретрансляцией, или распределенных региональных сетей "точка – многоточка" с одной или несколькими базовыми станциями и множеством клиентов.

Радиомаршрутизатор имеет защищенное всепогодное исполнение, позволяющее размещать его прямо под открытым небом в непосредственной близости от приемо-передающей антенны. Всепогодное исполнение конструкции радиомаршрутизатора решает задачу, связанную с надежной герметизацией электронных модулей. Данное всепогодное исполнение реализуется с помощью специального корпуса и герметизированных разъемов, которые позволяют применять радиомаршрутизатор в диапазоне температур от -60^{o}C до +55^{o}C, а так же обеспечивают ему защищенность от частиц и влаги класса IP67 по ГОСТ 14254-80.

---

1. Для устройств с поддержкой протокола 802.11ac

Технические характеристики

Радиомаршрутизатор имеет следующие технические характеристики:

Таблица 1. Технические характеристики RAPIRA RS3

Параметры радиоинтерфейса	
Диапазоны частот	2312-2712 МГц 2412-2472 МГц 5005-6075 МГц 6075-6425 МГц
Шаг сетки частот	Минимальный - 5 МГц

Параметры радиоинтерфейса	
Технология расширения спектра	• OFDM (IEEE 802.11a/n/ac) – для диапазонов 5xxx-64xx МГц • CCK, OFDM (IEEE 802.11b/g/n) для диапазона 2xxx МГц
Модуляция	• OFDM: BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM • CCK: BPSK, QPSK, DQPSK, DBPSK
Скорость передачи в диапазоне 2412-2472 МГц	300, 270, 240, 180, 120, 90, 60, 30 Мбит/с (IEEE 802.11n) 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Мбит/с (IEEE 802.11b/g)
Скорость передачи в диапазоне 5005-6075 МГц	866, 780, 650, 585, 520, 390, 260, 195, 130, 65 (IEEE 802.11ac) 300, 270, 240, 180, 120, 90, 60, 30 Мбит/с (IEEE 802.11n) 54, 48, 36, 24, 18, 12, 9, 6 Мбит/с (IEEE 802.11a)
Скорость передачи в диапазоне 6075-6425 МГц	300, 270, 240, 180, 120, 90, 60, 30 Мбит/с (IEEE 802.11a) 54, 48, 36, 24, 18, 12, 9, 6 Мбит/с (IEEE 802.11n)
Выходная мощность передатчика	От 10 до 30 дБм (в зависимости от выбранного канала и скорости передачи)
Пороговая чувствительность приемника (IEEE 802.11ac)	–72 дБм @ MCS9 –77 дБм @ MCS7 –95 дБм @ MCS0
Пороговая чувствительность приемника (IEEE 802.11a/n)	–75 дБм @ MCS7 –96 дБм @ MCS0 –78 дБм @ 54 Мбит/с –79 дБм @ 48 Мбит/с –83 дБм @ 36 Мбит/с –86 дБм @ 24 Мбит/с –90 дБм @ 18 Мбит/с –91 дБм @ 12 Мбит/с –92 дБм @ 9 Мбит/с –96 дБм @ 6 Мбит/с

Параметры радиоинтерфейса	
Пороговая чувствительность приемника (IEEE 802.11b/g/n)	**OFDM** –73 дБм @ MCS7 –96 дБм @ MCS0 –78 дБм @ 54 Мбит/с –79 дБм @ 48 Мбит/с –83 дБм @ 36 Мбит/с –86 дБм @ 24 Мбит/с –90 дБм @ 18 Мбит/с –91 дБм @ 12 Мбит/с –92 дБм @ 9 Мбит/с –96 дБм @ 6 Мбит/с **CCK** -94 дБм @ 11 Мбит/с -100 дБм @ 1 Мбит/с
Ширина спектра сигнала по уровню –3dB (IEEE 802.11ac)	20 / 40 / 80 МГц
Ширина спектра сигнала по уровню –3dB (IEEE 802.11n)	20 / 40 МГц
Ширина спектра сигнала по уровню –3dB (IEEE 802.11a/b/g)	5 / 10 / 20 / 40[1] МГц
Эффективная пропускная способность (IEEE 802.11ac)	до 480 Мбит/с
Эффективная пропускная способность (IEEE 802.11n)	до 220 Мбит/с
Эффективная пропускная способность (IEEE 802.11a)	до 56 Мбит/с
Эффективная пропускная способность (IEEE 802.11g)	до 35 Мбит/с
Разъем для антенны (для моделей без встроенной антенны)	N-типа Female (розетка), 50 Ом, 1-2шт
Безопасность и аутентификация для радиоканала	WPA-PSK, WPA-EAP с шифрованием TKIP и AES-256; WEP (64, 128, 154)
Способы доступа к среде (неколлизионный)	неколлизионный адаптивный динамический поллинг (опрос)
Способы доступа к среде (коллизионный)	CSMA/CA, прослушивание несущей с предотвращением коллизий
Управление выходной мощностью	от 1 до 30 дБм

Параметры радиоинтерфейса	
Динамический выбор скорости	в зависимости от SNR и потерь фреймов при передаче их в радиоканале
Исполнение	Внешнее, всепогодное
Диапазон рабочих температур	от -60°C до +55°C
Допустимая влажность	защита от частиц и влаги соответствует классу IP67
Крепление	на трубу диаметром 20-60 мм, уголок, хомут и подпятник в комплекте
Питание	24В (в стандартной комплектации) 48В (при установленном преобразователе напряжения) потребляемая мощность не более 24 Вт
Удаленное питание	через проводный интерфейс, до 100м, не требует отдельного питающего кабеля, инжектор PoE в комплекте (Passive PoE)
Проводной интерфейс	Ethernet 10/100/1000BaseT, герметичный соединитель витой пары в комплекте (IP67)

1. Для протокола IEEE 802.11a ширина спектра сигнала, равная 40 МГц, доступна для каналов 5210, 5250, 5290, 5760 и 5800 МГц.

Состав радиомаршрутизатора

В состав радиомаршрутизатора входят:

- внешний всепогодный блок изделия
- крепежно-поворотное устройство (КПУ)
- инжектор питания
- источник питания
- герметичный соединитель витой пары (IP67)
- компакт-диск с программным обеспечением и руководством пользователя

Более детально состав изделия рассматривается в разделе Стандартная комплектация радиомаршрутизатора.

Устройство и работа

Радиомаршрутизатор любой модификации имеет два вида интерфейсов: проводные, типа 1000BaseT для стыка с аппаратурой передачи данных, а также беспроводные интерфейсы, поддерживающие связь между радиомаршрутизаторами посредством радиоканала. С помощью проводных интерфейсов радиомаршрутизаторы могут быть соединены как между собой, так и с любым телекоммуникационным оборудованием, имеющим интерфейсы типа 1000BaseT.

Конструкция беспроводной широкополосной сети на основе различных модификаций данного радиомаршрутизатора осуществляется согласно топологии вида: Расширенная зона обслуживания (extended service set, ESS). Зона обслуживания (service set) в общем случае – это логически сгруппированные беспроводные устройства. Как правило, такая группа устройств имеет собственный идентификатор зоны обслуживания (service set identifier, SSID).

Использование топологии ESS подразумевает наличие как минимум одного особого устройства – базовой станции. Базовая станция – это центральный пункт связи для всех станций, входящих в данную зону обслуживания. Клиентские станции в топологии ESS не могут связываться непосредственно одна с другой. Вместо этого они связываются с базовой станцией, а уже она направляет фреймы станции адресату. При включении, клиентская станция должна обязательно осуществить процедуру ассоциации с какой-либо базовой станцией зоны обслуживания. В каждый отдельно взятый момент времени, клиентская станция может быть ассоциирована только с одной базовой станцией, а базовые станции, в свою очередь, могут быть соединены между собой по проводным каналам связи.

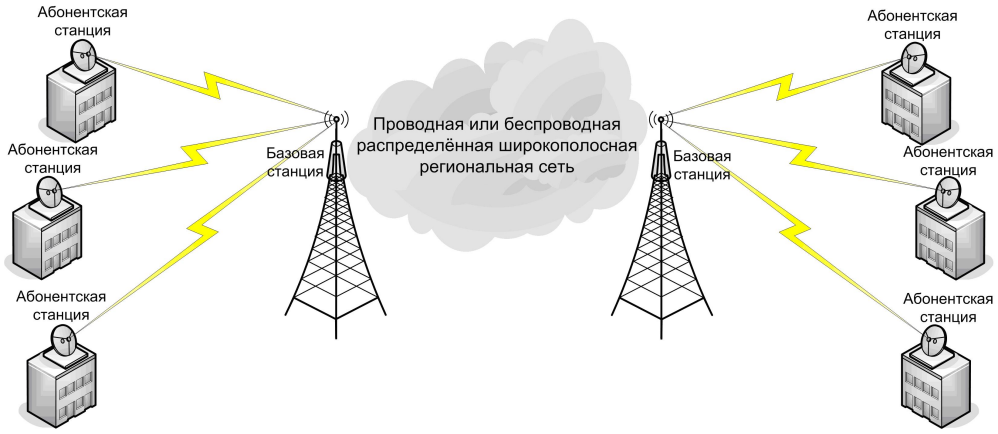


Рис. 1. Структура Расширенной зоны обслуживания ESS

Кроме базового доступа к среде передачи данных, описанного в семействе стандартов IEEE 802.11, который заключается в прослушивании несущей и предотвращении коллизий (метод CSMA/CA), радиомаршрутизатор поддерживает также и альтернативный метод доступа к среде передачи данных - неколлизионный адаптивный динамический поллинг (опрос).

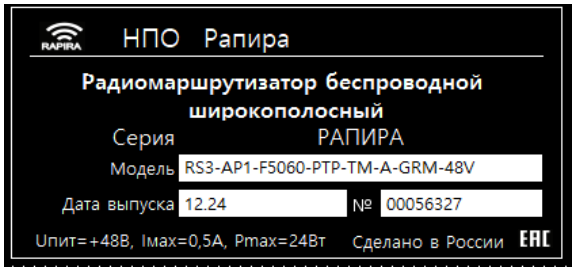
Стоит заметить, что в семействе стандартов IEEE 802.11 кроме базового доступа к среде передачи данных, также описан и механизм поллинга (так называемый режим PCF), однако, адаптивный динамический поллинг, применяемый в настоящем радиомаршрутизаторе, существенно отличается от описанного в стандарте и является отдельной самостоятельной разработкой. Механизм адаптивного динамического поллинга обеспечивает неколлизионный доступ к среде передачи данных, при котором ни одна клиентская станция не может осуществлять передачу, до тех пор, пока базовая станция не опросит ее.

Данный механизм позволяет эффективно решать проблему «скрытых станций», которая заключается в большом числе коллизий, возникающих при использовании базового метода доступа к среде в региональных сетях из-за того, что клиентские станции «слышат» в радиоэфире только Базовую станцию, и не слышат других Абонентских. В результате чего

часто две Клиентские станции начинают вести передачу одновременно, что неизбежно приводит к коллизии и к потере передаваемых фреймов. Кроме того, механизм адаптивного динамического поллинга обеспечивает гарантированную задержку передачи фреймов между станциями, чего не может обеспечить базовый механизм доступа к среде. Данное свойство адаптивного динамического поллинга дает возможность эффективно использовать беспроводные сети для передачи трафика, критичного к вариации задержки доставки фреймов, например для передачи голоса и видеоинформации. Радиомаршрутизаторы, объединенные в сеть, могут выступать как устройствами 2 уровня модели OSI (мосты), так и устройствами 3 уровня модели OSI (маршрутизаторы), в зависимости от структуры, а также от функций, которые должна выполнять беспроводная сеть.

Маркировка

Все радиомаршрутизаторы, поставляемые ООО «НПО РАПИРА», оснащены шильдом, который устанавливается на корпусе устройства со стороны крепления.



На шильде указаны: производитель, логотип фирмы, код модели, дата выпуска, серийный номер устройства, страна производитель и электрические параметры модели.

При обращении в службу технической поддержки, пожалуйста, называйте код модели изделия.

RSx	-	**тип**	-	**F0000**	-	**режим**	-	**дополнения**
1		2		3		4		5
Пример: **RS3-CPE-F5060-PTP-TM-A-GRM-48V**								

№	ПАРАМЕТР	ПРИМЕР
1	**Rx, RSx** - общее название линейки устройств, где X - поколение устройства: **R1** - линейка устройств, производимых до 2007 года. **R2** - линейка устройств, производимых с 2007 по 2011 год. **RS3** - линейка устройств, производимых с 2011 года по настоящее время.	**RS3**- третье поколение устройств
2	**Тип** устройства, где: **APx** - базовое устройство, где **x** – количество радиоинтерфейсов **CPE** – клиентское устройство	RS3-**AP1**... - базовая станция с одним радиоинтерфейсом

№	ПАРАМЕТР	ПРИМЕР
3	**F0000** - поддерживаемый частотный диапазон, где: **первые два цифровые символа** - обозначение начальной границы частотного диапазона **последние два цифровые символа** - обозначение конечной границы частотного диапазона	RS3-CPE-**F2425**... - клиентское устройство, работающее в диапазоне 2,4 – 2,5 ГГц
4	**Режим** - режим работы устройства, где: **PTP** – режим «точка-точка» **PTMP** – режим «точка-многоточка»	RS3-AP1-F5060-**PTMP** – базовая станция, работающая в режиме «точка-многоточка»
5	**Дополнения** – дополнительная информация об устройстве, где: **T** – интегрированная антенна **A** – встроенное устройство термостабилизации **M** – поддержка протокола MIMO **C** – поддержка протокола AC **48V** – встроенный преобразователь питания **GRM** – встроенный герметичный разъём	RS3-CPE-F5060-PTP-**TM** – клиентское устройство с интегрированной антенной, работающее в диапазоне 4,9-6,1 ГГц и поддерживающее протокол MIMO

Эксплуатационные ограничения

Эксплуатационные ограничения на Радиомаршрутизатор серии RAPIRA RS3.

Таблица 2. RAPIRA RS3. Эксплуатационные ограничения.

Напряжение питания	• 24-30В (в стандартной комплектации) • 18-72В (при установленном преобразователе напряжения)
Температура эксплуатации	от -60°С до +55°С (при установленном термостабилизаторе)
Максимально допустимый радиосигнал на входе беспроводного интерфейса	не более -3 дБм

Продукты серии RAPIRA RS3

Общая информация

Инструкция относится к продуктам ООО «НПО РАПИРА». В этой главе представлена общая информация по характеристикам и различным моделям продуктов серии RAPIRA RS3.

Базовые станции (AP)

Базовые станции (AP) управляют передачей данных внутри беспроводной сети и являются основной точкой доступа к сети для клиентского оборудования.

AP устанавливает связь со всеми клиентскими станциями (CPE) в системе, чтобы обеспечить каждую из CPE доступом в основную сеть. AP должна быть расположена так, чтобы обеспечить необходимый уровень приемного радиосигнала на CPE для устойчивой работы радиоканалов.

Клиентские станции (CPE)

Клиентское оборудование соединяет пользователей с базовой станцией по беспроводной связи. Такое соединение дает пользователю возможность общаться как с остальными пользователями беспроводной сети, так и сетью (Ethernet).

Предполагает установку на улице. CPE либо интегрирована с антенной, либо снабжена кабельной сборкой N-контактного типа (F), предназначенной для подсоединения внешней антенны. Тем самым, обеспечивается возможность использовать антенны разных типов: рупорные, планарные, офсетные и прямофокусные или другие специализированные антенны.

Беспроводная сеть сконцентрирована на базовой станции, которая является как точкой доступа в LAN (или WAN), так и точкой доступа для конечного пользовательского оборудования CPE (CPE не устанавливает связь и не общается напрямую с другими CPE, они общаются только через базовую станцию). Различные CPE выступают только как конечное звено беспроводного соединения.

Оборудование с интегрированной антенной

Оборудование с интегрированной антенной дает возможность снизить затраты на монтаж, поскольку нет необходимости монтировать отдельно антенну и соединять её через кабельную сборку с радиомаршрутизатором.

Также в этом случае улучшается качество связи по беспроводному каналу (по сравнению с решениями, где применяется внешняя антенна аналогичного типа), поскольку:

- отсутствуют дополнительные потери сигнала в антенно-фидерном тракте (АФТ)
- используется короткая внутренняя кабельная сборка с меньшим коэффициентом

затухания

- резко снижается деградация компонентов АФТ вследствие отсутствия прямого влияния внешней среды и возможного негативного влияния человеческого фактора при монтаже

Оборудование с внешней антенной

Внешние антенны используются либо в случае, когда необходимо задействовать антенны с более мощным коэффициентом усиления, чем это позволяет интегрированное решение, либо в случае, когда необходимо пространственно разделить блок маршрутизатора и антенну. Для соединения радиомаршрутизатора с антенной используется кабельная сборка длиной как правило 0.5 или 1.2 метра.

Системы «Точка-многоточка» (PTMP)

Для беспроводного соединения типа PTMP требуется два вида оборудования: оборудование базовой станции (AP) и клиентское оборудование (CPE), устанавливаемое у пользователя (абонента).

Оба типа оборудования могут состоять либо из радиомаршрутизатора с интегрированной антенной, (в данном случае в названии радиомаршрутизатора присутствует индекс **T**), либо радиомаршрутизатора с герметичными разъемами (как правило N-типа) для подсоединения внешней антенны.

Системы «Точка-точка» (PTP)

Соединения (каналы) «точка-точка» используются в случае необходимости прямого беспроводного соединения двух объектов, например для связи между базовыми станциями канала «точки-многоточки» (PTMP) и операционным центром сети, для соединения с магистралью Интернета и т.д.

Подготовка радиомаршрутизатора к использованию

Перед началом использования радиомаршрутизаторов необходимо заранее настроить устройства, которые планируется объединять в сеть, после чего можно приступать к монтажу радиомаршрутизаторов непосредственно на местности.

Предварительные требования к настройке оборудования

Внимание!

При работе радиоканала уровень сигнала не должен превышать **-30 dbm**. Это обусловлено тем, что из-за перегрузки приемного каскада радиомодуля возможен ускоренный износ элементной базы устройства, а в последствии выход устройства из строя.
Напоминаем, что кратковременно максимально возможный уровень сигнала на входе приемника составляет 0.5 мВт (-3 dBm).

Обратите внимание:

При соединении устройств с внешними антеннами кабельными сборками необходимо обеспечить затухание в кабелях не менее 33 дБм.

При настройке устройств с внешними антеннами перед возможной программной настройкой уровня приёмного сигнала необходимо **ДО ВКЛЮЧЕНИЯ** оборудования выполнить следующее:

1. Подключите внешнюю антенну к устройству, используя кабельную сборку. Если при настройке оборудования маршрутизаторы соединяются кабельными сборками напрямую между собой (без использования антенн), то необходимо обеспечить аттенюацию не менее 33 дБ.
2. На всех неиспользуемых радиовыходах установите эквивалент нагрузки равной 50 Ом.

Подайте питание на оборудование и проведите его настройку. После установления ассоциации проверьте, чтобы уровень приемного сигнала не превышал **-30 дБм**. При настройке устройств с интегрированными антеннами уровень приемного сигнала нечасто превышает указанное выше значение, но, при необходимости, он может быть настроен программно командой tx-power.

Для проверки уровня приёмного сигнала воспользуетесь командами signal и associated.

Настройка параметров радиомаршрутизатора RAPIRA RS3

В данном разделе рассказывается как настроить пару маршрутизаторов для обеспечения связи типа "точка-точка." В результате выполнения нижеследующих команд будут настроены основные параметры конфигурации прозрачного моста для обеспечения беспроводной связи БЕЗ НАСТРОЙКИ ДОПОЛНИТЕЛЬНЫХ ПАРАМЕТРОВ, таких как: шифрование, маршрутизация, фильтрация по MAC-адресам, настройка VLAN и т. д.

Внимание!

Параметр расстояния **distance** в данном примере равен 300 метрам. Не забудьте выставить реальное значение значение данного параметра.

Внимание!

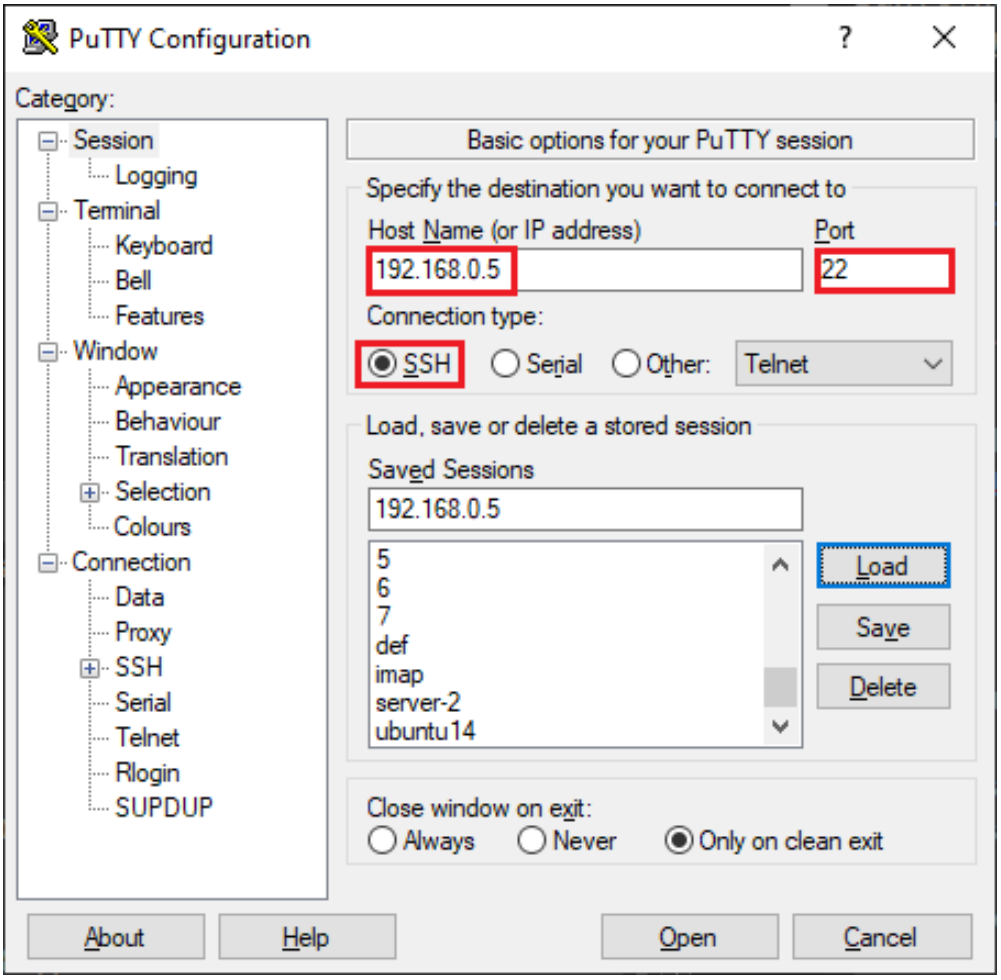
Параметр **ssid** в данном примере равен myssid12345. Не забудьте выставить ваше уникальное значение данного параметра и убедитесь , что данный параметр идентичен на базовом и клиентском маршрутизаторах.

1. Подключитесь к маршрутизатору по протоколу SSH, используя любую утилиту, поддерживающую данный протокол. Мы предлагаем воспользоваться утилитой Putty, запустив её либо с прилагаемого компакт диска, либо скачав по адресу: http://www.chiark.greenend.org.uk/~sgtatham/putty

Внимание!

Перед подключением к устройству убедитесь, что компьютер, с которого производится подключение, находится в этой же подсети.

1. После ввода IP-адреса по умолчанию - 192.168.0.5 - нажмите кнопку `Open`.



1. В появившемся окне введите следующие данные:
   - Стандартный логин: **admin**
   - Стандартный пароль: **123**

Символы пароля при вводе **не отображаются**.

Настройка клиентской станции

Для настройки радиомаршрутизатора введите следующие команды в указанном порядке:

```
RAPIRA: interface bridge 0

RAPIRA: interface bridge 0 ip address 192.168.0.5

RAPIRA: interface bridge 0 no shutdown

RAPIRA: interface Wireless 0

config-if: type station

config-if: channel 5800
//! Не устанавливается tx-power, если channel auto.
config-if: tx-power 26

config-if: wds-mode

config-if: distance 300

config-if: ssid myssid12345

config-if: speed auto auto

config-if: no shutdown

config-if: bridge-group 0

config-if: exit

RAPIRA: interface FastEthernet 0 bridge-group 0
```

После выполнения вышеуказанных команд сохраните конфигурацию:

```
RAPIRA: copy running-config startup-config
```

Настройка базовой станции

```
RAPIRA: interface bridge 0

RAPIRA: interface bridge 0 ip address 192.168.0.6

RAPIRA: interface bridge 0 no shutdown

RAPIRA: interface Wireless 0

config-if: type ap

config-if: channel 5800
```

```
config-if: tx-power 26

config-if: speed  auto auto

config-if: wds-mode

config-if: distance 300

config-if: ssid myssid12345

config-if: mode ht40+

config-if: no shutdown

config-if: bridge-group 0

config-if: exit

RAPIRA: interface FastEthernet 0 bridge-group 0
```

После выполнения вышеуказанной команды соединение с системой будет утеряно. **Не выключая маршрутизатор** заново войдите в систему, используя указанный ранее IP-адрес (192.168.0.6), и сохраните конфигурацию:

```
RAPIRA: copy running-config startup-config
```

Стандартная комплектация радиомаршрутизатора

Как базовое, так и клиентское оборудование как правило включает в себя следующие компоненты:

- **POE-инжектор.** Представляет из себя устройство небольшого размера, которое обеспечивает электропитание и подсоединение радиомаршрутизатора к сетевому оборудованию или к персональному компьютеру. Для подсоединения инжектора питания к радиомаршрутизатору используется так называемый кабель снижения, представляющий собой экранированный кабель для внешней прокладки CAT-5.
- **Крепёжно-поворотное устройство (КПУ).** Предназначено для крепления радиомаршрутизатора на мачте диаметром от 20 до 60мм. В стандартном варианте КПУ состоит их трёх элементов: уголок, хомут и подпятник.
- **Блок питания**. По умолчанию маршрутизатор поставляется с импульсным блоком питания ~220V/=24V. При заказе встроенного преобразователя напряжения - с импульсным блоком питания ~220V/=48V.
- **Герметичный соединитель витой пары**. Обеспечивает герметичное подключение витой пары к маршрутизатору (класс защиты IP67). Состоит из блочной части, вмонтированной в корпус маршрутизатора, и кабельной части, которая устанавливается на кабель снижения при монтаже устройства. Подробности работы с соединителем описаны в разделе Установка герметичного соединителя.
- **Антенна и фидер.** Для ряда моделей предусматривается использование внешней антенны и фидеров. Антенны и фидеры выбираются пользователем на основании тех требований, которые предъявляются к конкретной сети.

Дополнительная комплектация радиомаршрутизатора

По запросу заказчика стандартная комплектация изделия может быть изменена.
В частности, могут быть добавлены следующие компоненты:

- **Термостабилизатор** - обеспечивает **холодный старт** устройства в диапазоне температур -60°С до +55°С
- **Преобразователь напряжения** - обеспечивает необходимое напряжение питания устройства в случае, если длина кабеля снижения превышает 30 метров. Позволяет запитывать устройства от источника постоянного тока напряжением 18-72В
- **Уличная грозозащита СОСНА-М** - устанавливается между инжектором POE и радиомаршрутизатором, обеспечивает как защиту от повреждения высоковольтными импульсами, так и защиту от статического напряжения
- **Уличный инжектор POE** - позволяет запитать радиомаршрутизатор непосредственно на улице (класс защиты корпуса уличного инжектора - IP67)
- **Многопортовый инжектор PoE** - позволяет одновременно запитать несколько PoE-устройств
- **Антенны** с нестандартной диаграммой направленности.

Подробную информацию вы можете получить в нашей службе технической поддержки, написав по адресу: support@nporapira.ru

Установка RAPIRA RS3 на местности

Данный раздел посвящен инсталляции маршрутизатора RAPIRA RS3 на местности.

Прежде чем приступить к установке маршрутизатора RAPIRA RS3 на местности, необходимо выполнить следующее:

- Все компоненты должны быть настроены в соответствии с требованиями, описанными в разделе Подготовка радиомаршрутизатора к использованию.
- Должна быть завершена работа по подготовке места установки оборудования
- Должны быть подготовлены к работе все необходимые инструменты и оборудование
- Монтаж всех компонентов оборудования должен выполняться квалифицированным и профессионально подготовленным персоналом.

Для предотвращения выхода из строя радиомаршрутизатора при монтаже устройств с **внешними антеннами** запрещается подключать питание устройства без установленной нагрузки на выход радиоинтерфейса.

Важно!

При всех высотных монтажных работах рекомендуется использовать молниезащитное оборудование.

Предварительная подготовка

1. Перед началом монтажа радиомаршрутизатора следует убедиться, что имеется прямая видимость до объекта, с которым планируется устанавливать связь. После чего проводятся необходимые расчеты энергетического бюджета и размера 1й зоны Френеля – требуемого свободного пространства вокруг пути распространения радиоволн. Для точных расчетов зоны Френеля Вы можете воспользоваться калькулятором расчета радиуса зоны Френеля.
2. Монтаж изделия осуществляется на кронштейн - хорошо заземленную металлическую трубу диаметром 20 – 60мм.

Внимание!

Кронштейн и мачта должны быть надежно заземлены для исключения поражения оборудования и людей наведенным атмосферным статическим электричеством.

3. Определяется точка получения напряжения ~220В для питания радиомаршрутизатора и место для размещения блока питания, инжектора питания и устройства грозозащиты. Питающая розетка должна обеспечивать мощность не менее 24Ватт. Для обеспечения надежной связи источник должен по возможности обеспечивать бесперебойное питание радиомаршрутизатора.

Внимание!

Место для установки блока питания и инжектора питания, входящих в комплект поставки, должно быть оборудовано заземлением.

4. Следует заранее определить точку соединения радиомаршрутизатора с локальной сетью, коммутатором или иным подключаемым сетевым оборудованием. Размещение блока питания и инжектора питания может осуществляться в заземленной стойке или телекоммуникационном шкафу с сетевым оборудованием, с которым осуществляется соединение.
5. Далее следует определить трассу кабеля снижения, соединяющего радиомаршрутизатор с инжектором питания, а также трассу кабеля, соединяющего инжектор питания с сетевым оборудованием.

Внимание!

Совокупная длина кабеля снижения от радиомаршрутизатора до точки присоединения не должна превышать 95 метров.

