



O-T-S.ru
Объединённые
Технологии
Связи

Интернет-магазин
средств связи и визуализации
Для новичка и профессионала

Официальный поставщик
Ubiquiti Networks в России

Содержание

- 1 AirOS v5.3 Введение
- 2 AirOS v5.3 Руководство по конфигурации
 - 2.1 Навигация
 - 2.2 Страница Ubiquiti
 - 2.2.1 AirMax Settings
 - 2.2.2 AirSelect
 - 2.2.3 AirView
 - 2.2.4 AirControl
 - 2.3 Страница Main
 - 2.3.1 Status
 - 2.3.2 Monitor
 - 2.4 Страница Wireless
 - 2.4.1 Basic Wireless Settings
 - 2.4.2 Wireless Security
 - 2.4.2.1 WEP
 - 2.4.2.2 WPA/WPA2
 - 2.4.2.2.1 EAP Authentication - Station Mode
 - 2.4.2.2.2 EAP Authentication - AP Mode
 - 2.4.2.3 MAC ACL
 - 2.5 Страница Network
 - 2.5.1 Network settings
 - 2.5.1.1 Bridge Mode
 - 2.5.1.2 Router Mode
 - 2.5.1.2.1