Монтаж радиомаршрутизатора

Общий монтаж производится по указанной ниже схеме:

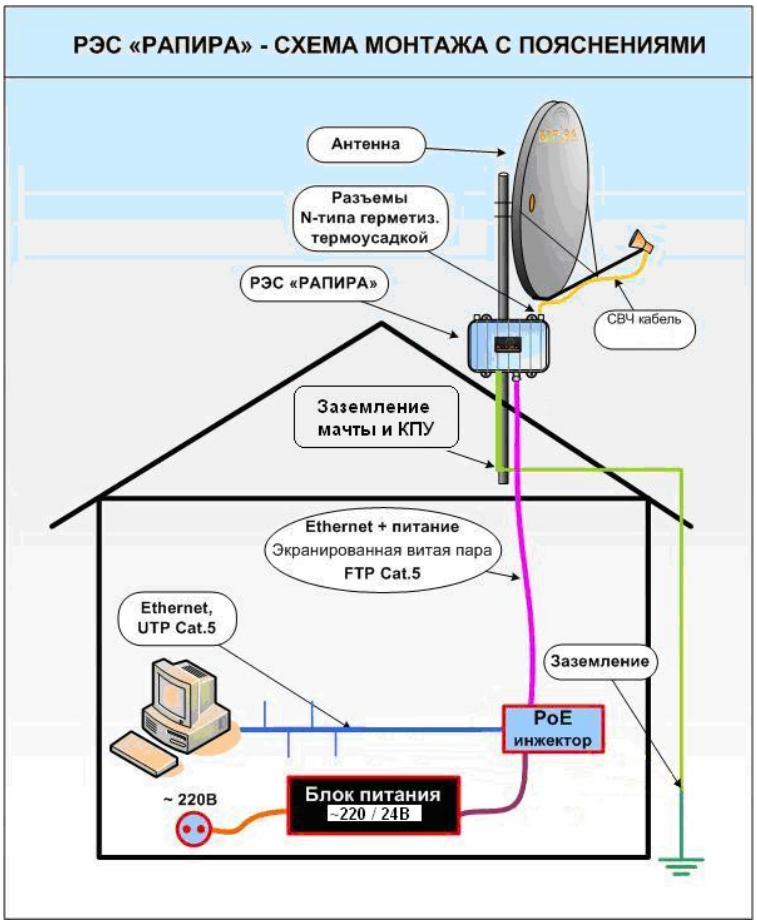


Рис. 2. Схема монтажа радиомаршрутизатора RAPIRA RS3

Монтаж радиомаршрутизатора с интегрированной антенной

1. При помощи метизов из комплекта крепежа закрепите на корпусе радиомаршрутизатора уголок из комплекта КПУ.
2. Зафиксируйте радиомаршрутизатор на трубостойке при помощи хомута, подпятника и комплекта метизов, предварительно произведя «нацеливание» на удаленный объект.
3. Проложите кабель снижения от места размещения инжектора питания до радиомаршрутизатора. В качестве кабеля снижения допускается использование только экранированных кабелей STP, FTP для наружной прокладки, не хуже 5й категории, имеющих 4 пары.
4. Обеспечьте герметичное соединение «витой пары» с разъёмом RJ-45 маршрутизатора, используя герметичный соединитель. Подробная процедура установки соединителя описана в разделе Сборка вилки герметичного соединителя.

Монтаж радиомаршрутизатора с внешней антенной

Для предотвращения выхода из строя радиомаршрутизатора с разъемами для внешней антенны **ЗАПРЕЩАЕТСЯ** подавать питание на радиомаршрутизатор **ДО** подключения антенны.

1. При помощи метизов из комплекта крепежа закрепите на корпусе радиомаршрутизатора уголок из комплекта КПУ.
2. Зафиксируйте радиомаршрутизатор на трубостойке при помощи хомута, подпятника и комплекта метизов
3. Произведите монтаж антенны, по возможности произведя «нацеливание» на удаленный объект.
4. Перед подсоединением ВЧ-кабеля внутренние поверхности разъема кабеля, а так же ответную часть разъема на маршрутизаторе протрите этиловым спиртом (ГОСТ 18300-87).
5. Подключите антенну при помощи высокочастотного кабеля с разъемом N – Male к соответствующему разъему на корпусе радиомаршрутизатора.
    - При подключении ВЧ-кабеля накидные гайки соединителей должны свободно перемещаться по сопрягаемому разъему.
    - Осевые кручения кабеля не допускаются!
    - При монтаже кабеля должны быть приняты меры, предотвращающие образование царапин на кабеле и попадание влаги на место сочленения кабеля с маршрутизатором.
6. Произведите надежную гидроизоляцию мест соединения ВЧ-кабеля, используя термоусадочную трубку с гелем (либо замажьте силиконовым герметиком для наружных работ и соответствующим температурным диапазоном применения). При применении термоусадочной трубки, необходимо произвести её равномерный прогрев термофеном или горелкой. Если антенна не имеет собственного кабеля, в качестве фидера рекомендуется использовать ВЧ-кабель с малыми потерями 8D-FB или

подобный. В этом случае необходимо надежно гидроизолировать соединения на обоих концах.

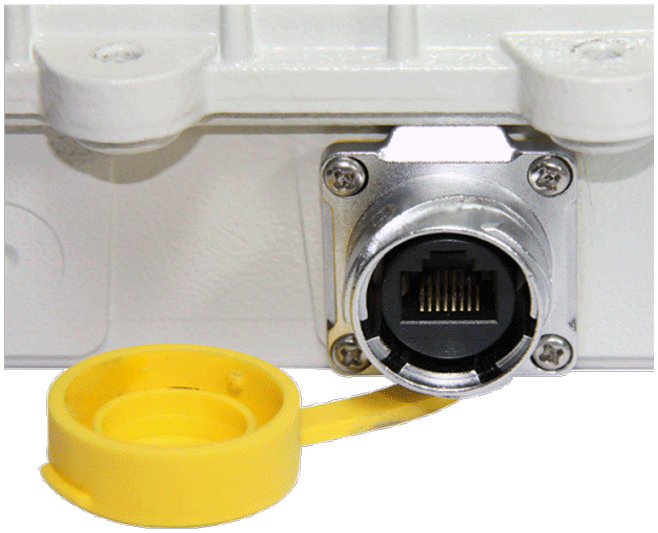
7. Рекомендуется использование антенн с замкнутым по постоянному току центральным ВЧ-контактом. Следует помнить, что кабель вносит существенное затухание ВЧ-сигнала и является антенной для наводок разрядов атмосферного электричества. По возможности следует использовать кабель кратчайшей длины и разъемы высокого качества.
8. Проложите кабель снижения от места размещения инжектора питания до радиомаршрутизатора. В качестве кабеля снижения допускается использование только экранированных кабелей STP, FTP для наружной прокладки, не хуже 5й категории, имеющих 4 пары.
9. Обеспечьте герметичное соединение «витой пары» с разъёмом RJ-45 маршрутизатора, используя герметичный соединитель. Подробная процедура установки соединителя описана в разделе Сборка вилки герметичного соединителя.

Для юстировки антенны можно использовать встроенный в маршрутизатор бипер. Подробнее см. описание команды beeper.

Также точность юстировки можно отслеживать по уровню принимаемого сигнала, см. описание команд signal и associated.

Сборка вилки герметичного соединителя

Герметичный разъем состоит из двух частей, первая часть (гнездо типа RJ-45) установлена на корпусе устройства:



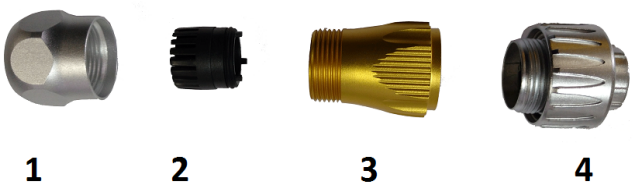
Вторая часть (вилка типа RJ-45) монтируется на нисходящий кабель (см. ниже).

Разъем обеспечивает герметичное соединение не хуже IP67 в собранном состоянии и IP65 при использовании закрывающего колпачка.

Для обеспечения класса защиты IP67 и исключения повреждения при установке разъёма на

кабель выполните с вилкой следующие действия:

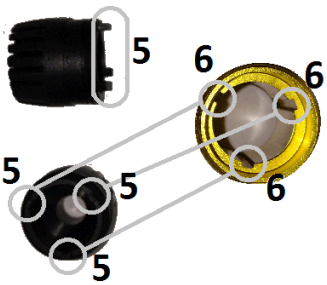
- Открутите накидную гайку (1)
- Выньте цанговый зажим (2) из корпуса разъема (3)
- На кабель последовательно установите накидную гайку (1), зажим (2)
- На кабель установите разъем RJ-45. Схема обжима кабеля описана в Приложении.
- Открутите корпус разъёма (3), для удобства можно вставить разъем в ответную часть на корпусе радиомаршрутизатора.
- Наденьте корпус разъёма (3) на кабель



- Установите разъем RJ-45 в пластиковый фиксатор в байонетном блоке (4) разъёма.

- Разъём устанавливается до характерного щелчка. Установленный разъем RJ-45 в пластиковом фиксаторе выглядит следующим образом :

- Накрутите корпус разъёма (3) на байонетный блок (4)
- Установите цанговый зажим (2) в корпус разъёма и проверьте, что три пластиковые выступа (5) попали в углубления в корпусе (6)



- Накрутите накидную гайку (1). Установленный на кабеле разъём выглядит следующим образом:

Установка герметичного соединителя

- Проверьте, что накидная гайка (1) ослаблена до такого состояния, что кабель свободно проходит через цанговый зажим.

- Проверьте,что корпус разъёма (3) откручен на 2-3 оборота
- Вставьте разъём в ответную часть на корпусе радиомаршрутизатора, для исключения ошибок при установке разъёма у него имеется три направляющие и один ключ
- Удостоверьтесь, что разъем установлен до упора
- Поворачивайте накидную часть на байонетном блоке (4) по часовой стрелке с нажатием на него в сторону корпуса радиомаршрутизатора до характерного защёлкивания байонетного соединения

Внимание!

Повороты байонетной накидной гайки должны быть свободные с небольшим усилием в конце закручивания (защёлкивание байонетного соединения). Если гайка идёт с большим усилием - ослабьте или открутите корпус разъёма (3).

- Закрутите до упора корпус разъёма (3)
- Закрутите до упора накидную гайку (1)

Процедура снятия герметичного соединителя или замена находящегося в нём разъёма RJ-45 описана в Приложении.

Подключение POE

По окончании установки подайте питание на радиомаршрутизатор.

При подключении POE-инжектора к радиомаршрутизатору RAPIRA RS3 необходимо соблюдать следующую последовательность действий:

1. Соедините кабелем снижения POE-разъем инжектора и Ethernet-разъем маршрутизатора.
2. Соедините кабель локальной сети с LAN-разъемом POE-инжектора.
3. Подключите штекер блока питания к DC-разъему POE-инжектора.
4. Подключите блок питания к сети переменного тока.

Осторожно!

Если сетевое оборудование не запитывается по технологии **POE**, не подсоединяйте кабель LAN RJ-45 к порту "POE" POE-инжектора, поскольку данный порт находится под напряжением, что может привести к повреждению внешнего оборудования.

Убедитесь, что индикатор «link» на порту присоединяемого оборудования горит. Если индикатор не загорелся, проверьте исправность всех кабелей, блока питания и правильность обжима соединений.

Настройка радиомаршрутизатора

С чего начать

Интерфейс командной строки

Общее описание

Интерфейс командной строки представляет собой текстовую консоль, с помощью которой происходит взаимодействие пользователя с системой. Данная консоль может быть выведена на экран при помощи любой программы, реализующей функции ssh-терминала (например - PuTTY), а также через системную консоль.

После запуска ssh-терминала в окне конфигурации достаточно указать имя сервера в поле Host name (or IP address) и выбрать Protocol: SSH. В качестве Host Name необходимо указать IP-адрес **192.168.0.5** и выбрать протокол SSH.

Рекомендуем сохранить настройки, указав произвольный текст в поле **Saved Sessions** и сохранив их кнопкой `Save`. В дальнейшем вы сможете начать работу с сервером, загрузив эти настройки. Для этого достаточно сделать двойной щелчок на указанном ранее имени в списке Saved Sessions. При первом входе в систему нужно указать установленные по умолчанию имя пользователя **admin** и пароль **123**.

Используя интерфейс командной строки, пользователь имеет возможность производить точную настройку радиомаршрутизатора, а также управлять его работой. Пользователь при помощи клавиатуры вводит команды, предназначенные для управления, настройки и мониторинга радиомаршрутизатора. Вводимые команды будут отображаться в текстовой консоли и, по завершению ввода команды, после нажатия клавиши “Enter”, встроенная операционная система радиомаршрутизатора произведет обработку команды и выведет на экран результаты работы. Если команда была введена с синтаксическими ошибками, то на консоль будет выведено сообщение об ошибке и указанно место, в котором произошла ошибка.

Большая часть команд консоли сгруппирована в древовидную структуру. Большая часть ветвей (корневых команд) имеют собственные группы команд, которые сгруппированы в различных ветвях по общему для них функциональному признаку. Пользователь, используя команды, имеет возможность перемещаться по ветвям дерева.

Составные части командной строки

Командная строка представляет собой последовательность ключевых слов и значений, с помощью которых составляется необходимая для выполнения команда.

Таблица 3. Правила ввода команд

Части строки:	**Ветвь**	**Подветвь**	**Команда**	**Значение (опция)**
Пример:	Interface	Wireless 0	ip address	192.168.0.5 255.255.255.0

Таблица 4. Составные части командной строки

Ключевые слова	Обобщенное название определенной последовательности символов, которые рассматриваются как единая команда. Ветви, команды и опции являются ключевыми словами.
Ветвь (корневая команда)	Первое ключевое слово (корневая команда), определяет тип выполняемой операции.
Команда (Подветвь)	Дополнительное ключевое слово, определяющее • объект корневой команды • особенности выполнения корневой команды
Значение	Значение относится всегда к какой-либо команде. В зависимости от команды, значение может быть: • пунктом списка (опцией) • числом • текстом Значения могут быть как обязательными, так и необязательными. Значение всегда отделяется от параметра пробелом.
Опция	Ключевое слово, являющееся пунктом списка значений и принадлежащее определенной команде.

Правила ввода команд

Таблица 5. Правила ввода команд

Синтаксис известен	Для ввода известной команды наберите ее в командной строке и нажмите `Enter`.
Синтаксис не известен	Если синтаксис команды не известен, наберите ? для получения подсказки.

Быстрый ввод команд

Таблица 6. Быстрый ввод команд

Автозавершение	Нажмите `TAB` для автозавершения команды или параметра. Должно быть набрано достаточное количество символов, чтобы система смогла определить соответствие набранных символов определенной команде, в противном случае будет выведен список команд, соответствующих введенным символам.
Аббревиатуры	Вы можете использовать аббревиатуры для набора наиболее популярных команд, например: `show ip route` или `sh ip ro` (просмотр содержимого таблицы маршрутизации).

Повтор введенных команд

Вы можете повторить ранее набранные команды, используя клавиши "стрелка вверх" и "стрелка вниз".

Условные обозначения

{ } - фигурные скобки; ключевое слово, обрамленное фигурными скобками, является обязательным для ввода

[ ] – квадратные скобки; ключевое слово, обрамленное квадратными скобками, является необязательным и может быть опущено при вводе команды

Веб-интерфейс

Описание раздела находится в стадии разработки.

Настройка конфигурации

Типы настроек

Одним из методов настройки маршрутизатора RAPIRA RS3 является интерфейс командной строки (CLI). Файл настроек представляет собой набор команд, которые настраивают систему в желаемое состояние сразу после запуска.

В маршрутизаторе RAPIRA RS3 представлены три вида настроек.

1. **Default configuration (стандартная конфигурация)** устанавливается производителем и загружается при восстановлении заводских настроек системы.
2. **Running configuration (исполняемая конфигурация)** представляет собой набор команд, которые необходимо выполнить, чтобы привести систему в текущее рабочее состояние. Рабочая настройка хранится в оперативной памяти (RAM) и отражает любое изменение параметров настройки системы. При выключении питания системы содержимое RAM пропадает. Чтобы сохранить текущее состояние системы, необходимо скопировать текущую конфигурацию в файл конфигурации запуска (см. ниже.)
3. **Startup configuration (пусковая конфигурация)** используется системой для самонастройки во время загрузки. Файл конфигурации запуска хранится в энергонезависимой флэш-памяти (ROM) и не уничтожается при выключении питания.

Просмотр конфигурации

Чтобы просмотреть текущую рабочую конфигурацию системы, используется команда `show running-config`. Для просмотра конфигурации запуска используется команда `show startup-config`.

Пример 1. Просмотр конфигурации

```
RAPIRA: show running-config
    show running-config
    interface Bridge 0
    interface Bridge 0
          ip
       address 192.168.0.250 255.255.255.0
          no shutdown
    !
    interface Wireless 0
     ssid 1
     type ap
     wds-mode
     bridge-group 0
     distance 3000
     channel 5760
     mode ht40+
     speed auto auto
     no beeper
     clientbridge
     tx-power 25
     no shutdown

    !
    interface FastEthernet 0
        bridge-group 0
        no shutdown
    !
```

Можно задавать эту команду с определенным параметром для просмотра только необходимой части файла конфигурации.

Пример 2. Просмотр части файла конфигурации

```
RAPIRA:  show running-config ip
interface Bridge 0
ip
address 192.168.0.250 255.255.255.0
```

Копирование файлов конфигураций

Для сохранения текущей исполняемой конфигурации, восстановления заводских настроек, загрузки резервных копий конфигураций и т.д. используется командная ветвь **copy**. Она имеет несколько подкоманд:

- `copy default-config startup-config` после следующего запуска оборудование восстанавливает работу в режиме заводских настроек.
- `copy running-config startup-config` сохраняет текущую исполняемую конфигурацию в

качестве пусковой конфигурации.

- `copy running-config tftp` копирует исполняемую конфигурацию на TFTP-сервер
- `copy startup-config tftp` копирует пусковую конфигурацию на TFTP-сервер
- `copy tftp startup-config` загружает пусковую конфигурацию с TFTP-сервера

Пример 3. Создание резервной копии и восстановление конфигурации

```
RAPIRA: copy running-config tftp 192.168.0.10 RAPIRA.bk
Running-config successfully copied to tftp://192.168.0.10 'RAPIRA.bk'.
RAPIRA: copy tftp startup-config 192.168.0.10 RAPIRA.bk
Startup-config successfully copied from tftp://192.168.0.10 'RAPIRA.bk'.
```

Внимание

При копировании исполняемой или пусковой конфигурации на TFTP-сервер следует убедиться, что вы используете такой сервер, который позволяет загружать файлы на удаленный компьютер. Некоторые реализации TFTP-сервера отказываются создавать новые файлы и могут только обновлять существующие.

Для редактирования вручную необходимо скопировать либо startup-config, либо running-config на TFTP-сервер, отредактировать ее в текстовом редакторе, а затем загрузить обновленный файл обратно.

Внимание

Не меняйте порядок команд в файлах конфигурации до тех пор, пока не будете точно уверены в том, что делаете.

Формат файла конфигурации

Файл конфигурации RAPIRA RS3 представляет собой иерархическую общую систему команд, которую можно конвертировать в команды маршрутизатора RAPIRA RS3. Прежде чем создать конфигурацию, каждая команда RAPIRA RS3 делится на набор строк в соответствии с различными уровнями дерева каталога. Например, команда маршрутизатора RAPIRA RS3

```
interface Wireless 0 ip address 192.168.0.3
```

автоматически конвертируется в

```
interface Wireless 0
 ip
  address 192.168.0.3
```

Аналогичным образом команды

```
interface Wireless 0 ip address 192.168.0.3
interface Wireless 0 ip mtu 1400
interface Wireless 0 channel 2442
```

конвертируются в

```
interface Wireless 0
 ip
  address 192.168.0.3
  mtu 1400
 channel 2442
```

Индикатором глубины командного уровня является количество символов пробела или символа табуляции в начале строки. Перед разделом команд одного и того же уровня должно находиться одинаковое количество пробелов или символов табуляции.

Тем не менее, можно установить упомянутые команды напрямую - они будут корректно интерпретированы:

```
interface Wireless 0 ip address 192.168.0.3
interface Wireless 0 ip mtu 1400
interface Wireless 0 channel 2442
```

Текст после символа"**!**" игнорируется. Наример:

```
!
! Use our own local NTP servers.
!
ntp
 server ntp-server-1.lan    ! This server is primary.
 server ntp-server-2.lan    ! This is a backup server.
```

Во все файлы конфигурации, прежде чем они окажутся скопированными в TFTP-сервер, добавляется заголовок, содержащий время последнего изменения файла:

```
!
! Last configuration change at Thu Jan  4 10:16:10 2007
!
```

Данные в заголовке автоматически обновляются при каждом копировании данных между RAPIRA RS3 и TFTP-сервером.

Список команд

```
copy default-config startup-config
```

Описание. Восстановление конфигурации в соответствии с заводскими настройками. После копирования настроек необходимо перезагрузить маршрутизатор.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

```
copy running-config startup-config
```

Описание. Сохранение исполняемой конфигурации во флэш-памяти.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

```
copy running-config tftp {server} {file}
```

Описание. Сохраняет исполняемую конфигурацию на TFTP-сервере.

Префикс NO. Не используется.

Аргументы.

server

Доменное имя или IP-адрес TFTP-сервера.

file

Файл на TFTP-сервере, содержащий сохраненную конфигурацию.

```
copy startup-config tftp {server} {file}
```

Описание. Сохраняет пусковую конфигурацию на TFTP-сервере. При выполнении данной команды обратите внимание, чтобы в установках TFTP-сервера не была отмечена опция READ ONLY.

Префикс NO. Не используется.

Аргументы.

server

Доменное имя или IP-адрес TFTP-сервера.

file

Файл на TFTP-сервере, содержащий сохраненную конфигурацию.

```
copy tftp startup-config {server} {file}
```

Описание. Восстанавливает пусковую конфигурацию, копируя файл пусковой конфигурации с TFTP-сервера.

Префикс NO. Не используется.

Аргументы.

server

Доменное имя или IP-адрес TFTP-сервера.

file

Файл на TFTP-сервере, содержащий сохраненную конфигурацию.

```
show running-config [искомый параметр]
```

Описание. Просмотр исполняемой конфигурации.

Префикс NO. Не используется.

Аргументы.

искомый параметр

Параметр, значение которого вы хотите просмотреть. Если введенная строка содержится в нескольких параметрах, то будут показаны ВСЕ значения соответствующих параметров.

```
show startup-config [искомый параметр]
```

Описание. Просмотр пусковой конфигурации.

Префикс NO. Не используется.

Аргументы.

искомый параметр

Параметр, значение которого вы хотите просмотреть. Если введенная строка содержится в нескольких параметрах, то будут показаны ВСЕ значения соответствующих параметров.

Запуск TFTP-сервера

Чтобы создать резервную копию, восстановить конфигурацию, установить новые версии программного обеспечения или импортировать цифровые сертификаты, необходимо запустить TFTP-сервер на каком-либо хосте сети. Можно использовать TFTP-сервер из пакета прогаммного обеспечения, находящегося на прилагаемом компакт-диске.

Сетевые интерфейсы

```
show interfaces [name index]
```

Описание. Отображение статуса интерфейсов сети. В случае отсутствия аргументов, на экран выводится весь список интерфейсов.

Префикс NO. Не используется.

Аргументы.

name

Указывает имя выводимого на экран интерфейса.

index

Указывает индекс интерфейса.

Пример 4. Просмотр статуса интерфейсов сети

```
RAPIRA: show interfaces
Bridge 0 is up
Hardware address:  0003.57ef.32a8
Internet address:  192.168.0.30 mask 255.255.255.0
broadcast:  192.168.0.255, MTU: 1500

Wireless 0 is up
Hardware address:  0015.6d54.32bb
Internet address:  0.0.0.0 mask 0.0.0.0
broadcast:  0.0.0.0, MTU: 1500
Type: ap, SSID:"test", Mode: 802.11g
Speed: 54 Mb/s, Access point: N/A
Channel: 2, Frequency: 2417 MHz, Tx-power: 10 dBm
RTS: off, Distance: 3000, WDS: on, FastFrame: on
Burst: on, Compression: off, WMM: on, Beacon: 100
Antenna: auto, IEEE 802.11g Protection: off

FastEthernet 0 is up
Hardware address:  0003.57ef.32a8
Internet address:  0.0.0.0 mask 0.0.0.0
broadcast:  0.0.0.0, MTU: 1500
```

Параметры беспроводного соединения

Основные радиопараметры

Настройка физического уровня

`interface {name} {index} mode {a | b | g | auto}`

Описание. Указывает режим IEEE 802.11, который может быть представлен в одном из вариантов: 802.1a, 802.11b или 802.11g.

Префикс NO. Не используется.

Аргументы.

mode

Режим: один из `a`, `b`, `g` или `auto` (рекомендуется). Если режим установлен в `auto`, то драйвер

маршрутизатора автоматически вычисляет оптимальный режим для данной частоты и скорости передачи данных.

Пример 5. Настройка режима работы устройства

```
RAPIRA: interface Wireless 0 mode a
The mode is set to 'a'.
```

`interface {name} {index} channel {frequency} | auto}`

Описание. Указывает частоту канала несущей частоты.

Префикс NO. Не используется.

Аргументы.

frequency

Указывает значение несущей частоты в мегагерцах. Ключевое слово `auto` применимо исключительно к клиентскому устройству. Если канал станции указан как `auto`, то сканируются все поддерживаемые каналы для данного SSID.

Важно:

Если вы определите конкретную частоту для оборудования, работающего в режиме «клиентская станция», то она будет опрашивать только эту частоту.

Обратите внимание:

Для режима «базовая станция» нельзя использовать значение **auto**.

Пример 6. Настройка частотного канала

```
RAPIRA: interface Wireless 0 channel 5805
Channel is set to '5805'.
```

`show interface {name} {index} channel-list`

Описание. Отображает список поддерживаемых каналов.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Обратите внимание:

Список поддерживаемых каналов может различаться в зависимости от установленного countrycode.

Пример 7. Просмотр списка поддерживаемых каналов

```
RAPIRA: show interface Wireless 0 channel-list

Channel:  -15 : 4.925 GHz (30 dBm) no_ht40-
Channel:  -14 : 4.930 GHz (30 dBm) no_ht40-
Channel:  -13 : 4.935 GHz (30 dBm) no_ht40-
Channel:  -12 : 4.940 GHz (30 dBm) no_ht40-
Channel:  -11 : 4.945 GHz (30 dBm)
Channel:  -10 : 4.950 GHz (30 dBm)
...
Channel:    1 : 5.005 GHz (30 dBm)
Channel:    2 : 5.010 GHz (30 dBm)
Channel:    3 : 5.015 GHz (30 dBm)
Channel:    4 : 5.020 GHz (30 dBm) no_ht40-
Channel:    5 : 5.025 GHz (30 dBm)
Channel:    6 : 5.030 GHz (30 dBm)
Channel:    7 : 5.035 GHz (30 dBm)
...
Channel:  196 : 5.980 GHz (30 dBm)
Channel:  197 : 5.985 GHz (30 dBm)
Channel:  198 : 5.990 GHz (30 dBm)
Channel:  199 : 5.995 GHz (30 dBm)
Channel:  200 : 6.000 GHz (30 dBm)
Channel:  201 : 6.005 GHz (30 dBm)
Channel:  202 : 6.010 GHz (30 dBm)
...
Channel:  214 : 6.070 GHz (30 dBm)
Channel:  215 : 6.075 GHz (30 dBm)
Channel:  216 : 6.080 GHz (30 dBm)
Channel:  217 : 6.085 GHz (30 dBm) no_ht40+
Channel:  218 : 6.090 GHz (30 dBm) no_ht40+
Channel:  219 : 6.095 GHz (30 dBm) no_ht40+
Channel:  220 : 6.100 GHz (30 dBm) no_ht40+
```

`interface {name} {index} speed {rate} | auto}`

Описание. Указывает скорость передачи данных по беспроводному каналу связи. Данная скорость является канальной скоростью передачи. Скорость передачи данных пользователя будет определяться энергетическими параметрами линии и характеристиками потока передаваемых данных.

Префикс NO. Не используется.

Аргументы.

rate

Скорость передачи данных выражается в мегабитах в секунду (Mbit/s). По стандартам IEEE 802.11a и IEEE 802.11g поддерживаются следующие скорости: 6, 9, 12, 18, 24, 36, 48 и 54 Mbit/s. По стандарту IEEE 802.11b поддерживаются следующие скорости: 1, 2, 5.5 и 11

Mbit/s. Если значение установлено в `auto`, то будет выбрана оптимальная скорость передачи данных.

Пример 8. Настройка скорости передачи данных

```
RAPIRA: interface Wireless 0 speed 54
Speed is set to 54 Mb/s.
```

Настройка опций MAC уровня

Настройка типа оборудования

В настоящее время RAPIRA RS3 работает либо в режиме базовой станции (AP), либо в режиме клиентской станции (CPE). Для установки определенного типа используется команда `interface {name} {index} type`. Для настройки подинтерфейсов используются другие команды, подробнее см. в разделе Настройка множественных SSID.

`interface {name} {index} type {ap | station}`

Описание. Установка типа оборудования: базовая (AP) или клиентская (CPE) станция.

Префикс NO. Не используется.

Аргументы.

type

Указание типа оборудования. Возможные значения: `ap` и `station`.

Пример 9. Настройка типа маршрутизавтора

```
RAPIRA: interface Wireless 0 type ap
Interface 'Wireless 0': type 'ap'.
RAPIRA: interface Wireless 0 type station
Interface 'Wireless 0': type 'station'.
```

Настройка SSID

SSID – это аббревиатура **S**ervice **S**et **Id**entifier. SSID является основным параметром интерфейсов беспроводной сети IEEE 802.11. Чтобы обеспечить беспроводную связь с удаленным оборудованием, необходимо указать идентичный SSID для беспроводного интерфейса базовой и клиентской станции.

Важно:

- При пустом поле SSID система работать не будет!
- Поле SSID не должно содержать пробелов!

`interface {name} {index} ssid {ssid}`

Описание. Для базовой станции: создание уникального идентификатора беспроводной

сети. Для клиентской станции: указание идентификатора беспроводной сети, к которой необходимо подключиться.

Префикс NO. Удаление SSID.

Аргументы.

ssid

Иденитфикатор беспроводной сети.

Пример 10. Настройка SSID

```
RAPIRA: interface Wireless 0 ssid ache
Interface 'Wireless 0': SSID 'ache'.
```

Настройка множественных SSID

Настоящая версия RAPIRA RS3 поддерживает режим «Нескольких базовых станций» на одном и том же беспроводном сетевом интерфейсе. Интерфейсы Wireless {индекс1}.{индекс2} с тем же самым {индекс1} используют один и тот же физический радиоинтерфейс, то есть они работают в пределах того же канала и используют одинаковые возможности физического уровня. В данном случае каждая базовая или клиентская станция реализуется как подинтерфейс. Подинтерфейсы обозначаются с помощью точки (“.”), после чего следует цифровой ID подинтерфейса. Таким образом, подинтерфейс «X.0» является псевдонимом для главного интерфейса, тогда как ID с ненулевой индикацией означают дополнительные подинтерфейсы. Каждый подинтерфейс может быть либо базовой, либо клиентской станцией.

Например, если маршрутизатор имеет два подинтерфейса **Wireless 0**, то беспроводной интерфейс в результате выполнения команды show interfaces будет выглядеть следующим образом:

```
Wireless 0 is up
Hardware address:  0015.6d54.32bb
Internet address:  0.0.0.0 mask 0.0.0.0
broadcast:  0.0.0.0, MTU: 1500
Type: ap, SSID: "test", Mode: 802.11g
Speed: 54 Mb/s, Access point: N/A
Channel: 2, Frequency: 2417 MHz, Tx-power: 16 dBm
RTS: off, Distance: 3000, WDS: on, FastFrame: on
Burst: on, Compression: off, WMM: on, Beacon: 100
Antenna: auto, IEEE 802.11g Protection: off

Wireless 0.1 is down
Hardware address:  0a15.6d54.32bb
Internet address:  0.0.0.0 mask 0.0.0.0
broadcast:  0.0.0.0, MTU: 1500
Type: ap, SSID: "test3", Mode: 802.11g (auto)
Speed: 0 Mb/s (auto), Access point: N/A
Channel: 0, Frequency: 0 MHz, Tx-power: 16 dBm
RTS: off, Distance: 3000, WDS: off, FastFrame: on
Burst: on, Compression: off, WMM: on, Beacon: 0
Antenna: auto, IEEE 802.11g Protection: off

Wireless 0.2 is down
Hardware address:  0615.6d54.32bb
Internet address:  0.0.0.0 mask 0.0.0.0
broadcast:  0.0.0.0, MTU: 1500
Type: ap, SSID: "test2", Mode: 802.11g (auto)
Speed: 0 Mb/s (auto), Access point: N/A
Channel: 0, Frequency: 0 MHz, Tx-power: 16 dBm
RTS: off, Distance: 3000, WDS: off, FastFrame: on
Burst: on, Compression: off, WMM: on, Beacon: 0
Antenna: auto, IEEE 802.11g Protection: off
```

Новый беспроводной подинтерфейс можно создать только с помощью команды interface ... ssid. Для нового подинтерфейса можно выбрать любой свободный ID. Если команда вызывается для уже существующего интерфейса, то она просто настраивает ssid. Интерфейс может быть настроен только после того, как он был создан:

```
RAPIRA: interface Wireless 0.2 type ap
No such interface 'Wireless 0.2'.
RAPIRA: interface Wireless 0.2 ssid gate12
Interface 'Wireless 0.2' created; SSID 'gate12' registered.
RAPIRA: interface Wireless 0.2 type ap
Interface 'Wireless 0.2': type 'ap'.
```

Каждый новый подинтерфейс после создания имеет тип "ap". Тип можно изменить, хотя в режиме множественных SSID возможны не все типы подинтерфейсов. На каждый интерфейс можно создать до 3 подинтерфейсов. Однако, в перечне подинтерфейсов может

быть только одна клиентская станция. В том случае, если основное устройство работает в режиме AP, то можно создать один подинтерфейс с типом "station", после этого можно создать другие подинтерфейсы с типом "ap".

см. также Настройка VLAN

Установка дополнительных параметров

Установка выходной мощности сигнала

Более высокая мощность передачи транслируется в более высокую мощность сигнала на приемнике. При более высоком отношении сигнал/шум (SNR) на приемнике снижается частота появления ошибок цифровой линии связи. Более высокое SNR позволяет также использовать систему, которая использует адаптацию связи, чтобы обеспечить более высокую скорость передачи. В результате, система обладает более высокой спектральной эффективностью.

Чем больше мощность TX, тем выше скорость поддерживаемых данных – тем более надежным является соединение при конкретной скорости передачи данных. Однако, неадекватно высокая мощность передачи может вызвать чрезмерные помехи (интерференцию). Максимальная величина мощности передачи ограничена нормами законодательства той страны, где используется оборудование.

```
interface {name} {index} tx-power {power}
```

Описание. Установка мощности передачи.

Префикс NO. Восстанавливает значение мощности по умолчанию.

Аргументы.

power

Значение мощности выражается в dBm, в целых числах. Приемлемый диапазон от 1 до 30.

Обратите внимание:

Учитывая неравномерность АЧХ передающего каскада на разных частотах, необходимо проверять максимально возможное значение мощности отдельно для каждой частоты.

Пример 11. Настройка мощности передачи

```
RAPIRA: interface Wireless 0 tx-power 26
The tx-power value is set to 26 dBm.
```

Настройка параметра расстояния

Параметр расстояния линии связи позволяет пользователю настроить множественный доступ с контролем несущей и уклонением от столкновений для определенного диапазона.

CSMA/CA для получения максимальной производительности.

Параметр расстояния линии связи выражается в метрах, значение должно быть кратно 300.

Обратите внимание:

Указание более короткой дистанции, нежели она есть, может привести к сбою в работе оборудования и снижению скорости передачи данных.

`interface {name} {index} distance {distance}`

Описание. Настройка дистанции между маршрутизаторами.

Префикс NO. Восстанавливает значение дистанции по умолчанию.

Аргументы.

distance

Дистанция измеряется в метрах, значение должно быть кратно 300. Приемлемый диапазон от 300 до 100200 метров.

Пример 12. Настройка дистанции между маршрутизаторами

```
RAPIRA: interface Wireless 0 distance 3000
A distance value is set to '3000'.
```

Настройка поллинга

Стандарт 802.11 не оговаривает конкретного алгоритма, согласно которому каждый раз в цикле PCF будет составляться список опроса. Каждый производитель волен разрабатывать этот алгоритм самостоятельно. В простейшем случае список опроса статический, опрашиваются все зарегистрированные станции, каждой из них при этом выделяется одинаковый промежуток времени для передачи.

Специально для РЭС RAPIRA RS3 был разработан алгоритм адаптивного динамического поллинга, который демонстрирует интеллектуальный подход к составлению списка опроса. Адаптивные свойства данного алгоритма заключаются в том, что для расчета отводимых каждой станции временных отрезков он осуществляет анализ целого комплекса параметров, таких как число активных станций, интенсивность передачи трафика каждой станцией в настоящее время и в прошлом, количество ошибок, разновидность трафика и т.д. При этом список опроса формируется в каждом цикле PCF динамически, то есть «на лету».

Данный алгоритм позволяет РЭС RAPIRA RS3 обеспечивать заданное качество обслуживания (QoS) для каждого абонента и класса трафика, а также высокую эффективность утилизации канала и достаточно справедливое разделение его ресурсов между всеми станциями.

Чтобы переключить работу системы в режим поллинга, необходимо задать команду polling.

Чтобы активировать алгоритм поллинга, также необходимо задать количество абонентов,

которые будут обслуживаться базовой станцией. Для этого используется команда polling-stations-max.

В автоматическом режиме для каждого клиентского терминала ведётся подробная статистика целого комплекса параметров, таких как число активных станций, интенсивность передачи трафика каждой станцией, количество ошибок, разновидность трафика и т.д. Накопленная информация анализируется, и по определившимся результатам базовая станция организует определённый порядок опроса клиентских устройств.

В режиме поллинга возможно ограничение максимальной скорости передачи для указанных клиентских станций. Для этого используется команда polling-max-rate. В этом случае скорость потока данных от станции к базе будет ограничена заданным значением в обратном канале; скорость потока данных от базовой станции к клиентской станции будет ограничена значением в прямом канале.

Минимальная гарантированная скорость устанавливается командой polling-min-rate и позволяет увеличить значение средней скорости передачи в прямом или обратном каналах до заданной при наличии ресурса, которым в данной системе связи является время. Если же ресурса недостаточно, то он будет отобран у других станций, имеющих более низкий приоритет, и поделен пропорционально запрошенной минимальной скорости между станциями с равным приориетом.

Приоритет станции задается числом от 1 до 100 при помощи команды polling-priority. Приоритет работает совместно с параметром минимальной гарантированной скорости и определяет, какие станции могут использовать чужой ресурс для выполнения своих требований по минимальной скорости, а какие будут вынуждены отдавать свой.

Все параметры могут быть заданы не только для конкретной абонентской станции, но и для всех станций сразу в виде параметра по умолчанию. Для этого необходимо в качестве MAC-адреса указать широковещательный адрес, равный FF:FF:FF:FF:FF:FF. Если у любых нескольких станций все параметры равны, то скорость передачи у данных станций будет равна как в прямом, так и в обратном каналах.

При включенном поллинге базовая станция работает в т.н. совмещенном режиме и взаимодействует как с клиентскими устройствами, поддерживающими поллинг, так и со стандартными WiFi-устройствами. В данном режиме время разбиватеся на 100 мс интервалы. Администратор базовой станции при помощи команды polling-percentage может выбрать процент от этого интервала, в течение которого базовая станция будет работать в режиме поллинга. Остальное время базовая станция работает в обычном режиме, взаимодействуя со стандартными WiFi-устройствами.

Настройка безопасности беспроводной связи

Общие положения по безопасности беспроводного соединения

Беспроводные сети незащищены и уязвимы для тех атак, которые сложно запустить в проводную сеть. Преимущество многих кабельных сетей состоит именно в общих свойствах физической безопасности. Маловероятно, чтобы хакер стал бы откапывать кабель и внедряться в сеть. Защитить же беспроводные каналы довольно сложно, так как они

используют общий эфир для трансляции сигнала. В эфир злоумышленник может легко проникнуть: подслушать, перехватить, ввести собственные данные или изменить передаваемые. Помимо всего остального, злоумышленники могут взаимодействовать с сетью на расстоянии, используя дорогостоящие радиотрансиверы и мощные рабочие станции.

В беспроводной индустрии разработан широкий спектр различных защитных технологий, которые способны обеспечить уровень конфиденциальности, сопоставимый с защитой традиционной кабельной сети.

WEP

WEP был первым опытом разработчиков для IEEE 802.11 и был призван решить следующие задачи: защитить беспроводное соединение от подслушивания предотвратить несанкционированный доступ к беспроводной сети и предупредить фальсификацию передаваемых сообщений. WEP использует групповой шифр RC4, который комбинирует 40-битовый WEP ключ с 24-битовым случайным числом. Он определяется термином Initialization Vector (IV) и служит для шифрования данных. Отправитель выполняет логическую операцию XOR , обрабатывая групповой шрифт вместе с реальными данными, и получает, тем самым, зашифрованный текст. На приемник направляется пакет, состоящий из комбинации IV с зашифрованным текстом. Приемник дешифрует пакет с помощью WEP ключа, хранящегося в памяти, и прилагаемого IV.

К сожалению, прежде чем выпустить протокол шифрования, следовало бы провести более широкий и углубленный экспертный анализ. Для протокола были характерны серьезные дефекты в плане безопасности. Применение WEP может остановить случайных дилетантов, однако, опытный хакер за 15 минут способен взломать WEP ключи в работающей сети. В целом, протокол WEP был признан неудачным.

Чтобы обеспечить совместимость, RAPIRA RS3 все еще поддерживает протокол WEP.

Режим WPA EAP (IEEE 802.1X)

Одной из слабых сторон WEP является простота аутентификации. Более совершенная аутентификация – первый шаг к устранению дефекта WEP в плане доступа к сети. Наиболее защищенным методом аутентификации был признан стандарт 802.1x.

Первоначально стандарт 802.1x был разработан для кабельных сетей, однако, его можно применять и для беспроводных соединений. Стандарт основан на управлении доступом через порты, он обеспечивает взаимную аутентификацию между клиентами и точками доступа через сервер аутентификации.

Стандарт 802.1x standard включает в себя три элемента:

- **Supplicant (Запрашивающий)** – опознаваемый пользователь или клиент. Это может быть клиентское ПО на портативном компьютере , PDA или любом другом беспроводном оборудовании.
- **Authentication server (Сервер аутентификации)** – система аутентификации типа сервера RADIUS, выполняющая аутентификации путем проверки логинов и паролей,

цифровых сертификатов или каких-либо иных средств аутентификации.

- **Authenticator (Аутентификатор)** – устройство, действующее как посредник между запрашивающим и сервером аутентификации. Как правило, таким устройством является базовая станция.

Взаимная аутентификация в (режиме/стандарте) 802.1x предусматривает три стадии:

- Запрашивающий инициирует соединение с аутентификатором. Аутентификатор обнаруживает инициацию и разрешает допуск порта запрашивающего. Следует отметить, что за исключением вариантов режима 802.1x весь остальной трафик блокирован, включая DHCP, HTTP, FTP, SMTP и POP3.
- Затем аутентификатор запрашивает идентичность у запрашивающего.
- После этого запрашивающий отвечает и сообщает идентичность. Аутентификатор передает идентичность на сервер аутентификации.
- Сервер аутентификации опознает идентичность запрашивающего. После того, как опознание завершено, аутентификатору посылается сообщение 'ACCEPT'. После этого аутентификатор переводит порт запрашивающего в состояние авторизованного.
- Далее запрашивающий запрашивает аутентичность у сервера аутентификации. Сервер аутентификации передает свою аутентификацию запрашивающему.
- После того, как запрашивающий опознал идентичность сервера аутентификации, все трафики передаются своим чередом.

EAP

Конкретный метод обеспечения идентичности называется «Расширенным протоколом аутентификации» (Extensible Authentication Protocol – сокр. EAP). EAP – это тот самый протокол, который стандарт 802.1x использует для управления взаимными аутентификациями. Обладая стандартизированным протоколом EAP, клиенту совершенно не требуется вникать в тонкости методов аутентификации. Аутентификатор просто работает посредником, формируя и «распаковывая» EAP-пакеты, чтобы направить их от запрашивающего на сервер аутентификации, где, собственно, и будет происходить сам процесс аутентификации.

На сегодяшний день используется несколько методов EAP:

1. **LEAP**. Стандарт разработан компанией Cisco. Для направления аутентификационных данных на RADIUS сервер для аутентификации LEAP использует комбинацию имя пользователя/пароль.
2. **EAP-TLS**. Это – стандарт, описанный в RFC 2716. Для выполнения аутентификации EAP-TLS использует сертификаты X.509. Как запрашивающий, так и сервер аутентификации обмениваются своими X.509 сертификатами.
3. **EAP-TTLS**. Стандарт разработан компанией Funk Software. EAP-TTLS представляет собой альтернативу EAP-TLS. Пока аутентификатор идентифицирует себя клиенту с помощью сертификата сервера, запрашивающий использует идентификацию типа «имя пользователя/пароль».

4. **EAP-PEAP** (Защищенный EAP). Еще один стандарт, разработанный для гарантии безопасной взаимной аутентификации. Новая разработка была создана, чтобы преодолеть некоторые слабые места других методов EAP.

WPA

Wi-Fi Protected Access (WPA) – промежуточный стандарт защищенного доступа к беспроводным сетям представляет собой спецификацию безопасности, имеющую возможность взаимодействовать с другими устройствами. Спецификация разработана таким образом, что для соответствия требованиям необходимы лишь новые версии программного обеспечения для существующего или традиционного оборудования. WPA направлен на повышение уровня безопасности как существующих, так и будущих беспроводных локальных сетей (LAN).

В основе WPA лежит подмножество стандарта IEEE 802.11i, включая следующие характеристики, которые должны устранить уязвимые места в защите WEP:

- Инструментарий аутентификации, основанной на 802.1x EAP, для усиления взаимной аутентификации.
- Протокол Applies Temporal Key Integrity Protocol (TKIP) – «Протокол ограниченной во времени целостности ключа» на существующем RC4 WEP для обеспечения надежного шифрования данных.
- Использует Michael Message Integrity Check для целостности сообщений. MIC («проверка целостности данных») основан на 128-битовом ограниченном во времени ключе (temporal key), общем как для клиентов, так и для базовых станций, при этом MAC-адрес клиентского оборудования и 48-битовый вектор инициализации описывает номер пакета.

Temporal Key Integrity Protocol (TKIP) «Протокол ограниченной во времени целостности ключа» корректирует выявленные слабости WEP в области шифрования данных. Основная специфика протокола TKIP – коррекция дефектов безопасности при многократном использовании ключа в WEP.

Для совместимости с существующим оборудованием TKIP использует те же алгоритмы шифрования (RC4), что и WEP. Таким образом, для применения TKIP нужна лишь новая версия ПО. По сравнению с WEP, TKIP изменяет ключи через каждые 10 000 пакетов. Такое динамическое изменение ключей оставляет для потенциальных «хакеров» слишком мало место, чтобы взломать ключ TKIP. В целом, большинство экспертов сходятся во мнениях, что протокол шифрования TKIP гораздо сильнее WEP. Однако, они столь же единодушны и в том, что TKIP предлагает лишь промежуточное решение, так как использует алгоритм RC4.

Наконец, Message Integrity Check (MIC) – это 64-битовое сообщение, которое рассчитано с помощью алгоритма"Michael". MIC гораздо более надежен, чем контрольная сумма CRC32 режима IEEE 802.11.

WPA PSK

WPA можно также использовать в менее надежном режиме pre-shared key (PSK) - режиме с ПРЕДУСТАНОВЛЕННЫМ КЛЮЧОМ, где всем запрашивающим выдается одна и та же

идентификационная фраза. WPA-PSK подходит для небольших сайтов, когда нецелесообразно использовать сервер аутентификации.

IEEE 802.11i WPA2

Спецификация 802.11i представляет собой результат работы специалистов, когда комитет IEEE 802.11 поставил задачу целенаправленно решить проблемы безопасности, порожденные WEP. Решение 802.11i обладает всеми вышеуказанными преимуществами WPA, указанными выше. Помимо этого, 802.11i предлагает следующие возможности:

- более надежное шифрование благодаря применению AES
- поддержка роуминга.

IEEE 802.11i использует режим CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Основным алгоритмом CCMP является Advanced Encryption Standard (AES) – «Усовершенствованный алгоритм шифрования». В отличие от TKIP, управление ключом и целостность сообщения в CCMP осуществляется с помощью одного компонента с использованием AES.

RAPIRA RS3 поддерживает шифрование как WPA, так и WPA2.

Настройка WEP

Маршрутизатор RAPIRA RS3 поддерживает 40-битное и 104-битное WEP-шифрование. Можно сконфигурировать до четырех WEP ключей на один интерфейс. Каждый ключ идентифицируется по индексу от 1 до 4. Ключи статические. Нельзя использовать несколько ключей одновременно (только один), ключи можно выбирать вручную, используя команду interface ... encryption key

Пример 13. Настройка WEP на базовой станции

```
RAPIRA: interface Wireless 0 type ap
Interface 'Wireless 0': type 'ap'.
RAPIRA: interface Wireless 0 ssid FooBar
Interface 'Wireless 0': SSID 'FooBar'.
RAPIRA: interface Wireless 0 encryption wep
Interface 'Wireless 0': WEP enabled.
RAPIRA: interface Wireless 0 encryption key 1 AB33948AB430298CD229830DEE
WEP key [1] = 0xAB33948AB430298CD229830DEE (104-bit).
RAPIRA: interface Wireless 0 no shutdown
Interface 'Wireless 0' is up.
```

В режиме станции можно использовать аутентификацию EAP одновременно с WEP. Для этого необходимо разрешить режим WPA EAP и следовать инструкциям из раздела WPA.

Пример 14. Настройка статической WEP EAP-MD5 на базовой станции

```
RAPIRA: interface Wireless 0 type ap
Interface 'Wireless 0': type 'ap'.
RAPIRA: interface Wireless 0 ssid FooBar
Interface 'Wireless 0': SSID 'FooBar'.
RAPIRA: interface Wireless 0 encryption wep
Interface 'Wireless 0': WEP enabled.
RAPIRA: interface Wireless 0 encryption key 1 AB33948AB430298CD229830DDD
WEP key [1] = 0xAB33948AB430298CD229830DDD (104-bit).
RAPIRA: interface Wireless 0 authentication wpa-eap
WPA EAP enabled.
RAPIRA: interface Wireless 0 authentication md5
EAP MD5 enabled.
RAPIRA: interface Wireless 0 authentication identity roger
Using identity 'roger'.
RAPIRA: interface Wireless 0 authentication password wpLsoeqkdf
Password saved.
RAPIRA: interface Wireless 0 no shutdown
Interface 'Wireless 0' is up.
```

Динамическая WEP

При работе станции в данном режиме, если допускается шифрование WEP, но не сконфигурирован ни один WEP-ключ, то предполагается, что ключи являются динамическими. Динамические ключи получают, используя процедуру аутентификации WPA EAP. Обмен динамическими ключами поддерживают только PEAP, EAP-TTLS и EAP-TLS. Подробное описание конфигурации WPA EAP содержится в разделе WPA.

Пример 15. Настройка динамической WEP TTLS на клиентской станции

```
RAPIRA: interface Wireless 0 type station
Interface 'Wireless 0': type 'station'.
RAPIRA: interface Wireless 0 ssid Barney
Interface 'Wireless 0': SSID 'Barney'.
RAPIRA: interface Wireless 0 encryption wep
Interface 'Wireless 0': WEP enabled.
RAPIRA: interface Wireless 0 authentication wpa-eap
WPA EAP enabled.
RAPIRA: interface Wireless 0 authentication ttls
EAP TTLS enabled.
RAPIRA: interface Wireless 0 authentication ca-cert thawte.crt
Using thawte.crt as CA certificate.
RAPIRA: interface Wireless 0 authentication identity jim
Using identity 'jim'.
RAPIRA: interface Wireless 0 authentication password wPldvork98
Password saved.
RAPIRA: interface Wireless 0 no shutdown
Interface 'Wireless 0' is up.
```

Список команд

`interface {name} {index} encryption wep`

Описание. Включить WEP-шифрование.

Префикс NO. Отключить WEP-шифрование.

Аргументы. Аргументы отсутствуют.

Пример 16. Включение WEP-шифрования

```
RAPIRA: interface Wireless 0 encryption wep
Interface 'Wireless 0': WEP enabled.
RAPIRA: interface Wireless 0 encryption no wep
Interface 'Wireless 0': WEP disabled.
```

`interface {name} {index} encryption key [key-index] [key]`

Описание. Установка или выбор существующего ключа WEP.

Префикс NO. Удаление ключа WEP, используя его порядковый номер.

Аргументы.

key-index

Указание порядкового номера ключа WEP. Возможные значения: от 1 до 4.

key

Установка ключа: 10 или 26 шестнадцатиричных чисел для 40 и 104 битных WEP ключей соответственно. Данный аргумент может быть опущен, если ключ был указан ранее.

Пример 17. Установка или выбор существующего ключа WEP

```
RAPIRA: interface Wireless 0 encryption key ?
{index: 1-4} {789ABC...}
RAPIRA: interface Wireless 0 encryption key 1 113AAB3325
WEP key [1] = 0x113AAB3325 (40-bit).
RAPIRA: interface Wireless 0 encryption key 2 AB33948AB430298CD229830DEE
WEP key [2] = 0xAB33948AB430298CD229830DEE (104-bit).
RAPIRA: interface Wireless 0 encryption key 2
Selected key [2]: 0xAB33948AB430298CD229830DEE.
RAPIRA: interface Wireless 0 encryption no key 1
Cleared WEP key [1].
```

Настройка WPA

RAPIRA RS3 поддерживает следующие типы шифрования: TKIP (WPA) и CCMP (WPA2), а также следующие режимы аутентификации: EAP-MD5, EAP-MSCHAPv2, PEAP, EAP-TLS, EAP-TTLS и PSK. Можно включать TKIP и CCMP одновременно, чтобы обеспечить комбинацию режимов WPA и WPA2.

Также можно использовать вместе различные протоколы аутентификации, однако, этой возможностью лучше пользоваться только в тестовом режиме работы. Не рекомендуется использование данной возможности в обычном режиме работы маршрутизатора.

EAP-MD5 и EAP-MSCHAPv2 не поддерживают обмен динамическими ключами, поэтому их можно использовать только в сочетании с PEAP, EAP-TLS и EAP-TTLS в качестве второй фазы алгоритмов аутентификации.

При использовании режимов PEAP или EAP-TTLS без указания EAP-MD5 или EAP-MSCHAPv2 конкретный механизм аутентификации будет выбран сервером аутентификации, поскольку PEAP и EAP-TTLS являются туннелями и аутентификацию не производят.

Беспроводной интерфейс может работать в режиме как клиентской станции, так и базовой станции, используя, соответственно, режим либо запрашивающего (supplicant), либо аутентификатора (authenticator).

При работе в режиме **базовой станции**, системе необходим только предустановленный ключ для режима WPA-PSK и профиль RADIUS для режима WPA EAP EAP. Для режима базовой станции не нужно указывать точный тип EAP аутентификации, так как сеанс аутентификации ретранслируется на RADIUS сервер.

Пример 18. Настройка базовой станции с использованием WPA+WPA2 PSK

```
RAPIRA: interface Wireless 0 type ap
Interface 'Wireless 0': type 'ap'.
RAPIRA: interface Wireless 0 ssid Acid
Interface 'Wireless 0': SSID 'Acid'.
RAPIRA: interface Wireless 0 encryption tkip
Interface 'Wireless 0': TKIP enabled.
RAPIRA: interface Wireless 0 encryption ccmp
Interface 'Wireless 0': CCMP enabled.
RAPIRA: interface Wireless 0 authentication wpa-psk qqKdoeeiUS2
WPA PSK enabled.
```

Пример 19. Настройка базовой станции с использованием WPA+WPA2 EAP

```
RAPIRA: interface Wireless 0 type ap
Interface 'Wireless 0': type 'ap'.
RAPIRA: interface Wireless 0 ssid Acid
Interface 'Wireless 0': SSID 'Acid'.
RAPIRA: interface Wireless 0 encryption tkip
Interface 'Wireless 0': TKIP enabled.
RAPIRA: interface Wireless 0 encryption ccmp
Interface 'Wireless 0': CCMP enabled.
RAPIRA: interface Wireless 0 authentication wpa-eap
WPA EAP enabled.
RAPIRA: radius-profile rad1 server 192.168.2.100
Added RADIUS server 192.168.2.100 to profile 'rad1'.
RAPIRA: interface Wireless 0 authentication radius-profile rad1
RADIUS profile 'rad1' mapped.
```

При работе в режиме **клиентской станции** режимы аутентификации требуют различных параметров установки, которые перечислены в таблице. Перед установкой требуемого параметра можно разрешить любой режим аутентификации. При этом следует отметить, что режим аутентификации начнет функционировать только после того, как будут получены все требуемые параметры.

Таблица 7. Таблица настройки WPA

Режим аутентификации	Список команд
PSK	interface authentication wpa-psk
EAP-MD5[1]	interface authentication wpa-eap
	interface authentication md5
	interface authentication identity
	interface authentication password
EAP-MSCHAPv2[1]	interface authentication wpa-eap
	interface authentication mschap-v2
	interface authentication identity
	interface authentication password
EAP-TTLS	interface authentication wpa-eap
	interface authentication ttls
	interface authentication identity
	interface authentication password
	interface authentication ca-cert
PEAP	interface authentication wpa-eap
	interface authentication peap
	interface authentication identity
	interface authentication password
	interface authentication ca-cert
EAP-TLS[2]	interface authentication wpa-eap
	interface authentication tls
	interface authentication ca-cert
	interface authentication client-cert
	interface authentication identity

1. EAP-MD5 и EAP-MSCHAPv2 могут использоваться с выключенным или статическим WEP-шифрованием или в сочетании с другими методами аутентификации типа EAP-TTLS, EAP-TLS и PEAP.

2. В режиме EAP-TLS аутентификация запрашивающего берется из атрибута CN сертификата клиента за исключением тех случаев, когда она явно подменяется командой **interface authentication identity**.

Внимание:

Для проверки достоверности CA-сертификатов и сертификатов клиентов крайне важно правильно установленное системное время. Установите системное время, используя NTP-клиента.

Пример 20. Настройка клиентской станции с использованием WPA2 PSK

```
RAPIRA: interface Wireless 0 type station
Interface 'Wireless 0': type 'station'.
RAPIRA: interface Wireless 0 ssid Acid
Interface 'Wireless 0': SSID 'Acid'.
RAPIRA: interface Wireless 0 encryption ccmp
Interface 'Wireless 0': CCMP enabled.
RAPIRA: interface Wireless 0 authentication wpa-psk qqKdoeeiUS2
WPA PSK enabled.
```

Пример 21. Настройка клиентской станции с использованием WPA PEAP

```
RAPIRA: interface Wireless 0 type station
Interface 'Wireless 0': type 'station'.
RAPIRA: interface Wireless 0 ssid Barney
Interface 'Wireless 0': SSID 'Barney'.
RAPIRA: interface Wireless 0 encryption tkip
Interface 'Wireless 0': TKIP enabled.
RAPIRA: interface Wireless 0 authentication wpa-eap
WPA EAP enabled.
RAPIRA: interface Wireless 0 authentication peap
PEAP enabled.
RAPIRA: interface Wireless 0 authentication ca-cert thawte.crt
Using thawte.crt as CA certificate.
RAPIRA: interface Wireless 0 authentication identity ivanov
Using identity 'ivanov'.
RAPIRA: interface Wireless 0 authentication password pWosIoffis
Password saved.
```

Пример 22. Настройка клиентской станции с использованием WPA2 EAP-TLS

```
RAPIRA: interface Wireless 0 type station
Interface 'Wireless 0': type 'station'.
RAPIRA: interface Wireless 0 ssid Candle
Interface 'Wireless 0': SSID 'Candle'.
RAPIRA: interface Wireless 0 encryption ccmp
Interface 'Wireless 0': CCMP enabled.
RAPIRA: interface Wireless 0 authentication wpa-eap
WPA EAP enabled.
RAPIRA: interface Wireless 0 authentication tls
EAP TLS enabled.
RAPIRA: interface Wireless 0 authentication ca-cert thawte.crt
Using thawte.crt as CA certificate.
RAPIRA: interface Wireless 0 authentication client-cert ivanov.crt
Using ivanov.crt as a client certificate (CN = ivanov).
RAPIRA: interface Wireless 0 authentication private-key ivanov.key s9*kffjUe8
Using ivanov.key as a private key.
RAPIRA: interface Wireless 0 no shutdown
Interface 'Wireless 0' is up.
```

Пример 23. Настройка клиентской станции с использованием WPA2 EAP-TTLS+MD5

```
RAPIRA: interface Wireless 0 type station
Interface 'Wireless 0': type 'station'.
RAPIRA: interface Wireless 0 ssid Desert
Interface 'Wireless 0': SSID 'Desert'.
RAPIRA: interface Wireless 0 encryption ccmp
Interface 'Wireless 0': CCMP enabled.
RAPIRA: interface Wireless 0 authentication wpa-eap
WPA EAP enabled.
RAPIRA: interface Wireless 0 authentication tls
EAP TLS enabled.
RAPIRA: interface Wireless 0 authentication md5
EAP MD5 enabled.
RAPIRA: interface Wireless 0 authentication ca-cert thawte.crt
Using thawte.crt as CA certificate.
RAPIRA: interface Wireless 0 no shutdown
Interface 'Wireless 0' is up.
```

Обратите внимание:

1. Все вышеуказанные сертификаты должны быть загружены заранее.
2. В примере, представленном выше, используются различные файлы для сертификата клиента и секретного ключа, однако, для них можно использовать и один общий файл.
3. В качестве идентификации клиента используется общее имя (CN) из сертификата клиента. Эту установку можно заменить, используя команду identity.
4. Для всех режимов аутентификации на базе EAP требуется параметр WPA EAP.

Список команд

`interface {name} {index} encryption tkip`

Описание. Включает шифрование TKIP (WPA). Команда применима как для режима клиентской станции, так и для режима базовой станции.

Префикс NO. Выключение TKIP.

Аргументы. Аргументы отсутствуют.

Пример 24. Включение шифрования TKIP (WPA).

```
RAPIRA: interface Wireless 0 encryption tkip
Interface 'Wireless 0': TKIP enabled.
RAPIRA: interface Wireless 0 encryption no tkip
Interface 'Wireless 0': TKIP disabled.
```

`interface {name} {index} encryption ccmp`

Описание. Включает шифрование CCMP (WPA2). Команда применима как для режима клиентской станции, так и для режима базовой станции.

Префикс NO. Выключение CCMP.

Аргументы. Аргументы отсутствуют.

Пример 25. Включение шифрования CCMP (WPA2).

```
RAPIRA: interface Wireless 0 encryption ccmp
Interface 'Wireless 0': CCMP enabled.
RAPIRA: interface Wireless 0 encryption no ccmp
Interface 'Wireless 0': CCMP disabled.
```

`interface {name} {index} authentication wpa-psk {pre-shared-key}`

Описание. Устанавливает ключ для WPA и WPA2, включает режим WPA-PSK. Команда применима как для режима клиентской станции, так и для режима базовой станции.

Префикс NO. Сброс режима с предустановленным ключом и выключение WPA-PSK.

Аргументы.

pre-shared-key

В качестве данного аргумента должен быть введен ключ.

Пример 26. Устанавка ключа для WPA и WPA2

```
RAPIRA: interface Wireless 0 authentication wpa-psk deo3Icodfer34
WPA PSK enabled.
RAPIRA: interface Wireless 0 authentication no wpa-psk
WPA PSK disabled.
```

`interface {name} {index} authentication radius-profile {profile-name}`

Описание. Устанавливает профиль RADIUS для аутентификации WPA EAP. Профиль RADIUS не должен быть пустым. Данная команда применима только для режима базовой станции. Устанавливает ключ для WPA и WPA2 и включает режим WPA-PSK. Эта команда применима как для режима клиентской станции, так и для режима базовой станции.

Префикс NO. Отключает профиль RADIUS.

Аргументы.

profile-name

Указание имя профиля RADIUS.

Пример 27. Установка профиля RADIUS

```
RAPIRA: interface Wireless 0 authentication radius-profile rad1
RADIUS profile 'rad1' mapped.
RAPIRA: interface Wireless 0 authentication no radius-profile
RADIUS profile unmapped.
```

`interface {name} {index} authentication wpa-eap`

Описание. Включает режим WPA EAP. Команда применима как для режима клиентской станции, так и для режима базовой станции.

Префикс NO. Выключение WPA EAP.

Аргументы. Аргументы отсутствуют.

Пример 28. Включение режима WPA EAP

```
RAPIRA: interface Wireless 0 authentication wpa-eap
WPA EAP enabled.
RAPIRA: interface Wireless 0 authentication no wpa-eap
WPA EAP disabled.
```

`interface {name} {index} authentication peap`

Описание. Включает PEAP. Команда применима как для режима клиентской станции, так и для режима базовой станции.

Префикс NO. Выключение PEAP.

Аргументы. Аргументы отсутствуют.

Пример 29. Включение PEAP

```
RAPIRA: interface Wireless 0 authentication peap
PEAP enabled.
RAPIRA: interface Wireless 0 authentication no peap
PEAP disabled.
```

`interface {name} {index} authentication md5`

Описание. Включает EAP-MD5. Данная команда применима только для режима клиентской станции. EAP-MD5 нельзя использовать в качестве одиночной аутентификации с динамической WEP, так как она не поддерживает обмен динамическими ключами. Однако, ее можно использовать в качестве 2 фазы метода аутентификации наряду с PEAP, EAP-TLS и EAP-TTLS.

Префикс NO. Выключение EAP-MD5.

Аргументы. Аргументы отсутствуют.

Пример 30. Включение EAP-MD5

```
RAPIRA: interface Wireless 0 authentication md5
EAP MD5 enabled.
RAPIRA: interface Wireless 0 authentication no md5
EAP MD5 disabled.
```

`interface {name} {index} authentication mschap-v2`

Описание. Включает EAP-MSCHAPv2. Команда применима только для режима клиентской станции. EAP-MSCHAPv2 нельзя использовать в качестве одиночной аутентификации с динамической WEP, поскольку она не поддерживает обмен динамическим ключами. Однако, ее можно применять в качестве 2 фазы метода аутентификации наряду с PEAP, EAP-TLS и EAP-TTLS.

Префикс NO. Выключение EAP-MSCHAPv2

Аргументы. Аргументы отсутствуют.

Пример 31. Включение EAP-MSCHAPv2

```
RAPIRA: interface Wireless 0 authentication mschap-v2
EAP MSCHAPv2 enabled.
RAPIRA: interface Wireless 0 authentication no mschap-v2
EAP MSCHAPv2 disabled.
```

`interface {name} {index} authentication tls`

Описание. Включает EAP-TLS. Команда применима только для режима клиентской станции. Для EAP-TLS требуется сертификат CA, сертификат клиента и секретный ключ.

Префикс NO. Выключение EAP-TLS.

Аргументы. Аргументы отсутствуют.

Пример 32. Включение EAP-TLS

```
RAPIRA: interface Wireless 0 authentication tls
EAP TLS enabled.
RAPIRA: interface Wireless 0 authentication no tls
EAP TLS disabled.
```

`interface {name} {index} authentication ttls`

Описание. Включает EAP-TTLS. Команда применима только для режима клиентской станции. Для EAP-TTLS. Требуется CA-сертификат, идентификатор клиента и пароль.

Префикс NO. Выключение EAP-TTLS.

Аргументы. Аргументы отсутствуют.

Пример 33. Включение EAP-TTLS

```
RAPIRA: interface Wireless 0 authentication ttls
EAP TTLS enabled.
RAPIRA: interface Wireless 0 authentication no ttls
EAP TTLS disabled.
```

`interface {name} {index} authentication ca-cert RAPIRA`

Описание. Устанавливает надежный CA-сертификат для аутентификации EAP-TLS, EAP-TTLS и PEAP в режиме клиентской станции. CA (Certificate Authority – «Центр сертификатов») является той самой службой, которая подписала сертификаты сервера RADIUS. Запрашивающий EAP (EAP supplicant) будет доверять только тем RADIUS серверам, которые высылают сертификаты, подписанные доверенным CA.

Префикс NO. Отключает сертификат CA.

Аргументы.

filename

Имя файла сертификата X.509 CA в формате PEM. Перед использованием файл сертификата должен быть загружен.

Пример 34. Установка CA-сертификата

```
RAPIRA: interface Wireless 0 authentication ca-cert verisign.crt
Using verisign.crt as CA certificate.
RAPIRA: interface Wireless 0 authentication no ca-cert
CA certificate cleared.
```

`interface {name} {index} authentication client-cert RAPIRA`

Описание. Устанавливает сертификат клиента для аутентификации EAP-TLS в режиме клиентской станции.

Префикс NO. Отключает сертификат клиента.

Аргументы.

filename

Имя файла сертификата X.509 CA в формате PEM. Перед использованием файл сертификата должен быть загружен.

Пример 35. Установка сертификата клиента

```
RAPIRA: interface Wireless 0 authentication client-cert carol.crt
Using carol.crt as a client certificate (CN = caroline).
RAPIRA: interface Wireless 0 authentication no client-cert
Client certificate cleared.
```

`interface {name} {index} authentication private-key RAPIRA [password]`

Описание. Устанавливает секретный ключ клиента для аутентификации EAP-TLS в режиме клиентской станции.

Префикс NO. Отключает секретный ключ клиента.

Аргументы.

filename

Секретный ключ RSA или DSA в формате PEM. Перед использованием файл ключа должен быть загружен. Сертификат клиента и секретный ключ могут храниться в общем файле.

password

Пароль (необходим в том случае, если ключ зашифрован).

Пример 36. Установка секретного ключа клиента

```
RAPIRA: interface Wireless 0 authentication private-key rogers.key q1w2e3r4
Using rogers.key as a private key.
RAPIRA: interface Wireless 0 authentication no private-key
Private key cleared.
```

`interface {name} {index} authentication identity {login}`

Описание. Установка аутентичности клиента для режимов аутентификации EAP-TLS, EAP-TTLS, EAP-MD5, EAP-MSCHAPv2 и PEAP. Данная команда применима только для режима клиентской станции.

Префикс NO. Удаляет значение аутентичности.

Аргументы.

login

Указание логина для аутентификации.

Пример 37. Установка аутентичности клиента

```
RAPIRA: interface Wireless 0 authentication identity 22dfvlkjlk4
Using identity '22dfvlkjlk4'.
RAPIRA: interface Wireless 0 authentication no identity
Identity cleared.
```

`interface {name} {index} authentication password {password}`

Описание. Устанавливает пароль для режимов аутентификации EAP-TTLS, EAP-MD5, EAP-MSCHAPv2 и PEAP. Данная команда применима только для режима клиентской станции.

Префикс NO. Удаляет пароль

Аргументы.

password

Устанавливает пароль аутентификации

Пример 38. Установка пароля для различных режимов аутентификации

```
RAPIRA: interface Wireless 0 authentication password frfoiu223098f
Password saved.
RAPIRA: interface Wireless 0 authentication no password
Password cleared.
```

Управление сертификатами

В настоящее время сертификаты и секретные ключи используются для соединения беспроводной клиентской станции с базовой станцией посредством аутентификации EAP-

TLS. Кроме того, сертификаты необходимо использовать, чтобы проверить сертификационную подпись аутентификатора в режимах EAP-TLS, EAP-TTLS и PEAP.

Чтобы скопировать цифровой сертификат или файл секретного ключа на маршрутизатор RAPIRA RS3, следует запустить TFTP-сервер на компьютере, содержащем сертификат.

Команды управления сертификатами можно просмотреть с помощью следующей команды:

```
RAPIRA: certificate ?
delete              - Delete certificate.
export              - Export certificate.
import              - Copy certificate from TFTP server.
```

Команды управления сертификатами могут обрабатывать только файлы формата PEM. Каждый файл может содержать сертификат клиента, CA сертификат или секретный ключ. Секретный ключ и сертификат клиента можно объединять в одном файле, например:

```
-----BEGIN CERTIFICATE-----
MIICrTCCAhagAwIBAgIBFTANBgkqhkiG9w0BAQQFADCBgjELMAkGA1UEBhMCUlUx
DzANBgNVBAgTBlJ1c3NpYTEPMA0GA1UEBxMGTW9zY293MREwDwYDVQQKEwhJSVRQ
...
ly7Ts5+5+O3M+aoRsOX07yA=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,F5A0234F4ED60C0B

sV7rnnqd/u297NbniT08l7rIWv+Wzhnu4JYNI/YV7/4QOOMqn2OiqQajJOlK5qRS
XKy8Kb6+h87H1UzVsn/tDnTZf7dPodW29q6WS3a47ezromYsT46yeC7YbXUEdFr5
...
pT6uvP3vMCBgK6GLuiqjG9irEnZDe+PxTicc7yS2IPyRqTKUqt3lBQ==
-----END RSA PRIVATE KEY-----
```

Список команд

`certificate import {server} {file} [password]`

Описание. Загрузка PEM-файла с TFTP-сервера

Префикс NO. Не используется.

Аргументы.

server

Доменное имя TFTP-сервера или IP-адрес.

file

Имя PEM-файла на сервере. Файл будет сохранен локально под тем же самым именем.

password

Пароль. Его можно использовать в том случае, если передаваемый файл (или часть файла) зашифрована.

Пример 39. Загрузка PEM-файла

```
RAPIRA: certificate import 192.168.201.20 ivanov.pem
    Can't copy certificate 'ivanov.pem' to the repository: bad password read
RAPIRA: certificate import 192.168.201.20 ivanov.pem aQsWde15r
    Certificate 'ivanov.pem' copied from tftp://192.168.201.20.
```

`certificate import {file}`

Описание. Импорт сертификата или секретного ключа. Можно скопировать содержимое файла с экрана и вставить его в локальный файл с помощью текстового редактора.

Префикс NO. Не используется.

Аргументы.

file

Имя локального файла сертификата.

`certificate delele {file}`

Описание. Удаление сертификата или секретного ключа из репозитория.

Префикс NO. Не используется.

Аргументы.

file

Имя локального файла сертификата.

`show certificate`

Описание. Просмотр содержимого репозитория сертификатов. Каждая запись может содержать сертификат или секретный ключ. Оба могут быть зашифрованы.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 40. Просмотр содержимого репозитория сертификатов

```
RAPIRA: show certificates
Name            Certificate  Encrypted     Key  Encrypted
ivanov.crt      Yes          Off           No   N/A
ivanov.key      No           N/A           Yes  On
ivanov.pem      Yes          Off           Yes  On
```

Фильтрация на основе MAC-адреса

Общие положения

Фильтрация по MAC-адресу основана на списках управления доступом к среде. Каждый список содержит MAC-адреса; списки имеют уникальные имена. Списки можно устанавливать на беспроводные интерфейсы базовой станции либо в режиме `black`, либо в режиме `white`:

- `black` («черный список») означает, что разрешены все MAC-адреса, за исключением тех, что внесены в список
- `white` («белый список») означает, что блокируются все MAC-адреса за исключением тех, что внесены в список

Устройства, MAC-адреса которых заблокированы, не могут ассоциироваться с указанным интерфейсом. Если ассоциация была установлена до того, как MAC-адрес попал в"черный список", то данную ассоциацию можно разорвать вручную с помощью команды kick-mac.

Список команд

`mac-access-list {name} address {mac-address}`

Описание. Добавление MAC-адреса к списку. Если список не существует, то он будет создан.

Префикс NO. Удаление MAC-адреса из списка.

Аргументы.

name

Название списка контроля доступа.

mac-address

MAC-адрес в шестнадцатиричном формате с разделителем в виде точки: `xxxx.xxxx.xxxx`.

Пример 41. Настройка ACL

```
RAPIRA: mac-access-list test address 1111.2222.3333
MAC address '1111.2222.3333' has been added to 'test'.
RAPIRA: mac-access-list test address 2222.3333.4444
MAC address '2222.3333.4444' has been added to 'test'.
RAPIRA: show running-config mac-ac
mac-access-list test
 address 1111.2222.3333
 address 2222.3333.4444
```

Пример 42. Ту же самую операцию можно выполнить, используя компактную форму команды:

```
RAPIRA: mac-access-list test
mac-access-list: address 1111.2222.3333
MAC address '1111.2222.3333' has been added to 'test'.
mac-access-list: address 2222.3333.4444
MAC address '2222.3333.4444' has been added to 'test'.
mac-access-list: exit
```

`interface {name} {index} mac-access-list {acl-name} {black|white}`

Описание. Назначение указанному интерфейсу списка доступа (MAC ACL) в режиме «черного» или «белого» списка. Одномоментно можно назначить только один MAC ACL.

Префикс NO. Отключение MAC ACL от указанного интерфейса.

Аргументы.

acl-name

Название MAC ACL.

mode

Выбор режима"черного" или"белого" списка (см. описание выше).

Пример 43. Назначение интерфейсу списка доступа

```
RAPIRA: interface Wireless 0 mac-access-list test black
MAC access list has been assigned to the interface 'Wireless 0'.
RAPIRA: mac-access-list test address 13e4.c034.1122
MAC address '13e4.c034.1122' has been added to 'test'.
RAPIRA: show running-config mac-ac
mac-access-list test
 address 13e4.c034.1122
interface Wireless 0
 mac-access-list test black
RAPIRA: interface Wireless 0 no mac-access-list
MAC access list has been removed from the interface 'Wireless 0'.
RAPIRA: no mac-access-list test
MAC access list 'test' has been deleted.
```

`interface {name} {index} kick-mac {mac-address}`

Описание. Немедленно отсоединяет клиентскую станцию от базовой станции. Если MAC-адрес не запрещен через MAC ACL, то её можно подсоединить снова.

Префикс NO. Не используется.

Аргументы.

mac-address

MAC-адрес в шестнадцатеричном формате с разделителем в виде точки: `xxxx.xxxx.xxxx`.

Пример 44. Немедленное отсоединение клиентской станции от базовой

```
RAPIRA: mac-access-list 1
mac-access-list: address 0011.95df.8870
MAC address '0011.95df.8870' has been added to '1'.
mac-access-list: address 0090.27af.7840
MAC address '0090.27af.7840' has been added to '1'.
mac-access-list: exit
RAPIRA: interface Wireless 0 mac-access-list 1 black
MAC access list has been assigned to the interface 'Wireless 0'.
RAPIRA: interface Wireless 0 kick-mac 0090.27af.7840
Client with MAC address '0090.27af.7840' was disconnected.
RAPIRA: interface Wireless 0 kick-mac 0011.95df.8870
Client with MAC address '0011.95df.8870' was disconnected.
```

Мониторинг беспроводного интерфейса

Радио-подсистема клиентских станций принимает служебные сигналы от различных базовых станций. Фреймы содержат информацию о SSID, частоте, качестве сигнала, режимах безопасности и т.д. Данную информацию можно вывести на экран с помощью следующей команды:

`show interface {name} {index} scan`

Пример 45. Сканирование радиоэфира

```
RAPIRA: show interface Wireless 0 scan
Cell 01 - Address: 60B.6B37.4DC3
ESSID:"IVYA"
Type: ap
Freq: 2.412 GHz  (Channel 1)
Quality=8/70 Signal level=87 dBm Noise level=95 dBm
Bit Rate: 1.0 Mb/s
Bit Rate: 2.0 Mb/s
Bit Rate: 5.5 Mb/s
Bit Rate: 11.0 Mb/s
Bit Rate: 6.0 Mb/s
Bit Rate: 9.0 Mb/s
Bit Rate: 12.0 Mb/s
Bit Rate: 18.0 Mb/s
Bit Rate: 24.0 Mb/s
Bit Rate: 36.0 Mb/s
Bit Rate: 48.0 Mb/s
Bit Rate: 54.0 Mb/s
```

Режим сканирования может быть включен только на **клиентской станции**.

Сканирование может быть выполнено только при **поднятом** беспроводном интерфейсе.

Настройка MAC-адреса

Для смены MAC-адреса на интерфейсе используется следующая команда, имеющая один обязательный аргумент:

`interface {name} {index} mac-address {mac-address}`

Описание. Установка MAC-адреса интерфейса.

Префикс NO. Не используется.

Аргументы.

mac-address

MAC-адрес в шестнадцатиричном формате с разделителем в виде точки: `xxxx.xxxx.xxxx`.

Пример 46. Настройка MAC-адреса интерфейса

```
RAPIRA: interface FastEthernet 0 mac-address 1234.5678.90ab
MAC address is set to '1234.5678.90ab'.
```

Команда применима только к интерфейсам на базе Ethernet, как то: **FastEthernet**, **Wireless** или **Bridge**.

Если интерфейс конфигурирован как DHCP-клиент, то после изменения MAC-адреса он может получать различные IP-адреса.

Для просмотра текущего MAC-адреса интерфейса, используйте команду: show interfaces.

Настройка режима прозрачного моста

см. также *Примеры конфигураций*

Создание прозрачного моста

см. также Настройка базовой станции в режиме прозрачного моста

Если прозрачный мост с указанным номером уже был создан ранее, то первый шаг необходимо пропустить.

Список доступных сетевых интерфейсов вы можете просмотреть заранее при помощи команды show interfaces.

Процесс создания и настройки прозрачного моста состоит из пяти шагов:

1. Создайте интерфейс **Bridge**. Выберите свободный ID интерфейса моста, начиная с 0 и наберите:

```
RAPIRA: interface Bridge 0
Bridge 0 is created.
```

2. Включите мост:

```
RAPIRA: interface Bridge 0 no shutdown
Interface 'Bridge 0' is up.
```

3. Настройте IP-адрес и маску:

```
RAPIRA: interface Bridge 0 ip address 192.168.1.1
Device 'Bridge 0' address 192.168.1.1 netmask 255.255.255.0
```

4. Установите флаг WDS на беспроводном интерфейсе, чтобы включить прозрачную ретрансляцию ethernet-фреймов:

```
RAPIRA: interface  Wireless 0 wds-mode
WDS mode is turned on.
```

5. Добавьте проводной и беспроводной интерфейсы в группу созданного моста:

```
RAPIRA: interface Wireless 0 bridge-group 0
Interface 'Wireless 0' was added to the bridge group 0.
RAPIRA: interface FastEthernet 0 bridge-group 0
Interface 'FastEthernet 0' was added to the bridge group 0.
```

Важно:

После того, как интерфейс добавлен в группу моста, IP-адрес интерфейса удаляется. Если управление оборудованием осуществляется через интерфейс, добавляемый в группу моста, то следует убедиться, что мост и интерфейс имеют одинаковый IP-адрес. В противном случае, контроль над оборудованием будет потерян, в этом случае необходимо заново подключиться к маршрутизатору, используя IP-адрес созданного моста.

Проверка статуса моста по окончании настройки:

```
RAPIRA: show interfaces
Bridge 0 is up, link state is up
   Hardware address:  18fd.74b9.b310
   Internet address:  192.168.0.6 mask 255.255.255.0
                      broadcast:  192.168.0.255, MTU: 1500
Wireless 0 is up, link state is up
   Hardware address:  18fd.74b9.b311  VLAN: none
   Internet address:  0.0.0.0 mask 0.0.0.0
                      broadcast:  0.0.0.0, MTU: 1500
   Type: ap, SSID: "YVY", Mode: ht40+
   Speed: 0 Mb/s (auto), Access point: N/A
   Channel: 152, Frequency: 5760 MHz, Tx-power: 25 dBm
   RTS: off, Distance: 3000, WDS: on
   WMM: off, Beacon: 100
   Antenna: auto, IEEE 802.11g Protection: ?
FastEthernet 0 is up, link state is up
   Hardware address:  18fd.74b9.b310  VLAN: none
   Internet address:  0.0.0.0 mask 0.0.0.0
                      broadcast:  0.0.0.0, MTU: 1500
RAPIRA: show bridge-group
bridge name     bridge id               STP           interfaces
Bridge 0        8000.000347df32a8       no            FastEthernet 0
```

Удаление моста

Чтобы удалить мост, необходимо назначить так называемого «наследника» - IP legatee интерфейс. После удаления моста интерфейс-наследник получит его IP-адрес. У моста может быть только один наследник. Если у моста, нет наследника, то его невозможно удалить. Как правило, наследником моста является тот интерфейс, который используется для настройки оборудования.

```
RAPIRA: interface Bridge 0 ip legatee FastEthernet 0
Bridge legatee assigned.
RAPIRA: no interface Bridge 0
Bridge 0 is removed.
```

Нельзя последовательно удалять интерфейсы из группы моста. Можно только удалить сам мост, тем самым удалив все интерфейсы из его группы.

Просмотр статуса моста

Просмотреть статус группы моста и таблицу MAC адресов можно с помощью команд show bridge-group и show interface mac-table:

```
RAPIRA: show bridge-group 0
Bridge name     Bridge ID               STP           Interfaces
Bridge 0        8000.06026f23138c       no            Wireless 0
                                                      FastEthernet 0
RAPIRA: show interface Bridge 0 mac-table
Interface       MAC address      Local      Ageing timer
FastEthernet 0  0003.475f.4a5c   No            0.75
Wireless 0      0011.95df.8870   Yes           0.00
FastEthernet 0  000e.a61b.cef6   No           77.30
FastEthernet 0  0018.f3bc.dded   Yes           0.00
FastEthernet 0  001b.6394.51b0   No           47.89
FastEthernet 0  0050.8b01.7b35   No           28.82
FastEthernet 0  0014.c2d8.8b3e   No          126.81
FastEthernet 0  000d.293d.9e81   No           11.10
FastEthernet 0  0001.6cd2.f27a   No           59.11
```

Список команд

`interface {name} {index} bridge-group {bridge-group-index}`

Описание. Добавление интерфейса в группу моста.

Префикс NO. Не используется.

Аргументы.

bridge-group-index

Индекс **Bridge**-интерфейса, который предварительно следует создать, включить и настроить, прежде чем добавлять отдельные интерфейсы в его группу.

Пример 47. Добавление интерфейса в группу моста

```
RAPIRA: interface Bridge 0
Bridge 0 has been created.
RAPIRA: interface Bridge 0 ip address 192.168.0.1
Device 'Bridge 0' address 192.168.0.1 netmask 255.255.255.0.
RAPIRA: interface Bridge 0 no shutdown
Interface 'Bridge 0' is up.
RAPIRA: interface Wireless 0 bridge-group 0
Interface 'Wireless 0' was added to the bridge group '0'.
```

`interface {name} {index} ip legatee {legatee-name} {legatee-index}`

Описание. Назначение IP-наследника моста. При удалении моста интерфейс–наследник получает соответствующие IP-адрес и маску. Команда применима исключительно к интерфейсам **Bridge**.

Префикс NO. Отключение IP-наследника

Аргументы.

legatee-name

Имя интерфейса-наследника. Наследник должен обязательно входить в группу моста. Невозможно удалить интерфейс **Bridge**, если в его группу добавлены интерфейсы, но нет наследника.

legatee-index

Индекс интерфейса-наследника.

Пример 48. Назначение IP-наследника моста

```
RAPIRA: no interface Bridge 0
Bridge 'Bridge 0' doesn't have a legatee.
RAPIRA: interface Bridge 0 ip legatee Wireless 0
Bridge legatee assigned.
RAPIRA: no interface Bridge 0
Bridge 0 has been removed.
```

`show bridge-group [bridge-group-index]`

Описание. Просмотр членов группы моста.

Префикс NO. Не используется.

Аргументы.

bridge-group-index

Индекс группы моста, который необходимо просмотреть. Если аргументы отсутствуют, то отображаются все группы моста.

Пример 49. Просмотр членов группы моста

```
RAPIRA: show bridge-group 0
Bridge name     Bridge ID               STP           Interfaces
Bridge 0        8000.06026f23138c       no            Wireless 0
                                                      FastEthernet 0
```

`show interface {name} {index} mac-address-table`

Описание. Просмотр MAC-адресов интерфейса **Bridge**.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 50. Просмотр MAC-адресов прозрачного моста

```
RAPIRA: show interface Bridge 0 mac-table
Interface       MAC address      Local      Ageing timer
FastEthernet 0  0003.475f.4a5c   No            0.75
Wireless 0      0011.95df.8870   Yes           0.00
FastEthernet 0  000e.a61b.cef6   No           77.30
FastEthernet 0  0018.f3bc.dded   Yes           0.00
FastEthernet 0  001b.6394.51b0   No           47.89
FastEthernet 0  0050.8b01.7b35   No           28.82
FastEthernet 0  0014.c2d8.8b3e   No          126.81
FastEthernet 0  000d.293d.9e81   No           11.10
FastEthernet 0  0001.6cd2.f27a   No           59.11
```

Настройка VLAN

Общие положения

Используя VLAN можно создавать логические группы в сети. Виртуальные VLAN являются неотъемлемыми конструктивными элементами 2 уровня, при этом подсети IP представляют из себя конструктивные элементы 3 уровня. VLAN создаются для обеспечения разделения сети на сегменты, которую в традиционных LAN настройках обеспечивают маршрутизаторы.

Каждый VLAN представляет из себя логическую сеть и пакеты, не относящиеся ни к одному из имеющихся VLAN должны пересылаться через маршрутизатор.

При настройке виртуальных LAN используется протокол IEEE 802.1Q. IEEE 802.1Q добавляет тег к Ethernet фреймам. Рубрика Заголовок пакета IEEE 802.1Q содержит 4-х битовый тег, который, в свою очередь, состоит из 2-битового тега идентификатора протокола (TPID) и 2-битового тега управляющей информации (TCI). TPID имеет фиксированное значение 0x8100, указывающее на то, что данный пакет содержит тег 802.1Q. TCI включает в себя следующие элементы:

- Трех-битовое поле приоритета
- Индикатор формата (CFI) длиной в один бит
- Идентификатор VLAN длиной в двенадцать бит (VID). Идентифицирует VLAN, к которому принадлежит кадр.

Интерфейсы VLAN системы RAPIRA RS3 всегда передают и принимают кадры, снабженные тегом. Виртуальные LAN работают на 2 уровне модели OSI. Каждый VLAN устанавливает соответствие с сетью или подсетью IP, что внешне выглядит как включение в работу 3 уровня. RAPIRA RS3 поддерживает до 32 виртуальных LAN-интерфейсов.

VLAN-интерфейсы можно создать на физических интерфейсах на базе Eternet, типа **FastEthernet** или **Wireless**. После того, как VLAN-подинтерфейс создан, можно настроить для него IP-адрес.

Пример 51. Создание подинтерфейса VLAN

```
RAPIRA: interface FastEthernet 0.1 vlan 101
Interface 'FastEthernet 0.1' created.
VLAN ID: 101.
RAPIRA: interface FastEthernet 0.1 ip address 172.16.0.10/26
Device 'FastEthernet 0.1' address 172.16.0.10 netmask 255.255.255.192.
RAPIRA: show interfaces FastEthernet 0.1
FastEthernet 0.1 is down
   Hardware address:  0003.47df.32a8  VLAN: 101
   Internet address:  172.16.0.10 mask 255.255.255.192
broadcast:  172.16.0.63, MTU: 1500
```

VLAN-подинтерфейсы могут работать в качестве автономных интерфейсов сети, обеспечивая транспортировку пакетов IP между виртуальными сетями VLAN. Кроме того, система RAPIRA RS3 позволяет построить мосты, используя интерфейсы VLAN и SSID в качестве портов моста (см. Настройка множественных SSID). Обе функции можно комбинировать в одном и том же маршрутизаторе в зависимости от решаемой задачи, что обеспечивает достаточно гибкий механизм интегрирования сети.

Вариант с использованием множественных SSID: на базовой станции настраиваем Wireless-подинтерфейс с ssid "test101", на клиентской станции интерфейсы FastEthernet и Wireless помещаем в прозрачный мост, прописывая "test101" в качестве SSID:

Пример 52. Помещение VLAN в прозрачный мост на базовой станции с использованием множественных SSID

```
RAPIRA: interface FastEthernet 0.1 vlan 101
Interface 'FastEthernet 0.1' created.
VLAN ID: 101.
RAPIRA: interface Wireless 0 type ap
Interface 'Wireless 0': type 'ap'.
RAPIRA: interface Wireless 0.1 ssid test101
Interface 'Wireless 0.1' created.
SSID 'test101' registered.
RAPIRA: interface Bridge 1
Bridge 1 has been created.
RAPIRA: interface Bridge 1 no shutdown
Interface 'Bridge 1' is up.
RAPIRA: interface Bridge 1 ip address 172.16.0.10/26
Device 'Bridge 1' address 172.16.0.10 netmask 255.255.255.192.
RAPIRA: interface FastEthernet 0.1 bridge-group 1
Interface 'FastEthernet 0.1' was added to the bridge group '1'.
RAPIRA: interface Wireless 0.1 bridge-group 1
Interface 'Wireless 0.1' was added to the bridge group '1'.
RAPIRA: show bridge-group
Bridge name     Bridge id               STP          Interfaces
Bridge 1        8000.000347df32a8       0            FastEthernet 0.1
                                                     Wireless 0.1
```

Наконец, возможно терминировать VLAN на беспроводном интерфейсе и передавать кадры в сеть без тега следующим образом: на базовой станции интерфейсы FastEthernet и Wireless помещаем в прозрачный мост, на клиентских устройствах настраиваем соответствующие Wireless-подинтерфейсы и помещаем их и проводной интерфейс в прозрачный мост:

Пример 53. Помещение VLAN в прозрачный мост на клиентской станции для передачи в сеть без тега

```
RAPIRA: interface Wireless 0.1 vlan 101
Interface 'Wireless 0.1' created.
VLAN ID: 101.
RAPIRA: interface Bridge 1
Bridge 1 has been created.
RAPIRA: interface Bridge 1 no shutdown
Interface 'Bridge 1' is up.
RAPIRA: interface Bridge 1 ip address 172.16.0.10/26
Device 'Bridge 1' address 172.16.0.10 netmask 255.255.255.192.
RAPIRA: interface FastEthernet 0 bridge-group 1
Interface 'FastEthernet 0' was added to the bridge group '1'.
RAPIRA: interface Wireless 0.1 bridge-group 1
Interface 'Wireless 0.1' was added to the bridge group '1'.
RAPIRA: show bridge-group
Bridge name     Bridge id               STP          Interfaces
Bridge 1        8000.000347df32a8       0            FastEthernet 0
                                                     Wireless 0.1
```

Важно:

Если вы хотите передавать помеченные тегами кадры прозрачно между физическими интерфейсами, то НЕТ НЕОБХОДИМОСТИ создавать VLAN-подинтерфейсы. Необходимо просто добавить интерфейсы FastEthernet и Wireless непосредственно к прозрачному мосту.

Важно:

В том случае, если VLAN-подинтерфейсы созданы на **беспроводном** интерфейсе, они используют SSID основного беспроводного интерфейса. Дополнительные подинтерфейсы SSID не снабжены тегами.

Список команд

`interface {name} {index} vlan {vlan-id}`

Описание. Создание подинтерфейса VLAN. Изменение тега VLAN, если подинтерфейс уже существует.

Префикс NO. Не используется.

Аргументы.

vlan-id

Идентификатор VLAN. Допустимые значения: от 1 до 4094.

см. также Общие положения

см. также Настройка множественных SSID

QoS

Процедура приоритезации трафика работает следующим образом. Сначала определяется, является ли кадр тегированным (802.1q). Если да, то приоритезация фрейма осуществляется на основании приоритета, выставленного в теге. Если приоритет в теге нулевой, то система просматривает поле ToS ip-пакета.

Если тег в кадре отсутствует, сразу же просматривается поле ToS. Значения полей и соответствующие им категории трафика представлены в таблице.

Таблица 8. Значение поля TCI в 802.1q теге.

1,2,3	стандартный трафик
4	видео-трафик
5,6,7	голосовой трафик

см. также wmm

Соответствие значения поля ToS (DSCP) категории трафика представлены ниже:

TOS (DSCP)	Priority
0	BK
1	BK
2	BK
3	BK
4	BK 4 reset to VO
5	BK 5 reset to VO
6	BK 6 reset to VO
7	BK 7 reset to VO
8	BK
9	BK
a	BK
b	BK
c	BK c reset to VO
d	BK d reset to VO

TOS (DSCP)	Priority
e	BK e reset to VO
f	BK f reset to VO
10	BK
11	BK
12	BK
13	BK
14	BK 14 reset to VO
15	BK 15 reset to VO
16	BK 16 reset to VO
17	BK 17 reset to VO
18	BK
19	BK
1a	BK
1b	BK
1c	BK 1c reset to VO
1d	BK 1d reset to VO
1e	BK 1e reset to VO
1f	BK 1f reset to VO
20	VI
21	VI
22	VI
23	VI
24	VI 24 reset to VO
25	VI 25 reset to VO
26	VI 26 reset to VO
27	VI 27 reset to VO
28	VO
29	VO
2a	VO
2b	VO
2c	VO 2c reset to VO
2d	VO 2d reset to VO
2e	VO 2e reset to VO

TOS (DSCP)	Priority
2f	VO2 f reset to VO
30	VO
31	VO
32	VO
33	VO
34	VO 34 reset to VO
35	VO 35 reset to VO
36	VO 36 reset to VO
37	VO 37 reset to VO
38	VO
39	VO
3a	VO
3b	VO
3c	VO 3c reset to VO
3d	VO 3d reset to VO
3e	VO 3e reset to VO
3f	VO 3f reset to VO

Настройка IP-параметров

Параметры интерфейса

Каждый интерфейс сети в маршрутизаторе RAPIRA RS3 имеет следующие параметры:

1. IP-адрес и сетевую маску
2. широковещательный IP-адрес
3. размер MTU - максимальный размер блока в байтах, который может быть передан на канальном уровне протокола TCP/IP

IP address

```
interface {name} {index} ip address {ip-address} | ip-address/prefix | ip-address netmask} [secondary]
```

Описание. Указание IP-адреса и сетевой маски интерфейса.

Префикс NO. Удаление IP-адреса интерфейса.

Аргументы.

ip-address

IP-адрес интерфейса.

prefix

сетевая маска с сокращенной нотации (выборочно)

netmask

сетевая маска с стандартной нотации (выборочно).Если аргументы `prefix` или `netmask` опущены, то устанавливается стандартная сетевая маска, соответствующаа классу A, B или C в зависимости от установленного IP-адреса.

secondary

Дополнительное ключевое слово, указывающее, что добавляемый IP-адрес является псевдонимом. Маршрутизатор RAPIRA RS3 поддерживает до **16** вторичных адресов на один интерфейс.

Пример 54. Указание IP-адреса и сетевой маски интерфейса

Вы можете установить новый адрес `192.168.0.1` с сетевой маской `255.255.255.0`, используя любую из трех приведенных ниже команд:

```
RAPIRA: interface FastEthernet 1 ip address 192.168.0.1
    Device 'FastEthernet 1' address 192.168.0.1 netmask 255.255.255.0.
RAPIRA: interface FastEthernet 1 ip address 192.168.0.1/24
    Device 'FastEthernet 1' address 192.168.0.1 netmask 255.255.255.0.
RAPIRA: interface FastEthernet 1 ip address 192.168.0.1 255.255.255.0
    Device 'FastEthernet 1' address 192.168.0.1 netmask 255.255.255.0.
```

Пример 55. Добавление вторичных IP адресов

```
RAPIRA: interface Wireless 0 ip address 10.0.0.1
Device 'Wireless 0' address 10.0.0.1 netmask 255.0.0.0.
RAPIRA: interface Wireless 0 ip address 192.168.1.0/24 secondary
Secondary IP 192.168.1.0 netmask 255.255.255.0 was added.

RAPIRA: show interfaces
Wireless 0 is up
Hardware address:  0002.6f23.138c
Internet address:  10.0.0.1 mask 255.0.0.0
broadcast:  10.255.255.255, MTU: 1500
Secondary address: 192.168.1.0 255.255.255.0
Type: station, SSID:"test", Mode: 802.11a
Speed: 0 Mb/s (auto), Access point: Not associated
Channel: 56, Frequency: 5280 MHz, Tx-power: 16 dBm
RTS: off, Distance: 300, WDS: off, FastFrame: on
Burst: on, Compression: off, WMM: on, Beacon: 0
Antenna: auto, IEEE 802.11g Protection: none
FastEthernet 0 is up
Hardware address:  0003.42df.32ac
Internet address:  192.168.0.5 mask 255.255.255.0
broadcast:  192.168.0.255, MTU: 1500
```

Пример 56. Удаление вторичного IP-адреса

Чтобы удалить какой-то определенный IP-адрес из вторичных адресов, следует ввести его с префиксом **no**:

```
RAPIRA: interface Wireless 0 no ip address 192.168.1.10
    Secondary IP '192.168.1.10' was removed.
```

Пример 57. Удаление основного IP-адреса

Если удален основной IP-адрес, то удаляются и все вторичные IP-адреса.

```
RAPIRA: interface Wireless 0 no ip address 10.0.0.1
    All IP addresses of 'Wireless 0' were cleared.
```

Динамический IP-адрес (DHCP)

RAPIRA RS3 поддерживает динамические IP-адреса. Для этих целей используется протокол DHCP. Для того, чтобы запустить или остановить клиента DHCP используется следующая команда:

`interface {name} {index} ip dhcp`

Описание. Запуск DHCP-клиента на сетевом интерфейсе. Невозможно выполнить данную команду для субинтерфейса.

Префикс NO. Останов DHCP-клиента.

Аргументы. Аргументы отсутствуют.

Пример 58. Запуск DHCP-клиента

```
RAPIRA: interface Wireless 0 ip dhcp
    DHCP client enabled.
RAPIRA: interface Wireless 0 ip no dhcp
    DHCP client disabled.
```

DHCP-клиент автоматически получает IP-адрес, маршрут по умолчанию и DNS-адреса с сервера DHCP. Все указанные динамические параметры можно просмотреть с помощью следующих команд: show interfaces, show ip route и show ip name-server

Широковещательный IP-адрес

Команда устанавливает на интерфейс широковещательный IP адрес. Для использования в качестве широковещательного адреса можно назначить любой IP-адрес.

```
interface {name} {index} ip broadcast-address {broadcast-address}
```

Описание. Указание IP-адреса, который должен быть установлен в качестве пункта назначения в широковещательных пакетах.

Префикс NO. Не используется.

Аргументы.

broadcast-address

Широковещательный IP-адрес интерфейса.

Пример 59. Указание широковещательного IP-адреса

```
RAPIRA: interface FastEthernet 1 ip broadcast-address 192.168.255.255
    Broadcast address is set to 192.168.255.255.
```

После изменения IP-адреса интерфейса система автоматически меняет широковещательный адрес на установленный по умолчанию для нового фрагмента подсети.

Размер MTU

Для выполнения точной настройки параметров сети можно изменить значение MTU IP-протокола интерфейса с помощью команды:

```
interface {name} {index} ip mtu {mtu}
```

Описание. Настройка размера MTU на сетевом интерфейсе.

Префикс NO. Не используется.

Аргументы.

mtu

Размер MTU в байтах. Возможный диапазон значений от **60** до **1500**.

Пример 60. Настройка размера MTU

```
RAPIRA: interface FastEthernet 1 ip mtu 1400
    MTU is set to 1400.
```

DNS

Список доменных имен в маршрутизаторе RAPIRA RS3 сохраняется с помощью команды `ip name-server`. Команда добавляет новые записи в список доменных имен.

Просмотреть содержимое списка можно с помощью команды show ip name-server.

`ip name-server {ip-address}`

Описание. Добавление IP-адреса DNS-сервера в список имен.

Префикс NO. Удаление IP-адреса DNS-сервера из списка имен.

Аргументы.

ip-address

IP-адрес DNS-сервера.

Пример 61. Добавление IP-адреса DNS-сервера в список имен

```
RAPIRA: ip name-server 10.0.0.2
Name server address added.
RAPIRA: no ip name-server 10.0.0.2
Name server address deleted.
```

`show ip name-server`

Описание. Просмотр списка имен.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 62. DNS - просмотр списка имен

```
RAPIRA: ip name-server 10.0.0.1
Name server address added.
RAPIRA: ip name-server 10.0.0.2
Name server address added.
RAPIRA: show ip name-server
Name server: 10.0.0.1
Name server: 10.0.0.2
```

Имя домена

Имя домена – это имя локального домена. Большинство запросов на имена внутри данного домена могут пользоваться относительно короткими именами. Для установки доменного имени используется следующая команда:

`ip domain-name {name}`

Описание. Указание имени локального домена.

Префикс NO. Удаление имени локального домена.

Аргументы.

name

Имя локального домена.

Пример 63. Указание имени локального домена

```
RAPIRA: ip domain-name my-domain.lan
New domain name: my-domain.lan
RAPIRA: no ip domain-name
Domain name cleared.
```

`show ip domain-name`

Описание. Просмотр имени локального домена.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 64. Просмотр имени локального домена

```
RAPIRA: show ip domain-name
Domain name: my-domain
```

Можно также просмотреть имя домена, фильтруя данные текущего файла конфигурации с помощью поискового ключа `domain`:

```
RAPIRA: show running-config domain
ip
 domain-name my-domain
```

Имя хоста

Имя хоста – имя локального хоста. Это строковый идентификатор, уникальный в диапазоне локального домена.

`ip hostname {name}`

Описание. Установка имени локального хоста.

Префикс NO. Удаление имени локального хоста.

Аргументы.

name

Имя локального хоста.

Пример 65. Настройка имени локального хоста

```
RAPIRA: ip hostname my-host
Host name set.
RAPIRA: no ip hostname
Host name deleted.
```

`show ip hostname`

Описание. Просмотр имени локального хоста.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 66. Просмотр имени локального хоста

```
RAPIRA: show ip hostname
Hostname: my-host
```

Можно также просмотреть имя хоста, фильтруя данные текущего файла конфигурации с помощью поискового ключа `hostn`:

Пример 67. Просмотр имени локального хоста в файле конфигурации

```
RAPIRA: show running-config hostn
ip
 hostname my-host
```

Таблица ARP

Таблица ARP (протокола разрешения адресов) представляет из себя кеш, в котором хранятся соответствия между адресами канального уровня (MAC) и адресами сетевого уровня (IP). Операционная система сохраняет кеш ARP в RAM, кеш может динамически обновляться с помощью протокола ARP. В таблицу можно добавлять статические пункты.

Для настройки таблицы ARP в маршрутизаторе RAPIRA RS3 используйте следующую команду:

```
ip arptable arp {ip-address} {mac-address}
```

Описание. Добавление новой статической записи в таблицу ARP.

Префикс NO. Удаление записи из таблицы ARP.

Аргументы.

ip-address

IP-адрес новой записи.

mac-address

MAC-адрес новой записи.

Пример 68. Удаление записи из таблицы ARP

```
RAPIRA: ip arptable no arp 83.166.121.12 000e.34b8.3345
Specify an IP address to delete an ARP record.
RAPIRA: ip arptable no arp 83.166.121.12
ARP record deleted.
```

```
ip arptable size {size}
```

Описание. Установка максимального количества записей в ARP-таблице

Префикс NO. Не используется.

Аргументы.

size

Количество записей в таблице, возможный диапазон от **128** до **8192**.

Пример 69. Настройка максимального количества записей в ARP-таблице

```
RAPIRA: ip arptable size 4096
New table size: 4096.
```

```
show ip arptable arp
```

Описание. Просмотр кеша ARP.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 70. Просмотр кеша ARP

```
RAPIRA: show ip arptable arp
Address            HWaddress            Device
83.166.121.7       000e.a61b.cef6       FastEthernet 0
83.166.121.8       0001.6cd0.d7ea       FastEthernet 0
83.166.121.1       000d.293d.9e81       FastEthernet 0
```

`show ip arptable size`

Описание. Просмотр размера кеша ARP.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 71. Просмотр размера кеша ARP

```
RAPIRA: show ip arptable arp
ARP table sise: 128
```

Статическая маршрутизация и шлюз по умолчанию

Для изменения таблицы статической маршрутизации существует две команды: `ip route` и `ip default-gateway`. Первая используется для управления записями в таблице маршрутизации; вторая – для установки шлюза по умолчанию.

Чтобы добавить новую запись в таблицу маршрутизации, следует задать сеть пункта назначения и либо шлюз, либо интерфейс. Можно также задать метрику. При добавлении в сеть нового маршрута используется сетевой IP-адрес с маской либо в стандартной, либо в компактной нотации.

`ip route {ip-address netmask | ip-address/prefix} {gateway | interface} [metric]`

Описание. Добавление статического маршрута.

Префикс NO. Удаление статического маршрута.

Аргументы.

ip-address

IP-адрес сети пункта назначения.

netmask

Маска сети пункта назначения (стандартная нотация).

prefix

Длина маски сети пункта назначения (компактная нотация).

gateway

IP-адрес шлюза.

interface

Название и номер сетевого интерфейса.

metric

Метрика.

Пример 72. Настройка статической маршрутизации

```
RAPIRA: ip route 192.168.0.0 255.255.255.0 10.0.0.1
Static route added.
```

Альтернативный вариант:

Пример 73. Настройка статической маршрутизации - альтернативный вариант

```
RAPIRA: ip route 192.168.0.0/24 10.0.0.1
Static route added.
```

Если интерфейс сети пункта назначения не Ethernet, то вместо IP-адреса отдаленного шлюза можно назначить интерфейс:

Пример 74. Настройка статической маршрутизации - назначение интерфейса

```
RAPIRA: ip route 192.168.0.0/24 PPP 0
Static route added.
```

`ip default-gateway {gateway}`

Описание. Установка IP-адреса шлюза по умолчанию.

Префикс NO. Удаление установленного по умолчанию шлюза из таблицы маршрутизации.

Аргументы.

gateway

IP-адрес шлюза.

Пример 75. Установка IP-адреса шлюза по умолчанию

```
RAPIRA: ip default-gateway 10.0.0.1
Default route changed.
RAPIRA: no ip default-gateway
Default route deleted.
```

`show ip route`

Описание. Просмотр таблицы маршрутизации.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 76. Просмотр таблицы маршрутизации.

```
RAPIRA: show ip route
Destination     Mask            Gateway         Metric   Iface
83.166.121.0    255.255.255.240 *               0        FastEthernet 0
192.168.0.0     255.255.255.0   *               0        Wireless 0
default         0.0.0.0         83.166.121.1    1        FastEthernet 0
```

Статические хосты

Таблицу поиска статических хостов можно использовать как дополнение к DNS. В отличие от DNS данная таблица контролируется администратором маршрутизатора.

Для управления таблицей статических хостов используется следующая команда:

`ip host {ip-address} {hostname}`

Описание. Добавление новой записи в таблицу статических хостов.

Префикс NO. Удаление записи из таблицы хостов.

Аргументы.

ip-address

IP-адрес хоста.

hostname

Имя хоста.

Пример 77. Добавление новой записи в таблицу статических хостов

```
RAPIRA: ip host 192.168.0.3 my-static-host.lan
Static host record '192.168.0.3 my-static-host.lan' was added.
RAPIRA: no ip host my-static-host.lan
Static host record 'my-static-host.lan' was deleted.
```

`show ip hosts`

Описание. Просмотр таблицы статических хостов.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 78. Просмотр таблицы статических хостов.

```
RAPIRA: show ip hosts
IP address      Host
192.168.0.1     my-static-host.lan
10.0.0.1        second-static-host.lan
```

DHCP-сервер

Общая информация

Dynamic Host Control Protocol (DHCP) – протокол динамической конфигурации хоста позволяет автоматически присваивать многократно используемые IP-адреса клиентам DHCP. RAPIRA RS3 позволяет полностью реализовать функциональные возможности сервера DHCP.

База данных сервера DHCP представляет собой набор пулов. Каждый пул имеет уникальное имя, IP адрес, сетевую маску и тип. Тип представлен двумя вариантами: либо сеть либо хост. Пулы организованы в виде дерева, таким образом, чтобы при наличии единого сетевого адреса пулы с более длинными сетевыми масками оказались вложены в пулы с более короткими масками. Например, сетевой пул `p1 = 10.0.0.0/16` является **родителем** сетевого пула `p2 = 10.0.0.0/24`, а `p2` является **дочерним элементом** пула `p1`. Сетевые пулы `p3 = 192.168.1.0/24` и `p4 = 192.168.2.0/24` являются **элементами одного уровня**.

Пулы хоста всегда представляют из себя листья дерева. По умолчанию пулы хоста имеют маску `255.255.255.255`, благодаря чему они являются листьями самых узких пулов сети. Если установить маску сети, то можно поместить пул хоста в более высокие родительские сети. Например, если существует два пула сети: `pp = 192.168.0.0/16` и `p3 = 192.168.1.0/24`, то пул хоста `h1 = 192.168.1.101` является дочерним `p3`, а пул хоста `h2 = 192.168.1.102/16` является дочерним `pp` из-за маски сети.

Пример дерева пула:

```
┬
│
├сеть"pp" 192.168.0.0 255.255.0.0
│    │
│    ├сеть"p3" 192.168.1.0 255.255.255.0
│    │    │
│    │    └хост"h1" 192.168.1.101 255.255.255.255
│    │
│    ├сеть"p4" 192.168.2.0 255.255.255.0
│    │
│    └хост"h2" 192.168.1.102 255.255.0.0
│
├сеть"p1" 10.0.0.0 255.255.0.0
│
└сеть"p2" 10.0.0.0 255.255.255.0
```

Дочерние пулы наследуют родительские параметры. Поэтому общие параметры, к примеру, доменное имя, следует настраивать на более высоких уровнях дерева. Унаследованные параметры можно подменять. Например, если параметр определен как в родительской сети, так и в подсети, то для хостов подсети используется определение подсети.

Параметры пула:

- **lease** - время существования DHCP-пула, до **8** дней
- **default-router** - IP-адрес шлюза по умолчанию, допускается до **8** адресов
- **dns-server** - адрес DNS-сервера, допускается до **8** адресов
- **range** - диапазон сетевых адресов DHCP-пула, данный параметр является обязательным
- **mac-address** - MAC-адрес хоста DHCP-пула, данный параметр является обязательным

После того, как сервер DHCP включен, пулы и диапазоны сети связываются с реальными интерфейсами сети. Несмотря на то, что процедура объединения в пул автоматически производит классификацию, все же рекомендуется перед запуском DHCP сервера скорректировать диапазоны.

Пример 79. Настройка сетевого пула

```
RAPIRA: ip dhcp pool p1

RAPIRA:(dhcp-config): network 10.0.0.0 255.255.0.0
Pool"p1": network 10.0.0.0 255.255.0.0

RAPIRA:(dhcp-config): default-router 10.0.0.1 10.0.0.3

RAPIRA:(dhcp-config): dns-server 10.0.0.1 94.66.78.1

RAPIRA:(dhcp-config): range 10.0.1.10 10.0.1.120
Added range: 10.0.1.10 10.0.1.120.

RAPIRA:(dhcp-config): range 10.0.1.140 10.0.1.160
Added range: 10.0.1.140 10.0.1.160.

RAPIRA:(dhcp-config): exit

RAPIRA:(config): show running-config p1
ip
dhcp
pool p1
network 10.0.0.0 255.255.0.0
range 10.0.1.10 10.0.1.120
range 10.0.1.140 10.0.1.160
default-router 10.0.0.1 10.0.0.3
dns-server 10.0.0.1 94.66.78.1
```

Пример 80. Запуск сервиса DHCP

```
RAPIRA:  service dhcp
DHCP service enabled.
```

Пример 81. Настройка пула хоста

```
RAPIRA: ip dhcp pool sue
RAPIRA:(dhcp-config): host 10.0.1.121
Pool "sue": host 10.0.1.121

RAPIRA:(dhcp-config): mac-address 00c5.45e3.112a
Pool"sue" mac-address: 00c5.45e3.112a

RAPIRA:(dhcp-config): exit
RAPIRA: show running-config sue
ip
dhcp
pool sue
host 10.0.1.121 255.255.255.255
mac-address 00c5.45e3.112a
```

Пул хоста `sue` используется для статического назначения IP-адреса `10.0.1.121` MAC-адресу `00c5.45e3.112a`. Все остальные параметры, как например, адреса шлюза по умолчанию и адрес DNS-сервера, наследуются из пула сети `p1`.

Список команд

ip dhcp pool network

Описание: Определение типа пула как **сетевой**, назначение IP-адреса и маски.

Префикс **NO**: Определение типа пула как **'не определён' (undefined)**.

Аргументы:

- IP-адрес
- Маска

Обратите внимание:

Указание маски возможно как в стандартной, так и в сокращенной нотации.

Пример 82. Определение сетевого пула (первые две команды функционально идентичны)

```
RAPIRA: ip dhcp pool p1 network 10.0.0.0 255.255.0.0
Pool"p1": network 10.0.0.0 255.255.0.0

RAPIRA: ip dhcp pool p1 network 10.0.0.0/16
Pool"p1": network 10.0.0.0 255.255.0.0

RAPIRA: ip dhcp pool p1 no network
Pool"p1": disabled
```

ip dhcp pool host

Описание: Определение типа пула как **хост**, назначение IP-адреса и (выборочно) маски. Маска по умолчанию: `255.255.255.255`.

Префикс **NO**: Определение типа пула как **'не определен' (undefined)**.

Аргументы:

- IP-адрес
- Маска

Пример 83. Определение пула"хост"

```
RAPIRA: ip dhcp pool h1 host 10.0.0.4
Pool"h1": host 10.0.0.4
```

ip dhcp pool range

Описание: Добавление диапазона адресов DHCP-клиента в **сетевой** пул. Возможно добавление нескольких диапазонов. Если указанный диапазон пересекается с уже существующим - диапазоны автоматически объединяются.

Префикс **NO**: Удаление DHCP-диапазона. Существующие диапазоны автоматически разделяются или усекаются в соответствии с аргументом.

Аргументы:

- Первый IP-адрес диапазона
- Последний IP-адрес диапазона

Пример 84. Добавление диапазона адресов DHCP-клиента

```
RAPIRA: ip dhcp pool p1 range 10.0.0.1 10.0.0.6
Added range: 10.0.0.1 10.0.0.6.

RAPIRA: ip dhcp pool p1 no range 10.0.0.3 10.0.0.4
Deleted range: 10.0.0.3 10.0.0.4.

RAPIRA: show running-config p1
ip
dhcp
pool p1
range 10.0.0.1 10.0.0.2
range 10.0.0.5 10.0.0.6
```

Обратите внимание:

Пулы **хост** или **неопределенный** пул могут принимать настройки диапазона даже учитывая, что никакого эффекта данное действие не возымеет.

ip dhcp pool lease

Описание: Настройка времени существования DHCP-пула в днях, часах и минутах, либо **бессрочно (infinite)**.

Префикс **NO**: Установка времени существования DHCP-пула как **бессрочно (infinite)**.

Аргументы:

- Дни, либо - до **7**, либо **infinite (бессрочно)**
- Часы (выборочно), от **0** до **23**
- Минуты (выборочно), от **0** до **59**

Пример 85. Установка времени существования DHCP-пула

```
RAPIRA: ip dhcp pool p1

RAPIRA:(dhcp-config): lease 0 12 0
Pool"p1": lease time is set to 43200 sec

RAPIRA:(dhcp-config): lease infinite
Pool"p1": lease time is set to infinite
```

ip dhcp pool default-router

Описание: Установка IP-адреса шлюза по умолчанию для DHCP-клиентов.

Префикс **NO**: Удаление IP-адреса шлюза по умолчанию для DHCP-клиентов.

Аргументы:

- До **8** IP-адресов шлюзов.

Пример 86. Установка IP-адреса шлюза по умолчанию для DHCP-клиентов

```
RAPIRA: ip dhcp pool p1

RAPIRA:(dhcp-config): default-router 10.0.0.10 10.0.0.11
```

ip dhcp pool dns-server

Описание: Установка IP-адреса DNS-сервера для DHCP-клиентов.

Префикс **NO**: Удаление IP-адреса DNS-сервера для DHCP-клиентов.

Аргументы:

- До **8** IP-адресов DNS-серверов.

Пример 87. Установка IP-адреса DNS-сервера для DHCP-клиентов

```
RAPIRA: ip dhcp pool p1

RAPIRA:(dhcp-config): dns-server 10.0.0.100 10.0.0.101
```

ip dhcp pool mac-address

Описание: Установка MAC-адреса для пула **хост**.

Префикс **NO**:Удаление MAC-адреса для пула **хост**.

Аргументы:

- MAC-адрес

Пример 88. Установка MAC-адреса для пула

```
RAPIRA: ip dhcp pool sue

RAPIRA:(dhcp-config): mac-address 00c5.45e3.112a
Pool"sue" mac-address: 00c5.45e3.112a
```

Обратите внимание:

Пулы **network (сеть)** или **undefined (не определён)** могут принимать настройки MAC-адреса, даже учитывая, что никакого эффекта данное действие не возымеет.

Firewall и NAT

Списки контроля доступа

Списки контроля доступа (Access Control Lists – ACLs) маршрутизатора RAPIRA RS3 позволяют пропускать или отклонять пакеты, поступающие с определенных IP-адресов отправителя на определенные IP-адреса или порты получателя. Они также позволяют назначать различные типы трафика, как например, ICMP, TCP или UDP.

Типичная запись ACL включает в себя четыре основных части:

- **Identifier (идентификатор)** списка ACL – положительное целое число, идентифицирующее список. Новые записи добавляются в конец списка.
- **Action (действие)** На данный момент возможны два действия: **разрешить (permit)** и **отклонить (deny)**.

- **Source (источник)** – указывает хост или сетевой адрес, после которого опционально указывается TCP или UDP порт.
- **Destination (получатель)** – параметр идет после **source** и имеет тот же самый формат (подробное описание формата см. ниже).

Запись также может содержать несколько необязательных полей:

- **Тип протокола**, возможные значения: **icmp**, **tcp** или **udp**.
- **Состояние соединения**, возможные значения: **new (новое)**, **established (установленное)** или **related (связанное с уже установленным соединением)**. РЭС RAPIRA RS3 применяет тип многоуровневого брандмауэра SPI (stateful packet inspection), т.е. отслеживает пакеты в контексте предыдущих соединений между тем же самым источником и получателем. Можно комбинировать ключевые слова состояния (соединения) в одной и той же записи ACL, отделяя их запятой («,»).

С учетом вышеизложенного, команды ACL имеют следующий формат:

```
access-list {id} {permit | deny} [protocol] {source} {destination} [state state]
```

Проходящие пакеты сравниваются с записями списка ACL в том порядке, в каком эти записи появляются в списке. Новые записи добавляются в конец списка. Когда соответствующая запись найдена, к пакету немедленно применяется действие: либо разрешить **(permit)** – либо отклонить **(deny)** прохождение пакета. Поэтому следует поставить часто употребляемые записи в начало списка. Кроме этого, последней записью в ACL списке должна стоять политика по умолчанию, которая блокирует или пропускает все не соответствующие списку пакеты.

Спецификаторы параметров source и destination

Каждая запись ACL может соответствовать или адресу хоста или группе адресов. В случае одного хоста, следует использовать ключевое слово **host** + IP-адрес. Группу адресов можно описать с помощью IP- адреса и перевернутой маски сети.

После этого источник и конечный пункт можно описать более точно, используя номер порта с соответствующим оператором сравнения.

- **eq** - "равно"
- **neq** - "не равно"
- **lt** - "меньше чем"
- **gt** - "больше чем"

Наконец, ключевое слово **any** используется, если необходимо разрешить любой IP-адрес и порт.

Таблица 9. Перечень спецификаторов

Тип	Формат
Одиночный адрес	`host {ip-address} [eq | neq | lt | gt port]`

Тип	Формат
Группа адресов	`{ip-address} {wildcard} [{eq | neq | lt | gt} port]`
Любой адрес и порт	any

Связывание списка доступа

Чтобы активировать ACL -список, его необходимо связать с сетевым интерфейсом при помощи следующей команды:

```
interface {name} {index}  access-group {ACL -id} {in | out}
```

Примеры настройки

Пример 89. ACL - полный запрет прохождения трафика

```
access-list 100 deny any any
interface FastEthernet 0 access-group 100 in
interface Wireless 0 access-group 100 in
```

Пример 90. ACL - разрешить TCP

```
access-list 100 permit tcp any any
access-list 100 deny any any
interface FastEthernet 0 access-group 100 in
interface Wireless 0 access-group 100 in
```

Пример 91. ACL - разрешить TCP для указанной подсети

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any
access-list 100 deny any any
access-list 101 permit tcp any any state established,related
access-list 101 deny any any
interface FastEthernet 0 access-group 100 in
interface Wireless 0 access-group 101 in
```

Пример 92. ACL - открыть различные TCP-порты

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80 state new
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 110 state new
access-list 100 permit tcp host 192.168.1.25 any eq 25 state new
access-list 100 deny any any
access-list 101 permit tcp any any state established,related
access-list 101 deny any any
interface FastEthernet 0 access-group 100 in
interface Wireless 0 access-group 101 in
```

Обратите внимание:

Обычно правила TCP отменяются правилом, разрешающим все установленные и связанные друг с другом пакеты. В большинстве случаев это необходимо для управления соединениями протокола TCP.

Просмотр списка ACL

Команда `show access-list` выводит на экран содержание списка контроля доступом.

```
show access-list [list-id]
```

Пример 93. Просмотр ACL

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80 state new
Rule added to access list '100'.
RAPIRA: access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 110 state new
Rule added to access list '100'.
RAPIRA: access-list 100 permit tcp host 192.168.1.25 any eq 25 state new
Rule added to access list '100'.
RAPIRA: access-list 100 deny any any
Rule added to access list '100'.
RAPIRA: access-list 101 permit tcp any any state established,related
Rule added to access list '101'.
RAPIRA: access-list 101 deny any any
Rule added to access list '101'.
RAPIRA: show access-list
access-list 100
deny tcp any any
permit tcp 192.168.1.0 0.0.0.255 any eq 80 state new
permit tcp 192.168.1.0 0.0.0.255 any eq 110 state new
permit tcp host 192.168.1.25 any eq 25 state new
deny any any
access-list 101
permit tcp any any state established,related
deny any any
RAPIRA: show access-list 101
access-list 101
permit tcp any any state established,related
deny any any
```

NAT

Преобразование сетевых адресов (NAT, Network Address Translation, второе название - Network Masquerading) – это метод приемо-передачи трафика по сети через маршрутизатор. NAT включает в себя трансляцию IP-адресов источника или получателя, а также (как правило) номеров TCP/UDP портов IP-пакетов по мере их прохождения в сети. Маршрутизатор RAPIRA RS3 транслирует как адреса получателя **(destination)**, так и адреса источника **(source)** - соответственно **DNAT** и **SNAT**.

SNAT заменяет адрес источника пакета определенным IP-адресом. В большинстве случаев, определенный адрес - это один из сетевых адресов интерфейса маршрутизатора. Иногда адрес маршрутизатора является динамическим. В этом случае в момент настройки NAT он неизвестен. В дополнение к SNAT и DNAT маршрутизатор RAPIRA RS3 предлагает опцию, называемую **МАСКАРАДИНГОМ** – она автоматически подставляет текущий адрес интерфейса сети вместо адреса источника.

Правила DNAT, SNAT и маскарадинг можно описать с помощью команды **nat-list**. Синтаксис команды очень похож на синтаксис списка ACL. Каждая запись в NAT имеет идентификатор списка, действие, источник и получателя. Различие состоит в том, что правила snat и dnat имеют дополнительный раздел **to**, в котором описываются адрес или диапазон адресов, которые используется для трансляции. Раздел **to** можно также использовать для того, чтобы указать те порты TCP/UDP, которые необходимо поместить в транслируемые пакеты.

```
nat-list {id} {snat | dnat} [protocol] {source} {destination} to {new-address-or-range} [eq | lt | gt port]
```

```
nat-list {id} {masquerade} [protocol] {source} {destination} [eq | lt | gt port]
```

Для того чтобы список NAT заработал, он должен быть присоединен к сетевому интерфейсу:

```
interface {name} {index} nat-group {list-id}
```

Важно:

Каждый сетевой интерфейс поддерживает только один список NAT.

Примеры настройки

Пример 94. Настройка NAT

1. В том случае, если частная сеть 192.168.1.0/24 подсоединена к **FastEthernet 0**, а беспроводной интерфейс **Wireless 0** имеет внешний адрес 10.0.0.1, то можно включить SNAT подобным образом:

   ```
   nat-list 110 snat 192.168.1.0 0.0.0.255 any to 10.0.0.1
   interface Wireless 0 nat-group 110
   ```

2. Если внешний адрес интерфейса неизвестен:

   ```
   nat-list 120 masquerade 192.168.1.0 0.0.0.255 any
   interface Wireless 0 nat-group 120
   ```

3. Если у частной сети имеется внутренний веб-сервер 192.168.1.10 и к нему необходимо предоставить доступ:

```
nat-list 120 dnat any any eq 80 to 192.168.1.10 eq 80
nat-list 120 dnat any any eq 443 to 192.168.1.10 eq 443
nat-list 120 dnat any any eq 8080 to 192.168.1.10 eq 8080
interface Wireless 0 nat-group 120
```

Просмотр списка NAT

Команда **show nat-list** выводит на экран содержимое списка NAT:

```
show nat-list [list-id]
```

PPP

Общая информация

Маршрутизатор RAPIRA RS3 поддерживает до 10 параллельных соединений клиентов точка-точка (PPP). Каждое соединение можно настроить сначала в разделе **interface**, а затем установив соответствующий тип (PPP) и индекс интерфейса. PPP в маршрутизаторе RAPIRA RS3 используется в качестве транспорта для протокола IP и поддерживает инкапсуляцию PPTP и PPP over Ethernet.

Для обеспечения PPP соединения с сервером доступа каждый PPP-интерфейс имеет как минимум три необходимых установки: инкапсуляция **(encapsulation)**, авторизация **(authentication)** и набор мандатов **(credentials)** - для авторизации. Инкапсуляция устанавливается с помощью команд interface pptp или interface pppoe, за которыми следуют конкретные параметры инкапсуляции. Авторизацией может быть один из следующих протоколов: PAP, CHAP, MSCHAP или MSCHAPv2. Некоторые PPP серверы доступа могут также потребовать протокол MPPE.

И, наконец, в набор мандатов входит identity и password.

После настройки всех необходимых установок, интерфейс PPP автоматически начинает устанавливать пробные соединения с удаленным PPP-концентратором. Вы можете отменить автосоединение, выбрав команду no connect или запустить его с помощью команды connect.

После успешной установки PPP-соединения, запускается процесс локального соединения точка-точка, при этом удаленный IP-адрес служит маршрутом по умолчанию и принимает адреса, динамически присвоенные удаленным DNS-сервером. Можно изменить предустановленное по умолчанию поведение, используя команды interface ip no default-gateway и interface ip no name-servers.

Пример 95. Интерфейс PPTP

```
RAPIRA: interface PPP 3
Interface 'PPP 3' has been created.
RAPIRA: interface PPP 3 no connect
PPP autoconnection disabled.
RAPIRA: interface PPP 3 pptp pptp.example.net
PPTP encapsulation enabled.
Using server pptp.example.net.
RAPIRA: interface PPP 3 authentication identity DOMAIN\00334
Using identity 'DOMAIN\00334'.
RAPIRA: interface PPP 3 authentication password eeoiu3098
Password has been saved.
RAPIRA: interface PPP 3 authentication mschap-v2
MSCHAPv2 enabled.
RAPIRA: interface PPP 3 encryption mppe
MPPE enabled.
RAPIRA: interface PPP 3 ip no default-gateway
PPP default route disabled.
RAPIRA: show running-config
...
!
interface PPP 3
interface PPP 3
 no connect
 pptp pptp.example.net
 authentication
  identity DOMAIN\00334
  password eeoiu3098
  mschap-v2
 encryption
  mppe
 ip
  no default-gateway
!
...
```

Пример 96. Интерфейс PPOE

```
RAPIRA: interface PPP 3
Interface 'PPP 3' has been created.
RAPIRA: interface PPP 3 pppoe FastEthernet 0 STREAM
PPPoE encapsulation enabled.
Using interface FastEthernet 0.
RAPIRA: interface PPP 3 authentication identity ppp0989330@mtu
Using identity 'ppp0989330@mtu'.
RAPIRA: interface PPP 3 authentication password 9OI39foi
Password has been saved.
RAPIRA: interface PPP 3 authentication chap
CHAP enabled.
RAPIRA: show services
Name                          Enabled  Running
...
Connector PPP 2               No       No
Connector PPP 3               Yes      Yes
RAPIRA: show running-config
...
!
interface PPP 3
interface PPP 3
 pppoe FastEthernet 0 STREAM
 authentication
  identity ppp0989330@mtu
  password 9OI39foi
  chap
!
...
RAPIRA: no interface PPP 3
Interface 'PPP 3' has been removed.
```

Список команд

`interface {name} {index} pptp {pptp-server}`

Описание. Включение PPTP-инкапсуляции.

Префикс NO. Выключение PPTP-инкапсуляции.

Аргументы.

pptp-server

IP-адрес или имя хоста PPTP-сервера, с которым предполагается соединение.

Пример 97. Включение PPTP-инкапсуляции

```
RAPIRA: interface PPP 1 pptp pptp.example.net
PPTP encapsulation enabled.
Using server pptp.example.net.
RAPIRA: interface PPP 1 no pptp
PPTP encapsulation disabled.
```

`interface {name} {index} pppoe {interface-name interface-index} [access-concentrator [service]]`

Описание. Включение PPPoE-инкапсуляции.

Префикс NO. Выключение PPPoE-инкапсуляции.

Аргументы.

interface-name

Имя того интерфейса на базе Ethernet, который предполагается использовать для PPPoE. Могут быть использованы интерфейсы: **FastEthernet** и **Bridge**.

interface-index

Индекс Ethernet-интерфейса.

access-concentrator

Идентификатор концентратора доступа PPPoE. Данный параметр необходимо использовать, если выбранный сегмент Ethernet имеет много концентраторов.

service

Идентификатор сервиса PPPoE. Данный параметр необходимо использовать, если выбранный концентратор доступа выполняет множество сервисов.

Пример 98. Включение PPPoE-инкапсуляции</title>

```
RAPIRA: interface PPP 1 pppoe FastEthernet 0 STREAM
PPPoE encapsulation enabled.
Using interface FastEthernet 0.
RAPIRA: interface PPP 1 no pppoe
PPPoE encapsulation disabled.
```

`interface {name} {index} authentication identity {login}`

Описание. Настройка логина PPP-аутентификации.

Префикс NO. Удаление логина PPP-аутентификации.

Аргументы.

login

Указание логина аутентификации.

Пример 99. Настройка логина PPP-аутентификаци

```
RAPIRA: interface PPP 1 authentication identity pango
Using identity 'pango'.
RAPIRA: interface PPP 1 authentication no identity
Identity has been cleared.
```

`interface {name} {index} authentication password {password}`

Описание. Указание пароля PPP-аутентификации.

Префикс NO. Удаление пароля PPP-аутентификации.

Аргументы.

password

Ввод пароля аутентификации.

Пример 100. Указание пароля PPP-аутентификации

```
RAPIRA: interface PPP 1 authentication password 508.drill?door
Password has been saved.
RAPIRA: interface PPP 1 authentication no password
Password has been cleared.
```

`interface {name} {index} connect`

Описание. Включение PPP-автосоединения.

Префикс NO. Отключение PPP-автосоединения. По умолчанию данный параметр включен. Состояние, когда автосоединение выключено, можно просмотреть только при просмотре `running-config`.

Аргументы. Аргументы отсутствуют.

Пример 101. Включение PPP-автосоединения

```
RAPIRA: interface PPP 0 connect
PPP autoconnection enabled.
RAPIRA: interface PPP 0 no connect
PPP autoconnection disabled.
```

`interface {name} {index} encryption mppe`

Описание. Включение MPPE-шифрования.

Префикс NO. Выключение MPPE-шифрования.

Аргументы. Аргументы отсутствуют.

Пример 102. Включение MPPE-шифрования

```
RAPIRA: interface PPP 2 encryption mppe
MPPE enabled.
RAPIRA: interface PPP 2 encryption no mppe
MPPE disabled.
```

`interface {name} {index} authentication pap`

Описание. Включение PAP-шифрования.

Префикс NO. Выключение PAP-шифрования.

Аргументы. Аргументы отсутствуют.

Пример 103. Включение PAP-шифрования

```
RAPIRA: interface PPP 1 authentication pap
PAP enabled.
RAPIRA: interface PPP 1 no authentication pap
PAP disabled.
```

`interface {name} {index} authentication chap`

Описание. Включение CHAP-шифрования.

Префикс NO. Выключение CHAP-шифрования.

Аргументы. Аргументы отсутствуют.

Пример 104. Включение CHAP-шифрования

```
RAPIRA: interface PPP 1 authentication chap
CHAP enabled.
RAPIRA: interface PPP 1 no authentication chap
CHAP disabled.
```

`interface {name} {index} authentication mschap`

Описание. Включение MSCHAP-шифрования.

Префикс NO. Выключение MSCHAP-шифрования.

Аргументы. Аргументы отсутствуют.

Пример 105. Включение MSCHAP-шифрования

```
RAPIRA: interface PPP 1 authentication mschap
MSCHAP enabled.
RAPIRA: interface PPP 1 no authentication mschap
MSCHAP disabled.
```

`interface {name} {index} authentication mschap-v2`

Описание. Включение MSCHAPv2-шифрования.

Префикс NO. Выключение MSCHAPv2-шифрования.

Аргументы. Аргументы отсутствуют.

Пример 106. Включение MSCHAPv2-шифрования

```
RAPIRA: interface PPP 1 authentication mschap-v2
MSCHAPv2 enabled.
RAPIRA: interface PPP 1 no authentication mschap-v2
MSCHAPv2 disabled.
```

`interface {name} {index} ip default-gateway`

Описание. Использование в качестве шлюза по умолчанию удаленного IP-адреса.

Префикс NO. Отключение использования в качестве шлюза по умолчанию удаленного IP-адреса. Состояние, когда данный параметр отключен, можно просмотреть только при просмотре running-config.

Аргументы. Аргументы отсутствуют.

Пример 107. Использование в качестве шлюза по умолчанию удаленного IP-адреса

```
RAPIRA: interface PPP 1 ip default-gateway
PPP default route enabled.
RAPIRA: interface PPP 1 ip no default-gateway
PPP default route disabled.
```

`interface {name} {index} ip name-servers`

Описание. Учитываются IP-адреса DNS-серверов.

Префикс NO. Игнорируются адреса IP-адресов DNS-серверов. Состояние, когда данный параметр отключён, можно просмотреть только при просмотре **running-config**.

Аргументы. Аргументы отсутствуют.

Пример 108. Учёт IP-адресов DNS-серверов.

```
RAPIRA: interface PPP 1 ip name-servers
PPP name servers enabled.
RAPIRA: interface PPP 1 ip no name-servers
PPP name servers disabled.
```

Настройка RADIUS

Общее описание

Маршрутизатор RAPIRA RS3 поддерживает авторизацию на базе RADIUS. Для настройки RADIUS необходимо создать профиль сервера RADIUS. В каждом профиле содержится список записей RADIUS-сервера. Каждая запись содержит набор параметров RADIUS-сервера: IP-адрес RADIUS сервера, порт авторизации, порт статистики соединения и секретное слово.

Если авторизация и порт статистики не указаны, то запись используется в качестве сервера авторизации с портом **1812**. Если установлены оба параметра: и порт авторизации и порт статистики, то запись используется для обоих.

На момент написания настоящей инструкции, профили RADIUS используются только для авторизации WPA.

Список команд

`radius-profile {name}`

Описание. Создание или настройка существующего профиля RADIUS.

Префикс **NO**: Удаление профиля.

Аргументы.

name

Имя профиля.

`radius-profile {name} server {ip-address} [auth-port auth-port] [acct-port acct-port] [key secret]`

Описание. Добавление в профиль записи RADIUS-сервера.

Префикс **NO**: Удаление записи из профиля.

Аргументы.

name

Имя профиля.

ip-address

IP-адрес RADIUS-сервера.

auth-port

Порт авторизации (выборочно) , по умолчанию используется 1812 порт.

acct-port

Порт статистики (выборочно), по умолчанию не используется.

secret

Секретное ключевое слово (выборочно).

Пример 109. Добавление в профиль записи RADIUS-сервера

```
RAPIRA: radius-profile r1
Created profile 'r1'.

RAPIRA:(config-rad-profile): server 10.0.1.40 auth-port 8012 key eRFiduKdjfr55
Added RADIUS server 10.0.1.40 to profile 'r1'.

RAPIRA:(config-rad-profile): server 10.0.1.41 acct-port 8013 key fkdIjehffidJ24
Added RADIUS server 10.0.1.41 to profile 'r1'.

RAPIRA:(config-rad-profile): server 10.0.1.42
Added RADIUS server 10.0.1.42 to profile 'r1'.

RAPIRA:(config-rad-profile): no server 10.0.1.42
Server '10.0.1.42' deleted.

RAPIRA:(config-rad-profile): exit
RAPIRA: show running-config rad
radius-profile r1
server 10.0.1.40 auth-port 8012 key eRFiduKdjfr55
server 10.0.1.41 acct-port 8013 key fkdIjehffidJ24
```

Настройка SNMP

Общее описание

Протокол SNMP используется для мониторинга состояния сетевых устройств, которые требуют участия администратора.

SNMP-агент обеспечивает интерфейс для мониторинга состояния устройства с помощью соответствующего протокола.

SNMP-агент позволяет сетевым администраторам осуществлять мониторинг работы сети, находить и оперативно решать возникающие сетевые проблемы.

Список команд

`snmp {allow | community | contact | location}`

Описание. Настройка параметров агента SNMP.

Префикс **NO**: удаление параметра.

Аргументы.

allow {ip} | {ip}/ {mask-length} | {ip} {mask}

Адраса устройств, с которых разрешён доступ к маршрутизатору.

community {community-name}

Пароль доступа к устройству.

contact {contact-info}

Контактная информация ответственного лица.

location {location-string}

Описание расположения устройства.

Пример 110. Настройка параметров агента SNMP

```
RAPIRA: service snmp
SNMP agent is enabled.

RAPIRA:snmp allow 192.168.0.130
An allow entry was added.

RAPIRA:snmp contact support@nporapira.ru
A contact string is set to 'support@nporapira.ru'.

RAPIRA:snmp community AsDfGhJk
A community name is set to 'AsDfGhJk'.

RAPIRA:snmp location here
A location string is set to 'here'.

RAPIRA: show running-config snmp
snmp
community AsDfGhJk
contact support@nporapira.ru
location here
allow 192.168.0.130
service
snmp
```

Обновление системы

Загрузка и обновление программного обеспечения

Описание

Маршрутизатор RAPIRA RS3 имеет встроенную функцию обновления. Чтобы обновить системное программное обеспечение (ПО), необходимо запустить и настроить tftp-сервер (имеется на прилагаемом компакт-диске), поместить в его корневую папку новое ПО, а затем выполнить следующее:

1. Загрузить новое системное ПО, используя команду `copy tftp flash {xxx.xxx.xxx.xxx} RAPIRA`, где **xxx.xxx.xxx.xxx** - ip-адрес tftp-сервера, **filename** - имя загружаемого файла, расположенного на tftp-сервере
2. Выполнить команду `system update`, подтверждая последующие вопросы ответом **Yes** (с соблюдением регистра символов при вводе).

Пример 111. Обновление системного ПО

```
RAPIRA: copy tftp flash 192.168.0.1 RAPIRA.img

392659 bytes copied.
780755 bytes copied.
...
14376358 bytes copied.
14768038 bytes copied.

New system update downloaded.
RAPIRA: system update

WARNING. Do you want to upgrade system ? (Yes/No) : Yes
WARNING. Are you sure? (Yes/No) : Yes
```

Ни в коем случае нельзя перезагружать систему во время обновления системного ПО. Это может привести к неработоспособности всей системы! Обновление ПО занимает не более 5 минут, после чего устройство будет автоматически перезагружено.

Список команд

`copy tftp flash {ip-address} RAPIRA`

Описание. Загрузка образа системного программного обеспечения с TFTP-сервера.

Префикс NO. Не используется.

Аргументы.

ip-address

IP-адрес TFTP-сервера.

filename

Имя файла образа.

Пример 112. Загрузка системного программного обеспечения с TFTP-сервера

```
RAPIRA: copy tftp flash 192.168.0.1 RAPIRA.img
392659 bytes copied.
780755 bytes copied.
...
14376358 bytes copied.
14768038 bytes copied.
New system update downloaded.
```

`system update`

Описание. Обновление системного программного обеспечения с использованием загруженного образа.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 113. Обновление системного программного обеспечения с использованием загруженного образа

```
RAPIRA: system update
WARNING. Do you want to upgrade system ? (Yes/No) : Yes
WARNING. Are you sure? (Yes/No) : Yes
```

Перезагрузка системы

Перезагрузка системы RAPIRA RS3 выполняется с помощью команды `reboot`. Вы так же можете запланировать отложенную перезагрузку, используя необязательный аргумент команды. Данная функция может быть полезна, если вы впервые работаете с системой и не уверены в корректности вводимых команд. Для этого:

1. Установите временной интервал перезагрузки.
2. Введите необходимые команды не сохраняя файл конфигурации. Если в результате настройки система работает не так как вы того хотели, то после перезагрузки система восстановит предыдущую конфигурацию.
3. Если результат настройки системы вас устраивает, вы можете отменить перезагрузку с помощью команды `no reboot`. Текущий статус таймера перезагрузки можно просмотреть с помощью команды `show reboot`.

Для устаревших моделей, поддерживающих только протоколы 802.11a/b/g:

Не применяйте отложенную перезагрузку, если вы меняете частотную сетку (см. Смена текущего countrycode), но при этом не уверены в правильности выбранного значения, поскольку сохранение нового значения происходит немедленно после смены countrycode!

`reboot [seconds]`

Описание. Немедленная или отложенная перезагрузка системы.

Префикс NO. Отмена перезагрузки.

Аргументы.

seconds

Необязательный временной интервал в секундах, после которого произойдет перезагрузка системы.

Пример 114. Отложенная перезагрузка системы

```
RAPIRA: reboot 60
Rebooting after 60 second(s).

RAPIRA: no reboot
Reboot timer stopped.
```

`show reboot`

Описание. Просмотр статуса таймера перезагрузки.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 115. Отложенная перезагрузка и просмотр статуса таймера перезагрузки

```
RAPIRA: reboot 100
Rebooting after 100 second(s).
RAPIRA: show reboot
Reboot after 97 second(s).
RAPIRA: no reboot
Reboot timer stopped.
RAPIRA: show reboot
Reboot timer disabled.
```

см. также Удаленная перезагрузка маршрутизатора

Настройка даты и времени

Установка даты и времени вручную

Дату и время можно установить либо автоматически, используя NTP, либо вручную, используя следующую команду:

```
system date {hours:minutes:seconds} [day [month [year]]]
```

Описание. Установка системной даты и времени.

Префикс NO. Не используется.

Аргументы.

hours

Часы, возможные значения от 0 до 23

minutes

Минуты, возможные значения от 0 до 59

seconds

Секунды, возможные значения от 0 до 59

day

День месяца. Если аргумент опущен, то параметры остаются прежними.

month

Аббревиатура соответствующего месяца: **an**, **feb**, **mar**, **apr**, **may**, **un**, **ul**, **aug**, **sep**, **oct**, **nov** или **dec**. Если аргумент опущен, то устанавливается текущий месяц.

year

Год, возможные значения от 1970 до 2068. Если аргумент опущен, то устанавливается текущий год.

Для просмотра текущих даты и времени используется команда `show date`.

Пример 116. Настройка системной даты и времени

```
RAPIRA: system date 10:26:00 5 mar
Date and time adjusted.

RAPIRA: show date
Mon Mar 5 10:26:00 2007
```

NTP

Синхронизирующий сетевой протокол (Network Time Protocol, NTP) – это протокол,

используемый для синхронизации часов системы через Интернет. Для синхронизации времени система RAPIRA RS3 использует сервис NTP.

Параметры сервиса:

- Список адресов NTP-серверов
- Таймаут: период ожидания ответа от сервера NTP прежде, чем будет принято решение о его недоступности
- Период синхронизации: временной интервал между двумя успешными синхронизациями
- Часовой пояс: разница во времени относительно UTC (Coordinated Universal Time)
- Количество попыток соединения: максимальное количество попыток соединения с NTP-сервером
- Интервал между попытками: временной интервал между попытками соединения с NTP-сервером

По умолчанию установлены следующие настройки сервиса NTP:

- Таймаут: 5 секунд
- Период синхронизации: 4*7*24*60*60 секунд
- Часовой пояс: 0
- Количество попыток соединения: 3
- Интервал между попытками: 5 секунд

Если значения, установленные по умолчанию изменены, то они появляются в **running-config**. Секцию NTP можно просмотреть с помощью команды `show running-config`, используя для удобства какой-либо поисковый ключ, например - `show running-config ntp`.

Пример 117. Настройка NTP

```
RAPIRA: ntp server ntp.ufes.br
Server 'ntp.ufes.br' has been added.

RAPIRA: no ntp server ntp.ufes.br
Server 'ntp.ufes.br' has been removed.

RAPIRA: ntp server europe.pool.ntp.org
Server 'europe.pool.ntp.org ' has been added.

RAPIRA: ntp server ntp.karpo.cz
Server 'ntp.karpo.cz' has been added.

RAPIRA: ntp retry-period 15
NTP retry period is set to 15 second(s).

RAPIRA: ntp timezone-offset 180
NTP local timezone offset is set to 180 minute(s).
```

```
RAPIRA:  ntp sync-period 86400
NTP synchronization period is set to 86400 second(s).

RAPIRA: service ntp
NTP client has been started.

RAPIRA: show running-config ntp
ntp retry-period 15
sync-period 86400
timezone-offset 180
server europe.pool.ntp.org
server ntp.karpo.cz
```

Список команд

service ntp

Описание: Запуск NTP-клиента

Префикс NO: Останов клиента.

Аргументы: Аргументы отсутствуют.

Пример 118. Запуск NTP-клиента

```
RAPIRA: service ntp
NTP client successfully started.

RAPIRA: no service ntp
NTP client successfully stopped.
```

ntp server

Описание: Добавление NTP-сервера в список серверов.

Префикс **NO**:Удаление выбранного NTP-сервера из списка.

Аргументы:

- Доменное имя или IP-адрес NTP-сервера.

Пример 119. Добавление NTP-сервера

```
RAPIRA: ntp server ntp.ufes.br
Server 'ntp.ufes.br' successfully added.

RAPIRA: no ntp server ntp.ufes.br
Server 'ntp.ufes.br' successfully removed.
```

Максимальное количество NTP серверов – **8**. Если NTP-сервер не указан, то сервис использует список серверов по умолчанию.

ntp retries

Описание: Максимальное количество попыток соединения с каждым NTP-сервером.

Префикс **NO**: Возврат к установкам по умолчанию.

Аргументы:

- Количество попыток соединения. Диапазон от **1** до **10**. Значение по умолчанию: **3**.

Пример 120. Настройка количества попыток соединения с каждым NTP-сервером

```
RAPIRA: ntp retries 5
NTP retry count is set to 5.
```

ntp retry-period

Описание: Установка временного интервала между неудачными попытками соединения.

Префикс **NO**: Возврат к установкам по умолчанию.

Аргументы:

- Интервал в секундах, целое число. Диапазон от **5** до **3600**. Значение по умолчанию: **5**.

Пример 121. Установка временного интервала между неудачными попытками соединения

```
RAPIRA: ntp retry-period 10
NTP retry period is set to 10 second(s).
```

ntp sync-period

Описание: Установка временного интервала между успешными синхронизациями времени.

Префикс **NO**: Возврат к установкам по умолчанию.

Аргументы:

- Временной интервал в секундах между синхронизациями, целое число. Диапазон от **60** до **(28 * 24 * 60 * 60)**. По умолчанию установлено значение, равное примерно 1 месяцу: **(28 * 24 * 60 * 60)**.

Пример 122. Установка временного интервала между успешными синхронизациями времени

```
RAPIRA: ntp sync-period 3600
NTP synchronization period is set to 3600 second(s).
```

ntp timeout

Описание: Установка тайм-аута соединения с NTP-сервером.

Префикс **NO**: Возврат к установкам по умолчанию.

Аргументы:

- Значение тайм-аута в секундах, целое число. Диапазон: от **1** до **60**. Значение по умолчанию: **5**.

Пример 123. Установка тайм-аута соединения с NTP-сервером.

```
RAPIRA: ntp timeout 15
NTP timeout is set to 15 second(s).
```

ntp timezone-offset

Описание: Установка часового пояса - разница во времени относительно UTC (Coordinated Universal Time).

Префикс **NO**: Возврат к установкам по умолчанию.

Аргументы: * Сдвиг в минутах, целое число. Диапазон: от **-780** до +**780**. Значение по умолчанию: **0**.

Пример 124. Установка часового пояса

```
RAPIRA: ntp timezone-offset +240
NTP region timezone offset is set to +240 minute(s).
```

Смена пароля доступа в систему

Для смены установленного пароля используется команда `system password`. Команда требует два обязательных аргумента:

```
system password {old-password} {new-password}
```

Описание. Смена пароля.

Префикс NO. Не используется

Аргументы.

old-password

Старый пароль.

new-password

Новый пароль.

Пример 125. Смена пароля

```
RAPIRA: system password 123 fgHg#4552
Password changed.
```

В случае утери пароля в консоли операционной системы запустите утилиту Power_soft_reset, расположенную на прилагаемом компакт-диске, с параметром **scan**.

Напишите в службу службой технической поддержки нашей компании и сообщите результат выполнения указанной команды. Необходимая информация для восстановления утраченного пароля будет выслана в ответном письме.

см. также Сброс параметров маршрутизатора в стандартные значения

см. также Получение IP-адреса маршрутизатора

Мониторинг и статистика

Подключение к удаленному маршрутизатору

Подключение выполняется с помощью следующей команды:

```
utilities ssh {admin@ip_address}
```

Описание. Команда позволяет подключиться к удаленному маршрутизатору из текущей консоли. Для завершения сеанса введите команду **exit**.

Префикс NO. Не используется.

Аргументы.

ip_address

IP-адрес хоста.

Пример 126. Подключение к удаленному маршрутизатору

```
RAPIRA: utilities ssh admin@192.168.0.130
```

Тест Host Echo

Тест выполняется с помощью следующей команды:

```
utilities ping {host}
```

Описание. Команда начинает пинговку данного хоста. Чтобы остановить процесс, следует нажать `Enter`.

Префикс NO. Не используется.

Аргументы.

host

IP-адрес или имя хоста.

Пример 127. Пинговка указанного хоста

```
RAPIRA: utilities ping google.com
PING google.com (64.233.187.99) 56(84) bytes of data.
64 bytes from jc-in-f99.google.com (64.233.187.99): icmp_seq=1 ttl=242 time=148 ms
64 bytes from jc-in-f99.google.com (64.233.187.99): icmp_seq=2 ttl=242 time=142 ms
64 bytes from jc-in-f99.google.com (64.233.187.99): icmp_seq=3 ttl=242 time=141 ms
```

Анализ сетевого трафика

RAPIRA RS3 дает возможность пользователю просматривать содержание сетевых пакетов, проходящих через систему. Принимая во внимание высокую интенсивность трафика, целесообразно уменьшать поток информации с помощью фильтров. Для анализа сетевых пакетов используется команда `utilities tcpdump`, имеющая следующий синтаксис:

```
utilities tcpdump [{iface-name} {iface-number}] [proto] [{node} | src {node} | src {node} dst {node} | dst {node}] [syslog]
```

Аргументы.

iface-name iface-number

Название и номер интерфейса.

proto

Один из возможных протоколов: **tcp**, **udp**, **icmp** и **ip**, где **ip** – это анализ всех трех протоколов **tcp**,**udp**, и **icmp**.

node

Адрес источника и/или получателя, где указывается IP-адрес или имя хоста с возможным указанием порта или диапазона портов: `{ip-address | host-name} [{port} | {port} {port}]`, где адрес указывается в виде:

- **src {node}** - указание только адреса источника.
- **src {src-node} dst {dst-node}** - указание и адреса источника, и адреса получателя.
- **dst {node}** - указание только адреса получателя.

syslog

Ключевое слово, с помощью которого можно отправлять все собранные пакеты на удалённый syslog service.

Например, необходимо собрать TCP пакеты на интерфейсе **Wireless 0**, адрес источника 192.168.0.1, диапазон портов [0—1023], адрес получателя 10.0.0.1, диапазон портов [1024—65535] и отправить содержимое всех собранных пакетов на удаленный syslog:

Пример 128. Использование tcpdump

```
RAPIRA: utilities tcpdump wireless 0 tcp src 192.168.0.1 0 1023 dst 10.0.0.1 1024
65535 syslog
    Logging to syslog...
```

Система будет собирать пакеты, пока не будет нажата клавиша `Enter`.

Трассировка маршрута

Для трассировки IP-маршрутов используется следующая команда:

```
utilities traceroute {host}
```

Описание. Команда начинает трассировку и заканчивает процесс, когда весь маршрут пройден. Процесс можно остановить, нажав клавишу `Enter`.

Префикс NO. Не используется.

Аргументы.

host

IP-адрес хоста.

Пример 1. Трассировка маршрута

```
RAPIRA: utilities traceroute google.com
1  tp-noc.ru (183.16.21.1)  1.652 ms  1.095 ms  1.326 ms
2  cs-main.ru (183.16.96.41)  2.204 ms  1.454 ms  1.495 ms
3  msk-m9-b1-ge1-3-0-vlan2.fiord.ru (62.140.239.25)  3.716 ms  2.868 ms  3.539 ms
4  mow-b2-link.telia.net (213.248.97.237)  3.875 ms  3.768 ms  3.076 ms
5  s-bb2-link.telia.net (80.91.249.98)  27.668 ms  28.077 ms  27.602 ms
6  kbn-bb2-link.telia.net (213.248.65.166)  38.792 ms  37.341 ms  38.076 ms
```

Ведение журнала

RAPIRA RS3 поддерживает функцию ведения журнала на удаленном хосте. Для запуска или останова (при использовании префикса **no**) сервиса ведения журнала используется следующая команда:

```
service syslog {ip-address} [port]
```

Описание. Запуск сервиса, отправляющего записи журнала на указанный хост.

Префикс NO. Останов сервиса.

Аргументы.

ip-address

IP-адрес хоста.

port

Номер UDP-порта удаленного syslog-сервиса, значение по умолчанию равно **512**.

Пример 1. Ведение журнала на удаленном хосте

```
RAPIRA: service syslog 192.168.0.9
Syslog has started using the remote log server 192.168.0.9:514.
RAPIRA: no service syslog
Syslog has stopped.
```

Информация о системе - список команд ветви SHOW

Система RAPIRA RS3 предусматривает несколько команд для просмотра текущего состояния системы. Все команды сгруппированы в командной ветви `show`.

Список команд ветви SHOW

access-list

Описание: см. access-list

bridge-group

Описание: помещение указанного интерфейса в группу прозрачного моста, подробнее см. в разделе Создание прозрачного моста.

certificates

Описание. Просмотр содержимого репозитария сертификатов. Каждая запись может содержать сертификат или секретный ключ. Оба могут быть зашифрованы.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 129. Просмотр содержимого репозитария сертификатов

```
RAPIRA: show certificates
Name            Certificate  Encrypted     Key  Encrypted
ivanov.crt      Yes          Off           No   N/A
ivanov.key      No           N/A           Yes  On
ivanov.pem      Yes          Off           Yes  On
```

cpu

Описание: просмотр среднего уровня загрузки центрального процессора (CPU).

Аргументы: Аргументы отсутствуют.

Пример 130. Просмотр уровня загрузки центрального процессора

```
RAPIRA: show cpu
```

date

Описание: Просмотр системной даты и времени.

Аргументы: Аргументы отсутствуют.

Пример 131. Просмотр системной даты и времени

```
RAPIRA: show date
```

INTERFACE (подветвь)

`show interface {name} {index} {команда}`

Описание: Просмотр детальной информации о параметрах интерфейса.

Аргументы:

name
Имя интерфейса.

index
Номер интерфейса.

Команды подветви Interface

- access-group
- associated
- channel-list
- mac-access-list
- nat-group
- polling-rules
- polling-tolerance
- scan
- signal
- statistics
- tx-power-range
- wds-table
- wireless-statistics

access-group

Описание: Просмотр access-group, в которую входит указанный интерфейс

см. также Связывание списка доступа

см. также access-list

Аргументы: Аргументы отсутствуют.

Пример 132. Просмотр access-group

```
RAPIRA: show interface wireless 0 access-group
```

associated

`associated [watch]`

Описание: Отображение клиентских станций, ассоциированных с базовой станцией.

Команда доступна только для радиомаршрутизаторов типа «базовая станция».

см. также Настройка типа оборудования

см. также команду signal

см. также команду show interfaces

Аргументы:

watch

позволяет просматривать характеристики ассоциации в реальном времени. Для прекращения выполнения команды нажмите `Enter`.

Пример 133. Отображение клиентских станций, ассоциированных с базовой станцией

```
RAPIRA: show interface wireless 0 associated watch
```

channel-list

Описание: Просмотр списка доступных частот. Если необходимая частота отсутствует в списке - воспользуйтесь командой system countrycode.

см. также Отображение текущего countrycode

Аргументы: Аргументы отсутствуют.

Пример 134. Просмотр списка доступных частот

```
RAPIRA: show interface wireless 0 channel-list
```

mac-access-list

Описание: Просмотр содержимого списка управления доступом.

см. также Фильтрация на основе MAC-адреса

Аргументы: Аргументы отсутствуют.

Пример 135. Просмотр содержимого списка управления доступом

```
RAPIRA: show interface wireless 0 mac-access-list
```

nat-group

Описание: Просмотр списка NAT, присоединенного к указанному интерфейсу.

см. также NAT

Аргументы: Аргументы отсутствуют.

Пример 136. Просмотр списка NAT

```
RAPIRA: show interface wireless 0 nat-group
```

polling-rules

Описание: Просмотр правил поллинга.

Аргументы: Аргументы отсутствуют.

Пример 137. Просмотр правил поллинга

```
RAPIRA: show interface wireless 0 polling-rules
```

polling-tolerance

Описание: Просмотр значения времени, в течение которого базовая станция не будет пытаться опросить станции, не передающие данных.

Аргументы: Аргументы отсутствуют.

Пример 138. Просмотр значения времени, в течение которого базовая станция не будет пытаться опросить неактивные станции

```
RAPIRA: show interface wireless 0 polling-tolerance
```

scan

`scan [freq частота]`

Описание: Сканирование всех частотных диапазонов и отображение информации об обнаруженных базовых станциях.

Команда доступна только для радиомаршрутизаторов типа «клиентская станция».

см. также Настройка типа оборудования

Аргументы:

freq

аргумент используется только в MIMO-устройствах и позволяет сканировать только указанную частоту, что значительно сокращает время сканирования, особенно при работе в расширенном списке частот.

Пример 139. Сканирование всех доступных частотных диапазонов

```
RAPIRA: show interface wireless 0 scan
```

Пример 140. Сканирование частоты 5800 МГц

```
RAPIRA: show interface wireless 0 scan freq 5800
```

signal

`signal [watch]`

Описание: Отображение характеристик принимаемого сигнала.

Команда доступна только для радиомаршрутизаторов типа «клиентская станция».

см. также Настройка типа оборудования

см. также команду associated

см. также команду show interfaces

Аргументы:

watch

позволяет просматривать характеристики принимаемого сигнала в реальном времени. Для прекращения выполнения команды нажмите `Enter`.

Пример 141. Отображение характеристик принимаемого сигнала

```
RAPIRA: show interface wireless 0 signal watch
```

см. также beeper

statistics

`statistics`

Описание: Просмотр статистики указанного интерфейса.

Аргументы:

watch

позволяет просматривать характеристики принимаемого сигнала в реальном времени. Для прекращения выполнения команды нажмите `Enter`.

Пример 142. Просмотр статистики указанного интерфейса в реальном времени

```
RAPIRA: show interface wireless 0 statistics watch
```

tx-power-range

`tx-power-range`

Описание: Просмотр допустимых значений мощности радиоинтерфейса (дБм).

Аргументы: Аргументы отсутствуют.

Пример 143. Просмотр допустимых значений мощности радиоинтерфейса

```
RAPIRA: show interface wireless 0 tx-power-range
```

wds-table

`wds-table`

Описание: Просмотр содержимого таблицы WDS.

Аргументы: Аргументы отсутствуют.

Пример 144. Просмотр содержимого WDS-таблицы

```
RAPIRA: show interface wireless 0 wds-table
```

wireless-statistics

`wireless-statistics`

Описание: Просмотр подробной статистики беспроводного интерфейса.

Аргументы:

watch

позволяет просматривать характеристики принимаемого сигнала в реальном времени. Для прекращения выполнения команды нажмите `Enter`.

Пример 145. Просмотр подробной статистики беспроводного интерфейса в реальном времени

```
RAPIRA: show interface wireless 0 wireless-statistics watch
```

interfaces

Описание: Просмотр детальной информации о доступных сетевых интерфейсах.

Аргументы:

Имя интерфейса (выборочно)

watch (выборочно)

Позволяет отслеживать изменение параметров в реальном времени. Чаще всего применяется при просмотре интерфейсов на клиентской станции, позволяя оперативно отслеживать наличие ассоциации с базовой станцией, текущую скорость соединения, используемую частоту (если частота на клиенте установлена как **auto**). Для прекращения выполнения команды нажмите `Enter`.

Пример 146. Просмотр детальной информации о доступных сетевых интерфейсах

```
RAPIRA: show interfaces

        Bridge 0 is up, link state is up
           Hardware address:  0015.6d6b.bc6e
           Internet address:  10.17.2.3 mask 255.255.255.0
            broadcast:  10.17.2.255, MTU: 1500

        FastEthernet 0 is up, link state is up
           Hardware address:  d4ca.6d7e.28fa  VLAN: none
           Internet address:  0.0.0.0 mask 0.0.0.0
            broadcast:  0.0.0.0, MTU: 1500

        Wireless 0 is up, link state is up
           Hardware address:  0015.6d6b.bc6e  VLAN: none
           Internet address:  0.0.0.0 mask 0.0.0.0
            broadcast:  0.0.0.0, MTU: 1500
           Type: station, SSID: "rs3", Mode: 802.11a
           Speed: 54 Mb/s (auto), Access point: 0015.6d6b.bc54
           Channel: 180, Frequency: 5900 MHz, Tx-power: 25 dBm
           RTS: off, Distance: 900, WDS: on, FastFrame: on
           Burst: on, Compression: off, WMM: off, Beacon: 100, DFS: off
           Antenna: auto, ATPC: off
```

см. также команду associated

см. также команду signal

IP (подветвь)

Команды подветви IP

- arptable
- domain-name
- hostname
- hosts
- name-server
- route

arptable

```
ip arptable {arp|size}
```

Описание: Просмотр содержимого или размера таблицы ARP.

см. также Таблица ARP

Аргументы:

arp
Содержимое таблицы ARP.

size
Размер таблицы ARP.

Пример:

```
RAPIRA: show  ip arptable arp
```

domain-name

Описание: Отображение имени локального домена.

см. также Имя домена

Аргументы: Аргументы отсутствуют.

Пример:

```
RAPIRA: show ip domain-name
```

hostname

Описание: Отображение имени локального хоста.

см. также Имя хоста

Аргументы: Аргументы отсутствуют.

Пример:

```
RAPIRA: show ip hostname
```

hosts

Описание: Просмотр таблицы статических хостов.

см. Статические хосты

Аргументы: Аргументы отсутствуют.

Пример:

```
RAPIRA: show ip hosts
```

name-server

Описание: Просмотр ip-адреса сервера имен.

см. Просмотр списка имен

см. также DNS

route

Описание:

см. Просмотр таблицы маршрутизации.

см. также Статическая маршрутизация и шлюз по умолчанию

nat-list

Описание: просмотр одержимого списка NAT.

см. также NAT

Аргументы: Аргументы отсутствуют.

Пример 147. Просмотр детальной информации о доступных сетевых интерфейсах

```
RAPIRA: show nat-list
```

polling-rules

Описание: Просмотр правил поллинга.

Команда может быть выполнена только на базовой станции.

Обратите внимание:

Перед выполнением команды поллинг должен быть включён, в противном случае будет выдано сообщение: "Polling not operational."

Аргументы: Аргументы отсутствуют.

Пример 148. Просмотр правил поллинга

```
RAPIRA: show interface Wireless 0 polling-rules
```

см. также polling

см. также Настройка поллинга

polling-tolerance

Описание: Просмотр времени, в течение которого базовая станция не будет пытаться опросить станции, не передающие данных.

Команда может быть выполнена только на базовой станции.

Обратите внимание:

Перед выполнением команды поллинг должен быть включён, в противном случае будет выдано сообщение: "Polling not operational."

Аргументы: Аргументы отсутствуют.

Пример 149. Просмотр времени, в течение которого базовая станция не будет пытаться опросить станции, не передающие данных.

```
RAPIRA: show interface Wireless 0 polling-tolerance
```

см. также polling

см. также Настройка поллинга

reboot

Описание: просмотр статуса перезагрузки.

см. также Перезагрузка системы

Аргументы: Аргументы отсутствуют.

Пример 150. Просмотр статуса перезагрузки

```
RAPIRA: show reboot
```

running-config

Описание: просмотр исполняемой конфигурации.

см. также Настройка маршрутизатора RAPIRA RS3

Аргументы: Аргументы отсутствуют.

Пример 151. Просмотр исполняемой конфигурации

```
RAPIRA: show running-config
```

services

Описание: просмотр статуса сервисов.

Аргументы: Аргументы отсутствуют.

Пример 152. Просмотр статуса сервисов

```
RAPIRA: show services
```

см. также Режим WPA EAP (IEEE 802.1X)

см. также WPA

см. также DHCP

см. также beeper

см. также DNS

см. также NTP

см. также Настройка SNMP

startup-config

Описание: просмотр пусковой конфигурации.

см. также Настройка маршрутизатора RAPIRA RS3

Аргументы: Аргументы отсутствуют.

Пример 153. Просмотр пусковой конфигурации

```
RAPIRA: show startup-config
```

SYSTEM (подветвь)

Команды подветви System

countrycode

Описание: Отображение текущего countrycode.

Аргументы: Аргументы отсутствуют.

Пример:

```
RAPIRA: show system countrycode
```

см. также Смена текущего countrycode

см. также Просмотр списка доступных частот

uptime

Описание: Просмотр времени работы системы с момента последнего включения маршрутизатора.

Аргументы: Аргументы отсутствуют.

Пример 154. Просмотр времени работы системы

```
RAPIRA: show uptime
```

version

Описание: Просмотр версии установленного программного обеспечения.

Аргументы: Аргументы отсутствуют.

Пример 155. Просмотр версии установленного программного обеспечения

```
RAPIRA: show version
```

xml-running-config

Описание: Просмотр исполняемой конфигурации в формате XML.

см. также Формат файла конфигурации

Аргументы: Аргументы отсутствуют.

Пример 156. Просмотр исполняемой конфигурации в формате XML

```
RAPIRA: show xml-running-config
```

Настройка интерфейсов

В командной ветви Interface сгруппированы все команды, управляющие настройками входящих в радиомаршрутизатор интерфейсов, такими как:

- запуск и остановка интерфейса
- установка и изменение MTU интерфейсов
- задание скорости передачи данных для интерфейса
- изменение MAC адреса интерфейса
- настройка IP протокола для интерфейса
- настройка уникальных параметров беспроводных интерфейсов
- настройка уникальных параметров проводных интерфейсов
- применение списков доступа на интерфейсе

Параметры ветви Interface

```
interface {name} {index}
```

Параметры:

name

Имя интерфейса. Возможные значения:

wireless

настройка беспроводного интерфейса

ethernet

настройка проводного интерфейса

bridge

создание/настройка интерфейса прозрачного моста. Подробнее о работе с данным интерфейсом см. в разделе Создание прозрачного моста.

index

Номер интерфейса.

Список команд ветви INTERFACE

access-group

Описание: см. Связывание списка доступа

см. также access-list

allmulticast

Описание: Включение режима многоадресной рассылки (мультикаст). По умолчанию данная опция **выключена**. Для работы в данном режиме необходимо разрешить мультикасты на беспроводном интерфейсе клиентского маршрутизатора.

Префикс NO. Выключение режима многоадресной рассылки.

Аргументы: Аргументы отсутствуют.

Пример 157. Включение режима многоадресной рассылки

```
RAPIRA: interface  Wireless 0 allmulticast
```

antenna

`antenna {a|b|auto}`

Описание: Определение антенного выхода радиокарты, который будет использован. Команда актуальна ТОЛЬКО для устройств с поддержкой протоколов 802.11a/b/g и не актуальна для устройств с поддержкой протокола 802.11n (MIMO). Рекомендуется использовать параметр **auto**.

Пример 158. Определение антенного выхода радиокарты

```
RAPIRA: interface  Wireless 0 antenna auto
```

AUTHENTIFICATION (подветвь)

ca-cert

Описание: см. Установка CA-сертификата

см. также Настройка WPA

client-cert

Описание: см. Установка сертификата клиента для аутентификации EAP-TLS

см. также Настройка WPA

identity

Описание: см. Установка аутентичности клиента

см. также Настройка WPA

wpa-eap

Описание: см. Включение режима WPA EAP

см. также Настройка WPA

md5

Описание: см. Включение режима EAP-MD5

см. также Настройка WPA

mschap-v2

Описание: см. Включение режима EAP-MSCHAPv2

см. также Настройка WPA

password

Описание: см. Установка пароля для различных режимов аутентификации

см. также Настройка WPA

peap

Описание: см. Включение PEAP

см. также Настройка WPA

private-key

Описание: см. Установка секретного ключа клиента

см. также Настройка WPA

radius-profile

Описание: см. Установка профиля RADIUS для аутентификации WPA EAP

см. также Настройка WPA

см. также EAP

tls

Описание: см. Включение EAP-TLS

см. также Настройка WPA

см. также EAP

ttls

Описание: см. Включение EAP-TTLS

см. также Настройка WPA

см. также EAP

wpa-psk

Описание: см. Включение WPA-PSK

см. также Настройка WPA

beacon

```
beacon {milliseconds} [hide]
```

Описание: Установка интервала рассылки широковещательного идентификатора сети. Рассылка осуществляется базовой станцией для синхронизации работы беспроводной сети. Интервал исчисляется в миллисекундах, допустимые значения: от 25 до 20000 мс. Стандартное значение - 100 мс.

Не меняйте этот параметр без явной необходимости!

Префикс NO. отключение рассылки широковещательного идентификатора сети.

Аргументы:

milliseconds

Указание временного интервала.

hide

Продолжение рассылки с нулевым значением поля SSID, т.о. радиомаршрутизатор переходит в режим HIDE SSID. Для отключения данного режима требуется вызвать команду **beacon** с указанием временного интервала и БЕЗ указания ключевого слова **hide**.

Пример 159. Настройка beacon

```
RAPIRA:  interface  Wireless 0 beacon 100
```

beeper

Описание: включение звукового сигнала. Данная команда применяется при юстировке антенны. Интервалы звучания сигнала обратно пропорциональны уровню приёмного сигнала.

Префикс NO. отключение звукового сигнала.

Аргументы: Аргументы отсутствуют.

Пример 160. Включение звукового сигнала

```
RAPIRA: interface  Wireless 0 beeper
```

см. также signal

bridge-group

Описание: помещение указанного интерфейса в группу прозрачного моста, подробнее см. в разделе Создание прозрачного моста.

burst

Описание: включение режима отправки большего количества кадров за тот же фиксированный временной интервал.

Обратите внимание:

Команда актуальна ТОЛЬКО для устройств с поддержкой протоколов 802.11a/b/g и не доступна для устройств с поддержкой протокола 802.11n (MIMO).

Префикс NO. отключение режима отправки большего количества кадров за тот же фиксированный временной интервал.

Аргументы: Аргументы отсутствуют.

Пример 161. Настойка burst

```
RAPIRA: interface  Wireless 0 burst
```

channel

Описание. Настройка канала несущей частоты.

Префикс NO. Не используется.

Аргументы.

frequency

Указывает значение несущей частоты в мегагерцах. Ключевое слово **auto** применимо исключительно к клиентскому устройству. Если канал станции указан как **auto**, то сканируются все поддерживаемые каналы для данного SSID.

Важно:

Если вы определите конкретную частоту для оборудования, работающего в режиме «клиентская станция», то станция будет опрашивать только эту частоту.

Обратите внимание:

Для режима «базовая станция» нельзя использовать значение **auto**.

Пример 162. Настройка канала несущей частоты

```
RAPIRA: interface Wireless 0 channel 5805
Channel is set to '5805'.
```

см. также Просмотр списка доступных частот.

см. также Смена countrycode

clientbridge

Описание. Включение режима прохождения трафика между клиентскими маршрутизаторами при использовании конфигурации "точка-многоточек". По умолчанию данный режим выключен.

Префикс NO. Запрет прохождения трафика между клиентскими маршрутизаторами.

Аргументы: Аргументы отсутствуют.

Пример 163. Включение режима запрета прохождения трафика между клиентскими маршрутизаторами при использовании конфигурации "точка-многоточек".

```
RAPIRA: interface Wireless 0  no clientbridge
```

dfs

Описание. Включение режима автоматического выбора оптимальной частоты (Dynamic Frequency Selection). Режим может быть использован только на базовой станции, при этом параметр **channel** на всех маршрутизаторах должен быть установлен в **auto**.

Префикс NO. Отключение режима автоматического выбора оптимальной частоты.

Аргументы: Аргументы отсутствуют.

Пример 164. Включение режима автоматического выбора оптимальной частоты

```
RAPIRA: interface Wireless 0 dfs
```

см. также channel

distance

Описание. Установка дистанции между маршрутизаторами.

Префикс NO. Не используется.

Аргументы.

distance

Дистанция измеряется в метрах, значение должно быть кратно 300. Приемлемый диапазон от 0 до 100200 метров.

Пример 165. Установка дистанции между маршрутизаторами в 3 км.

```
RAPIRA: interface Wireless 0 distance 3000
A distance value is set to '3000'.
```

см. также Настройка параметра расстояния

ENCRYPTION (подветвь)

ccmp

Описание: см. Включение шифрования CCMP (WPA2)

см. также IEEE 802.11i WPA2

key

Описание: см. Установка или выбор существующего ключа WEP

см. также WEP

см. также Настройка Wired Equivalent Privacy (WEP)

tkip

Описание: см. Включение шифрования TKIP (WPA)

см. также Настройка WPA

wep

Описание: см. Включение шифрования WEP

см. также WEP

см. также Настройка Wired Equivalent Privacy (WEP)

fast-frame

Описание: включение режима объединения кадров.

Обратите внимание:

Команда актуальна ТОЛЬКО для устройств с поддержкой протоколов 802.11a/b/g и не актуальна для устройств с поддержкой протокола 802.11n (MIMO).

Префикс NO. отключение режима объединения кадров.

Аргументы: Аргументы отсутствуют.

Пример 166. Настройка fast-frame

```
RAPIRA: interface  Wireless 0 fast-frame
```

IP (подветвь)

см. Параметры интерфейса

kick-mac

Описание: см. Отсоединение клиентской станции от базовой

см. также Фильтрация на основе MAC-адреса

mac-access-list

Описание: см. в разделе Фильтрация на основе MAC-адреса

macnat-mode

Описание. Включение режима совместимости со стандартным Wi-Fi - оборудованием. Трансляция 4-х адресной схемы mac-адресов в 3-х адресную. При включении данного режима флаг WDS не используется и снимается автоматически.

Префикс NO. Отключение режима совместимости со стандартным Wi-Fi - оборудованием.

Аргументы: Аргументы отсутствуют.

Пример 167. Включение режима совместимости со стандартным Wi-Fi оборудованием

```
RAPIRA: interface Wireless 0  macnat-mode
```

см. также wds-mode

mode

Описание команды mode для устройств с поддержкой протокола MIMO (802.11a/b/g/n).

Команда указывает ширину полосы пропускания и может быть представлена в одном из вариантов: noht, ht20, ht40- или ht40+. В режиме noht используется протокол 802.11a или 802.11g - в зависимости от используемого частотного диапазона.

Префикс NO. Не используется.

Аргументы.

mode

Режим: один из `noht`, `ht20`, `ht40-` или `ht40+` (рекомендуется).

Пример 168. Установка режима ht40+

```
RAPIRA: interface Wireless 0 mode ht40+
The mode is set to 'ht40+'.
```

Описание для устройств с поддержкой протоколов 802.11a/b/g.

Команда указывает режим IEEE 802.11, который может быть представлен в одном из вариантов: 802.11a, 802.11b или 802.11g.

Префикс NO. Не используется.

Аргументы.

mode

Режим: один из a, b, g или auto (рекомендуется). Если режим установлен в `auto`, то драйвер маршрутизатора автоматически вычисляет оптимальный режим для данной частоты и скорости передачи данных.

Пример 169. Установка режима auto

```
RAPIRA: interface Wireless 0 mode auto
The mode is set to 'auto'.
```

nat-group

Описание: см. NAT

polling

Описание: Включение режима поллинга. Комманда должна быть выполнена на базовой и на клиентских станциях.

Префикс NO. Выключение режима поллинга.

Аргументы: Аргументы отсутствуют.

Пример 170. Включение режима поллинга

```
RAPIRA: interface  Wireless 0 polling
```

см. также polling-rules

см. также Настройка поллинга

polling-stations-max

`polling-stations-max {number of stations}`

Описание. Указание максимального количества абонентов, которые будут обслуживаться базовой станцией. Команда может быть выполнена только на базовой станции.

Префикс NO. Не используется.

Аргументы.

number of stations

Максимально допустимое число подключаемых клиентов.

Пример 171. Указание максимального количества абонентов

```
RAPIRA: interface  Wireless 0 polling-max-station 25
```

см. также polling-percentage

см. также polling-tolerance-max

см. также Настройка поллинга

polling-max-rate

`polling-max-rate {MAC-адрес} {ЗНАЧЕНИЕ}`

Описание. Установка максимальной скорости передачи в прямом (от базы к клиенту) и в обратном (от клиента к базе) направлениях. Команда может быть выполнена только на базовой станции.

Префикс NO. Не используется.

Аргументы.

MAC-адрес

MAC-адрес беспроводного интерфейса клиентской станции.

ЗНАЧЕНИЕ

составное значение скорости для прямого и обратного направления в виде : ЗНАЧЕНИЕ_ПР/ЗНАЧЕНИЕ_ОБР. Скорость может указываться как битах, так и в сокращенной нотации с помощью суффиксов "M" - мегабит и "K" - килобит (суффиксы не чувствительны к регистру).

Пример 172. Установка максимально допустимой скорости передачи в прямом и в обратном направлениях

```
RAPIRA: interface wireless 0 polling-max-rate 00:15:6d:54:31:0f 16M/6M
```

Если ЗНАЧЕНИЕ_ПР или ЗНАЧЕНИЕ_ОБР равно "0", то скорость в данном направлении контролироваться не будет (если нет правила по умолчанию - см. ниже). Таким образом, если необходимо отказаться от одного из ранее введенных параметров нужно просто еще раз вызвать данную команду со значением равным 0, при этом, если поставить равным "0" оба параметра (0/0), то правило удалится так же, как при использовании команды polling-delete.

Если в качетсве MAC-адреса будет указан широковещательный адрес: FF:FF:FF:FF:FF:FF - то данное правило будет являтся правилом по умолчанию и будет использоваться для всех клиентов, у которых не заданы данные параметры.

Пример 173. Установка правила по умолчанию

```
RAPIRA: interface wireless 0 polling-max-rate FF:FF:FF:FF:FF:FF 1M/0
```

Таким образом, для всех клиентов, у которых отсутствует правило на ограничение скорости в прямом направлении (ЗНАЧЕНИЕ_ПР), скорость будет ограничена значением 1M. На скорость в обратном направлении конкретно данная команда не повлияет.

см. также polling-min-rate

см. также Настройка поллинга

polling-min-rate

`polling-min-rate {MAC-адрес} {ЗНАЧЕНИЕ}`

Описание. Установка минимальной скорости передачи в прямом (от базы к клиенту) и в обратном (от клиента базе) направлениях. Команда может быть выполнена только на базовой станции.

Система пытается не допустить снижения скорости ниже заданной (при наличии ресурса, разумеется). При недостатке ресурса скорость распределяется пропорционально заданному значению, например, если реальная скорость передачи составляет 10 мбит/с, но при этом в правилах одному клиенту гарантировали 20 мбит/с, а другому 10 мбит/с, то итоговая скорость у каждого клиента будет соответственно 6.66 Мбит/с и 3.33 мбит/с. Если же одному клиенту ничего не гарантировали, то ему достанутся лишь остатки ресурса.

Все вышесказанное верно при распеределении скоростей как в прямом, так и обратном направлениях, как для одного, так и для нескольких клиентов.

Префикс NO. Не используется.

Аргументы.

MAC-адрес

MAC-адрес беспроводного интерфейса клиентской станции.

ЗНАЧЕНИЕ

составное значение скорости для прямого и обратного направления в виде

ЗНАЧЕНИЕ_ПР/ЗНАЧЕНИЕ_ОБР. Скорость может указываться как битах, так и в сокращенной нотации с помощью суффиксов "M" - мегабит и "K" - килобит (суффиксы не чувствительны к регистру).

Пример 174. Установка минимально допустимой скорости передачи в прямом и в обратном направлениях

```
RAPIRA: interface wireless 0 polling-min-rate 00:15:6d:54:31:0f 10M/5M
```

Если ЗНАЧЕНИЕ_ПР или ЗНАЧЕНИЕ_ОБР равно "0", то скорость в данном направлении контролироваться не будет (если нет правила по умолчанию - см. ниже). Таким образом, если необходимо отказаться от одного из ранее введенных параметров нужно просто еще раз вызвать данную команду со значением равным 0, при этом, если поставить равным "0" оба параметра (0/0), то правило удалится так же, как при использовании команды polling-delete.

Если в качетсве MAC адреса будет широковещательный адрес: FF:FF:FF:FF:FF:FF - то данное правило будет являтся правилом по умолчанию и будет использоваться для всех клиентов, у которых не заданы данные параметры.

Пример 175. Установка правила по умолчанию

```
RAPIRA: interface wireless 0 polling-min-rate FF:FF:FF:FF:FF:FF 1M/0
```

Таким образом, для всех клиентов, у которых отсутствует правило на минимальное ограничение скорости в прямом направлении (ЗНАЧЕНИЕ_ПР), скорость будет не менее 1M. На скорость в обратном направлении конкретно данная команда не повлияет.

см. также polling-max-rate

см. также Настройка поллинга

polling-priority

`polling-priority {MAC-address} {priority (integer [0:100])}`

Описание. Установка приоритетов клиентских станций. Команда может быть выполнена только на базовой станции.

Приоритет в данной системе является жестким, таким образом, если у одного клиента приоритет хоть на 1 выше чем у другого, то первый клиент получит весь ресурс, если у него нет ограничений на максимальную скорость. Клиенты с равным приоритетом равноправны.

Префикс NO. Не используется.

Аргументы.

MAC-address

MAC-адрес клиента, например 00:15:6d:54:30:da.

priority (integer [0:100])

значение приоритета от 0 до 100.

Пример 176. Установка приоритетов клиентских станций

```
RAPIRA: interface  Wireless 0 polling-priority 00:15:6d:54:30:da 2
```

Если в качетсве MAC-адреса будет широковещательный адрес: FF:FF:FF:FF:FF:FF - то данное правило будет являтся правилом по умолчанию и будет использоваться для всех клиентов, у которых не заданы данные параметры.

Пример 177. Установка приоритета по умолчанию

```
RAPIRA: interface wireless 0 polling-priority FF:FF:FF:FF:FF:FF 1
```

см. также polling-tolerance-max

см. также polling-max-rate

см. также polling-min-rate

см. также Настройка поллинга

polling-percentage

`polling-percentage {процент времени [10:100]}`

Описание. Установка соотношения времени работы базы в полинге и без поллинга. Команда может быть выполнена только на базовой станции.

Время разбивается на периодические интервалы длительностью в 100 мс. Команда устанавливает процент от 100 мс, в котором базовая станция работает с клиентскими станциями, поддерживающими поллинг. Оставшееся время база работает с клиентскими станциями, не поддерживающими поллинг (либо с отключеным поллингом).

Префикс NO. Не используется.

Аргументы.

процент времени

процент от 100 мс, в котором AP работает с клиентами.

Пример 178. Установка соотношения времени работы базы в полинге и без поллинга

```
RAPIRA: interface  Wireless 0 polling-percentage 90
```

см. также polling-tolerance-max

см. также polling-stations-max

см. также polling-max-rate

см. также polling-min-rate

см. также Настройка поллинга

polling-tolerance-max

```
polling-percentage {время в миллисекундах [3:128]}
```

Описание. Данное значение опеределяет максимальное время, в течение которого базовая станция не будет пытаться опросить станции, не передающие данных. **Не меняйте данный параметр, если вы не уверены в своих действиях!** Значение по умолчанию равно 32 мс. Значние по умолчание не отображается в файле конфигурации. Команда может быть выполнена только на базовой станции.

Префикс NO. Не используется.

Аргументы.

миллисекунды

время в миллисекундах, в интервале 3 - 128 мс

Пример 179. Установка максимального время, в течение которого базовая станция не будет пытаться опросить станции, не передающие данных

```
RAPIRA: interface  Wireless 0 polling-tolerance-max 64
```

см. также polling-priority

см. также polling-max-rate

см. также polling-min-rate

см. также Настройка поллинга

polling-delete

```
polling-delete {MAC-address}
```

Описание. Удаление всех правил поллинга для клиентской станции с заданым MAC-адресом, а именно: максимальной сокрости, минимальной и приоритета. Если на данный момент существуют правила по умолчанию они применются к данной станции автоматически. Команда может быть выполнена только на базовой станции.

Префикс NO. Не используется.

Аргументы.

MAC-address

MAC-адрес клиента, например 00:15:6d:54:30:da.

Пример 180. Удаление правил для конкретной клиентской станции

```
RAPIRA: interface  Wireless 0 polling-delete 00:15:6d:54:30:da
```

см. также polling-clear

см. также Настройка поллинга

polling-clear

`polling-clear`

Описание. Удаление всех правил поллинга из системы. Команда удаляет все правила, включая правила по умолчанию. Команда может быть выполнена только на базовой станции.

Префикс NO. Не используется.

Аргументы. Аргументы отсутствуют.

Пример 181. Удаление всех правил поллинга из системы.

```
RAPIRA: interface  Wireless 0 polling-clear
```

см. также polling-delete

см. также Настройка поллинга

shutdown

Описание: Поднятие указанного интерфейса.

Префикс NO. Поднять указанный интерфейс.

Аргументы: Аргументы отсутствуют.

Пример 182. Поднятие интерфейса.

```
RAPIRA: interface  Wireless no shutdown
```

speed

Описание. Настройка скорости передачи данных по беспроводному каналу связи. Данная скорость является канальной скоростью передачи. Скорость передачи данных пользователя будет определяться энергетическими параметрами линии и характеристиками потока передаваемых данных.

1. **Описание команды speed для устройств с поддержкой протокола MIMO (802.11a/b/g/n).**

```
interface {name} {index} speed {auto} | скорость в Мбит/с {auto} | индекс MCS
```

Префикс NO. Не используется.

Аргументы.

rate

Параметр имеет смысл менять только при использовании протоколов 802.11a и 802.11g (когда параметр mode выставлен в значение noht). Скорость передачи данных выражается в мегабитах в секунду (Mbit/s). По стандартам IEEE 802.11a и IEEE 802.11g поддерживаются следующие скорости: 6, 9, 12, 18, 24, 36, 48 и 54 Mbit/s. Если используется протокол 802.11n(параметр mode выставлен в значение ht20/ht40+/ht40-), то параметр должен быть выставлен в значение auto. Если значение установлено в auto, то будет выбрана оптимальная скорость передачи данных.

индекс MCS

Индекс модуляции и схемы кодирования MCS (Modulation and Coding Scheme)- целое число в диапазоне от 0 до 15, присваиваемое каждому варианту модуляции. Число определяет тип модуляции радиочастоты, скорость кодирования, защитный интервал и значения скорости передачи данных. Сочетание перечисленных факторов определяет канальную скорость передачи данных при использовании 2-х потоков в диапазоне от 6,5 Мбит/с до 144 Мбит/с (при ширине полосы в 20 МГц) и от 15 Мбит/с до 300 Мбит/с (при ширине полосы в 40 МГц). Если значение установлено в auto, то будет выбран оптимальный индекс. Скорости, поддерживаемые стандартом IEEE 802.11n детально представлены в нижеприведённой таблице.

Таблица 10. Параметры при частотном разносе каналов 40 МГц (ht40+ и ht40-).

Номер схемы MCS	Модуляция	Количество потоков	Скорость передачи данных, Мбит/с (защитный интервал 400 нс)
0	BPSK	1	15
1	QPSK	1	30
2	QPSK	1	45
3	16-QAM	1	60
4	16-QAM	1	90
5	64-QAM	1	120
6	64-QAM	1	135
7	64-QAM	1	150
8	BPSK	2	30
9	QPSK	2	60
10	QPSK	2	90
11	16-QAM	2	120

Номер схемы MCS	Модуляция	Количество потоков	Скорость передачи данных, Мбит/с (защитный интервал 400 нс)
12	16-QAM	2	180
13	64-QAM	2	240
14	64-QAM	2	270
15	64-QAM	2	300

Пример 183. Автоматическая настройка скорости (MIMO)

```
RAPIRA: interface Wireless 0 speed auto auto
Speed is set to 'auto', mcs 'auto' in mode 'ht40+'.
```

2. **Описание для устройств с поддержкой протоколов 802.11a/b/g.**

```
interface {name} {index} {speed} {rate} | auto
```

Аргументы.

rate

Скорость передачи данных выражается в мегабитах в секунду (Mbit/s). По стандартам IEEE 802.11a и IEEE 802.11g поддерживаются следующие скорости: 6, 9, 12, 18, 24, 36, 48 и 54 Mbit/s. По стандарту IEEE 802.11b поддерживаются следующие скорости: 1, 2, 5.5 и 11 Mbit/s. Если значение установлено в auto, то будет выбрана оптимальная скорость передачи данных.

Пример 184. Установка значения канальной скорости при работе по протоколу 802.11a/g

```
RAPIRA: interface Wireless 0 speed 54
Speed is set to 54 Mb/s.
```

ssid

```
interface {name} {index} ssid {value}
```

Описание. Установка SSID.

Префикс NO. Не используется.

Аргументы.

value

Поле SSID должно содержать не менее одного символа и не должно содержать пробелов.

Пример 185. Настройка SSID

```
RAPIRA: interface Wireless 0 ssid nsolod
Interface 'Wireless 0': SSID 'nsolod'.
RAPIRA: show interfaces Wireless 0
Wireless 0 is up
Hardware address:  18fd.74b9.b311  VLAN: none
Internet address:  0.0.0.0 mask 0.0.0.0
                   broadcast:  0.0.0.0, MTU: 1500
Type: ap, SSID: "nsolod", Mode: ht40+
Speed: 270 Mb/s (auto), Access point: N/A
Channel: 152, Frequency: 5760 MHz, Tx-power: 26 dBm
RTS: off, Distance: 3000, WDS: on
WMM: off, Beacon: 100
Antenna: auto, IEEE 802.11g Protection: ?
```

см. также Настройка SSID

traffic-shape group

`traffic-shape group {access-list} {bit-rate} [burst-size]`

Описание: Ограничение пропускной способности по группам.

Префикс NO. Не используется.

Аргументы:

access-list

Имя списка контроля доступа.

bit-rate

Максимальная скорость передачи (бит/с), допустимо использовать суффиксы: m (мегабит) и k (килобит). Допустимы значения от 32000 до 100000000 бит.

burst-size

Всплеск - объем данных, который будет передан в начальный момент времени на максимальной скорости. Минимальное значение - 128000 бит.

Если значение burst-size не указано, то оно рассчитывается автоматически и находится в оптимальных пределах. Данное значение необходимо указывать только в крайнем случае.

Несколько примеров настройки рассмотрены ниже:

A. Выделение полосы в 1 Мбит/с на интерфейсе Wireless 0 для каждого из клиентов с IP адресами 192.168.0.2, 192.168.0.3 и 192.168.0.4.

Пример 186. Выделение полосы для каждого клиента по IP-адресу

```
RAPIRA: access-list 101 permit any host 192.168.0.2
RAPIRA: access-list 102 permit any host 192.168.0.3
RAPIRA: access-list 103 permit any host 192.168.0.4
RAPIRA: interface Wireless 0 traffic-shape group 101 1000000
RAPIRA: interface Wireless 0 traffic-shape group 102 1000000
RAPIRA: interface Wireless 0 traffic-shape group 103 1000000
```

B. Выделение следующих полос на интерфейсе Wireless 0 для указанных IP-адресов:192.168.0.2 - 1 Мбит/с; 192.168.0.3 - 512 Кбит/с; 192.168.0.4 - 3 Мбит/с.

Пример 187. Выделение определенной полосы для каждого клиента по IP-адресу

```
RAPIRA: access-list 101 permit any host 192.168.0.2
RAPIRA: access-list 102 permit any host 192.168.0.3
RAPIRA: access-list 103 permit any host 192.168.0.4
RAPIRA: interface Wireless 0 traffic-shape group 101 1000000
RAPIRA: interface Wireless 0 traffic-shape group 102 512000
RAPIRA: interface Wireless 0 traffic-shape group 103 3000000
```

C. Выделение полосы на интерфейсе Wireless 0 в 7 Мбит/с для узлов подсети 192.168.1.0/24 и 10 Мбит/с для узлов подсети 192.168.2.0/24.

Пример 188. Выделение полосы на каждую подсеть

```
RAPIRA: access-list 101 permit any 192.168.1.0 0.0.0.255
RAPIRA: access-list 102 permit any 192.168.2.0 0.0.0.255
RAPIRA: interface Wireless 0 traffic-shape group 101 7000000
RAPIRA: interface Wireless 0 traffic-shape group 102 10000000
```

D. Для HTTP и HTTPS трафика ограничить полосу на интерфейсе Wireless 0 до 3 Мбит/с, всплеск 5000 байт (40000 бит)

Пример 189. Ограничение трафика HTTP(s).

```
RAPIRA: access-list 101 permit any eq 80 any
RAPIRA: access-list 101 permit any eq 443 any
RAPIRA: interface Wireless 0 traffic-shape group 101 3000000 40000
```

E. Для ICMP-трафика на интерфейсе Wireless 0 ограничить полосу до 3 Мбит/с.

Пример 190. Ограничение трафика ICMP.

```
RAPIRA: access-list 101 permit icmp any any
RAPIRA: interface Wireless 0 traffic-shape group 101 3000000
```

см. также Списки контроля доступа

traffic-shape rate

`traffic-shape rate {bit-rate} [burst-size]`

Описание: Ограничение общей пропускной способности.

Префикс NO. Не используется.

Аргументы:

bit-rate

Максимальная скорость передачи (бит/с), допустимо использовать суффиксы: m (мегабит) и k (килобит). Допустимы значения от 32000 до 100000000 бит.

burst-size

Всплеск - объем данных, который будет передан в начальный момент времени на максимальной скорости. Минимальное значение - 128000 бит.

Если значение burst-size не указано, то оно рассчитывается автоматически и находится в оптимальных пределах. Данное значение необходимо указывать только в крайнем случае.

Пример 191. Ограничение пропускной способности на проводном интерфейсе до 512 кбит/с.

```
RAPIRA: interface FastEthernet 0 traffic-shape rate 512k
```

tx-power

`interface {name} {index} tx-power {power}`

Описание. Установка мощности передачи.

Префикс NO. Восстанавливает значение мощности по умолчанию.

Аргументы.

power

Значение мощности выражается в dBm, в целых числах. Приемлемый диапазон от 1 до 30.

Просмотр допустимых значений мощности конкретного устройства осуществляется командой tx-power-range.

Обратите внимание:

Учитывая неравномерность АЧХ передающего каскада на разных частотах, необходимо проверять максимально возможное значение для каждой частоты.

Пример 192. Настройка мощности передачи

```
RAPIRA: interface Wireless 0 tx-power 29
         The tx-power value is set to 29 dBm.
```

см. также Установка выходной мощности сигнала

type

Описание. В настоящее время RAPIRA RS3 работает либо в режиме базовой станции (AP), либо в режиме клиентской станции (station). Для установки определенного типа используется следующая команда:

`interface {name} {index} type {ap | station}`

Пример 193. Настройка типа оборудования

```
RAPIRA: interface Wireless 0 type ap
Interface 'Wireless 0': type 'ap'.
RAPIRA: interface Wireless 0 type station
Interface 'Wireless 0': type 'station'.
```

wds-mode

Описание. Если **беспроводной (wireless)** интерфейс включен в группу моста, необходимо установить флаг **WDS**, чтобы включить прозрачную ретрансляцию ethernet-фреймов.

Префикс NO. Снятие флага WDS.

Аргументы: Аргументы отсутствуют.

Пример 194. Настройка WDS

```
RAPIRA: interface Wireless 0 wds-mode
WDS mode is turned on.
```

см. также Создание прозрачного моста

wmm

Описание:Включение QoS.

Префикс NO. Отключение QoS.

Аргументы: Аргументы отсутствуют.

Пример:

```
        RAPIRA: interface  Wireless 0 wmm
```

см. также QoS

Список команд ветви SYSTEM

countrycode

1. **Смена countrycode в устройствах с поддержкой протокола 802.11n (MIMO)**

```
countrycode {default | xx}
```

Описание: Смена countrycode.

Аргумент **xx** позволяет использовать расширенный список частот с шагом 5 МГц.

Для применения новых настроек в MIMO-устройствах нет необходимости перезагружать систему.

При работе в расширенном списке частот рекомендуется выполнять сканирование с параметром **freq**, что значительно сокращает время выполнения команды.

Для настройки ширины частотного канала в MIMO-устройствах используется команда mode.

см. также Просмотр списка доступных частот

см. также Отображение текущего countrycode

2. **Смена countrycode в устройствах с поддержкой протоколов 802.11a/b/g**

```
countrycode {default | e1 | e2 | e3 | e4 | e5 | e9}
```

Описание: Смена countrycode. Указанные аргументы актуальны для устройств с поддержкой ТОЛЬКО протоколов 802.11a/b/g.

Данная функция позволяет менять частотную сетку в соответствии с нижеприведенной таблицей. Шаг сетки частот равен 20 МГц. При необходимости величина шага может быть изменена (см. ниже).

Таблица 11. Доступные частотные диапазоны

countrycode	Частотный диапазон	
	5xxx МГц	2xxx МГц
default	5180-5825 МГц	2412-2482 МГц
e1	4920-6060 МГц	-
e2	4925-6065 МГц	-
e3	4930-6070 МГц	-
e4	4915-6075 МГц	-
e5	-	2312-2372 МГц

e9	5900-6000 МГц [1]	-

1. Доступен 21 канал с шагом в 5 МГЦ.

Для применения новых настроек в устройствах с поддержкой только протоколов 802.11a/b/g необходимо перезагрузить систему.

Пример 195. Настройка coutrycode

```
RAPIRA: system countrycode default
The country code is set to 'default'.
Reboot the system to apply changes.
RAPIRA:  reboot
```

При использовании вышеуказанных countrycode ширина частотного канала составляет 20 Мгц. Это значение при необходимости можно изменить на следующие:

Таблица 12. Ширина частотного диапазона

countrycode	Ширина частотного диапазона (МГц)
e1-e5, e9	20
h1-h5, h9	10
q1-q5, q9	5

date

Описание:

см. Настройка даты и времени

password

Описание:

см. Смена пароля доступа в систему

update

Описание:

см. Загрузка и обновление программного обеспечения

Сброс параметров маршрутизатора в стандартные значения

Сброс всех параметров маршрутизатора RAPIRA RS3 (кроме пароля доступа в систему) возможен несколькими способами:

1. **IP-адрес маршрутизатора известен**

   Выполните следующие команды:

   Пример 196. Сброс настроек маршрутизатора с помощью команды COPY

   ```
   RAPIRA: copy default-config startup-config
   RAPIRA: reboot
   ```

2. **IP-адрес маршрутизатора не известен и нет возможности выключить питание маршрутизатора**

   В консоли операционной системы запустить утилиту Power_soft_reset, расположенную на прилагаемом компакт-диске, с параметром **scan**:

   Пример 197. Получение серийных номеров доступных радиомаршрутизаторов

   ```
   c:\Power_soft_reset scan

   MAC                Type        Serial
   00:0c:42:37:b5:e5  Ethernet    12570
   00:0c:42:37:b5:e5  Bridge      12570
   ```

После выполнения команды **scan** связжитесь со службой технической поддержки нашей компании и сообщите результат её выполнения для получения уникального пароля маршрутизатора.

Вновь запустите утилиту Power_soft_reset, с параметром `reset xx:x:xx:xx:xx:xx [password]` , где **xx:x:xx:xx:xx:xx** - Ethernet-MAC-адрес из левого столбца результата выполнения команды **scan**. После появления приглашения введите пароль, полученный от службы технической поддержки (с учетом регистра символов). По соображениям безопасности рекомендуется указывать пароль не в командной строке, а ввести его после запроса:

Пример 198. Сброс всех параметров маршрутизатора без выключения питания

```
c:\Power_soft_reset reset 00:10:00:00:01:29
Device password: QwErTyUiOp

c:\
```

После этого устройство будет перезагружено; для связи с маршрутизатором используйте

стандартный ip-адрес: 192.168.0.5

В некоторых случаях работа данной утилиты может вызвать срабатывание детектора сетевых атак. Рекомендуется отключать его перед проведением процедуры сброса.

см. также Смена пароля доступа в систему

Получение IP-адреса маршрутизатора

Существует возможность получения IP-адреса маршрутизатора в случае его утери.

Данная возможность будет полезна в случае, когда IP-адрес устройства не известен, а произвести сброс настроек - недопустимо (например, маршрутизатор работает в режиме бриджа и доступ к нему возможен только по радиоканалу).

Для этого необходимо заранее получить серийный номер маршрутизатора и его уникальный пароль (см. Получение серийных номеров доступных радиомаршрутизаторов), а затем выполнить следующие действия:

В консоли операционной системы запустить утилиту Power_soft_reset, расположенную на прилагаемом компакт-диске, с параметром **getip** и MAC-адресом устройства (Device MAC), а затем ввести пароль маршрутизатора:

Пример 199. Получение IP-адреса маршрутизатора, настроенного прозрачным мостом

```
c:\power_soft_reset.exe getip 00-10-00-00-01-29
Device password:
.............................
Device with MAC '00:10:00:00:01:29': Operation success.
Interface type: Ethernet
Device interface IP: 0.0.0.0

Device with MAC '00:10:00:00:01:29': Operation success.
Interface type: Bridge
Device interface IP: 192.168.0.251
```

см. также Сброс параметров маршрутизатора в стандартные значения

см. также Смена пароля доступа в систему

Удаленная перезагрузка маршрутизатора

Стандартный процесс перезагрузки системы описывает раздел Перезагрузка системы.

Существует также возможность удаленной перезагрузки маршрутизатора, даже если IP-адрес устройства не известен и нет доступа к питанию устройства.

Для этого необходимо заранее получить MAC-адрес маршрутизатора и его уникальный пароль (см. Получение серийных номеров доступных радиомаршрутизаторов), а затем выполнить следующие действия:

В консоли операционной системы запустить утилиту Power_soft_reset, расположенную на прилагаемом компакт-диске, с параметром **reboot** и MAC-адресом устройства (Device MAC), а затем ввести пароль маршрутизатора:

Пример 200. Удаленная перезагрузка маршрутизатора

```
c:\power_soft_reset.exe reboot 00-10-00-00-01-29
Device password:
.............................
Device with MAC '00:10:00:00:01:29': Operation success.
Device rebooted.
```

см. также Сброс параметров маршрутизатора в стандартные значения

см. также Смена пароля доступа в систему

Примеры конфигураций

Настройка базовой станции в режиме прозрачного моста

см. также Создание прозрачного моста

Пример показывает, как выполнить следующие операции:

- Настройка базового беспроводного соединения в локальной сети (LAN) между базовой и клиентской станциями.
- Настройка базовой станции (AP) в режиме прозрачного моста с открытой авторизацией.
- Определение группы моста, а также включение в группу беспроводного и проводного интерфейсов
- Проверку возможности соединения между клиентской и базовой станциями.

Впоследствии, для просмотра настроенной конфигурации Вы можете воспользоваться следующими основными командами:

- **show running-config** - просмотр текущей конфигурации
- **show interfaces** - просмотр статуса интерфейсов
- **show interface wireless 0 associated** - просмотр ассоциированных с базой клиентских станций
- **show interface wireless 0 signal** - просмотр характеристик принимаемого станцией сигнала
- **show interface wireless 0 scan** - просмотр информации об обнаруженных базовых станциях
- **show interface wireless 0 statistics** - просмотр статистики беспроводного интерфейса
- **show interface wireless 0 channel-list** - просмотр списка доступных частот

Для просмотра полного перечня команд, отображающих информацию о системе, обратитесь в Список команд ветви SHOW

Пример 201. Настройка базовой станции по протоколу 802.11g в режиме прозрачного моста без использования шифрования

```
RAPIRA: interface bridge 0
Bridge 0 is created.

RAPIRA: interface bridge 0

config-if: ip address 192.168.1.1
Device 'Bridge 0' address 192.168.1.1 netmask 255.255.255.0.

config-if: no shutdown
Interface 'Bridge 0' is up.
config-if: exit

RAPIRA: interface Wireless 0

config-if: type ap
Interface 'Wireless 0': type 'ap'.

config-if: ssid gsp1
Interface 'Wireless 0': SSID 'EMSCH'.

config-if: speed auto
Speed is set to 'auto'.

config-if: fast-frame
Fast frame is turned on.

config-if: channel 2412
Channel is set to '2412'.

config-if: tx-power 26
The tx-power value is set to 26 dBm.

config-if: wds-mode
WDS mode is turned on.

config-if: distance 15000
A distance value is set to '15000'.

config-if: no shutdown
Interface 'Wireless 0' is up.

config-if: bridge-group 0
Interface 'Wireless 0' was added to the bridge group '0'.

config-if: exit

RAPIRA: interface FastEthernet 0 bridge-group 0
```

Если адрес прозрачного моста отличается от IP-адреса, присвоенному интерфейсу FastEthernet, то после выполнения вышеуказанной команды соединение с системой будет утеряно. Необходимо **не выключая маршрутизатор** заново войти в систему, используя IP-адрес созданного прозрачного моста и сохранить конфигурацию:

```
RAPIRA: copy running-config startup-config
Running-config successfully copied.
```

Пример 202. Настройка базовой станции по протоколу 802.11n в режиме прозрачного моста с использованием шифрования (WPA2)

```
RAPIRA: interface bridge 0
Bridge 0 is created.

RAPIRA: interface bridge 0

config-if: ip address 192.168.1.1
Device 'Bridge 0' address 192.168.1.1 netmask 255.255.255.0.

config-if: no shutdown
Interface 'Bridge 0' is up.
config-if: exit

RAPIRA: interface Wireless 0

config-if: type ap
Interface 'Wireless 0': type 'ap'.

config-if: ssid gsp1
Interface 'Wireless 0': SSID 'MVK'.

config-if:interface Wireless 0 mode ht40+
The mode is set to 'ht40+'.

config-if:  interface Wireless 0 speed auto auto
Speed is set to 'auto', mcs 'auto' in mode 'ht40+'.

config-if: channel 5800
Channel is set to '5800'.

config-if: tx-power 30
The tx-power value is set to 30 dBm.

config-if: wds-mode
WDS mode is turned on.

config-if: distance 5000
A distance value is set to '5000'.

config-if: no shutdown
```

```
Interface 'Wireless 0' is up.

config-if: authentication wpa-psk qwe!@57'~?asdZXC
WPA PSK enabled.

config-if: encryption ccmp
Interface 'Wireless 0': CCMP enabled.

config-if: bridge-group 0
Interface 'Wireless 0' was added to the bridge group '0'.

config-if: exit

RAPIRA: interface FastEthernet 0 bridge-group 0
```

Если адрес прозрачного моста отличается от IP-адреса, присвоенному интерфейсу FastEthernet, то после выполнения вышеуказанной команды соединение с системой будет утеряно. Необходимо **не выключая маршрутизатор** заново войти в систему, используя IP-адрес созданного прозрачного моста и сохранить конфигурацию:

```
RAPIRA: copy running-config startup-config
Running-config successfully copied.
```

Обратите внимание:

- допустимая длина вводимого при настройке шифрования пароля составляет 9-63 символа
- пароли в команде `authentication wpa-psk` должны **полностью совпадать** на состоящих в мосте маршрутизаторах

Настройка маршрутизатора в качестве DHCP-сервера

Допустим, клиентским станциям необходимо раздавать

ip-адреса из диапазона 10.1.1.5 - 10.1.1.25;

ip-адрес default-gateway - 192.168.3.100;

ip-адрес FastEthernet-интерфейса радиомаршрутизатора - 192.168.3.253;

ip-адрес Wireless-интерфейса радиомаршрутизатора - 10.1.1.1

Пример 203. Настройка базовой станции в качестве DHCP-сервера

```
RAPIRA: interface Wireless 0

RAPIRA: interface Wireless 0 ip address  10.1.1.1/24
```

```
Device 'Wireless 0' address 10.1.1.1 netmask 255.255.255.0.

config-if: type ap
Interface 'Wireless 0': type 'ap'.

config-if: ssid KVG
Interface 'Wireless 0': SSID 'KVG'.

config-if: speed auto
Speed is set to 'auto'.

config-if: fast-frame
Fast frame is turned on.

config-if: channel 2412
Channel is set to '2412'.

config-if: tx-power 26
The tx-power value is set to 26 dBm.

config-if: distance 5000
A distance value is set to '5100'.

config-if: no shutdown
Interface 'Wireless 0' is up.

config-if: exit

RAPIRA: ip dhcp pool p1

dhcp-config: network 10.1.1.0 255.255.255.0
Network pool: 10.1.1.0 255.255.255.0.

dhcp-config: range 10.1.1.5 10.1.1.25
Range added: 10.1.1.5 10.1.1.25

dhcp-config: default-router 10.1.1.1
Default router 10.1.1.1 has been added.

dhcp-config: dns-server 81.25.35.2 10.7.3.40
DNS server 81.25.35.2 has been added.
DNS server 10.7.3.40 has been added.

dhcp-config: exit

RAPIRA: service dhcp
DHCP service enabled.

RAPIRA: nat-list 123 snat any any to 192.168.3.253

RAPIRA:interface FastEthernet 0 nat-group 123
```

```
RAPIRA: ip  default-gateway 192.168.3.100
Default route changed.
```

При этом на клиентских устройствах необходимо выполнить следующую команду и сохранить конфигурацию:

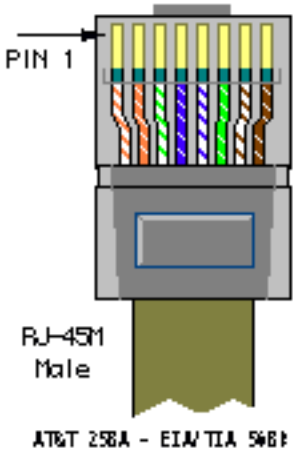
```
RAPIRA: interface Wireless 0 ip dhcp
    DHCP client enabled.
RAPIRA: copy running-config startup-config
    Running-config successfully copied.
```

DHCP-клиент автоматически получает IP-адрес, маршрут по умолчанию и DNS-адреса с сервера DHCP.

Приложение

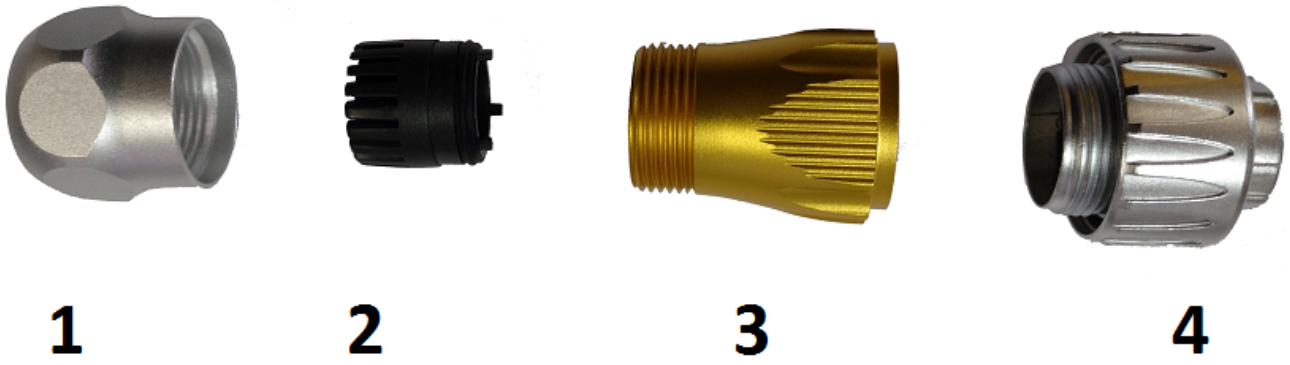
Схема обжима кабеля

Контакт	EIA/TIA 568B
1	Белый+Оранжевый
2	Оранжевый
3	Белый+Зелёный
4	Синий
5	Белый+Синий
6	Зелёный
7	Белый+Коричневый
8	Коричневый



Снятие герметичного соединителя

Процедуры сборки и установки герметичного соединителя описаны в разделе Подготовка радиомаршрутизатора к использованию.



- Открутите накидную гайку (1)
- Ослабьте на 2-3 оборота корпус разъёма (3)
- Поворачивайте накидную часть на байонетном блоке (4) против часовой стрелки примерно на 45°с нажатием на него в сторону корпуса радиомаршрутизатора.

Внимание!

Повороты байонетной накидной гайки должны быть свободные с небольшим усилием (выход упоров из защёлки) при раскручивании. Если гайка идёт с большим усилием, то ослабьте или открутите корпус разъёма (3).

- Разъедините разъёмы.

Замена разъёма RJ-45, установленного в герметичном соединителе

- Открутите накидную гайку (1)
- Выньте цанговый фиксатор (2) из корпуса разъёма (3)
- Удалите фиксирующий хвостик разъёма RJ-45, для этого рекомендуется использовать бокорезы модели PM-722F или аналогичные.

Внимание!

Пластиковый хвостик должен быть срезан заподлицо, поэтому располагайте плоскость режущих частей бокорезов по корпусу разъема RJ-45.

- Вытяните кабель с разъёмом RJ-45.
- Смонтируйте шнур питания и блок питания со встроенным инжектором. Подключите кабель маршрутизатора к разъему «PoE Out», кабель локальной сети - к разъему «Data», а шнур питания - к соответствующему разъему питания инжектора.

Внимание!

Неправильное подсоединение POE-инжектора может привести к поломке сетевого оборудования!

Внимание!

Используйте только специальный не экранированный разъем RJ-45 для FTP кабеля при оконцовке кабеля снижения с нижней стороны. Запрещается подключать дренажный проводник кабеля к заземлению стойки, где расположен источник питания, поскольку это может привести к образованию токовой петли и повреждению кабеля.

Внимание!

Настоятельно рекомендуется дополнительно герметизировать места ввода и сочленения кабелей (кабельная муфта, кабельные вводы).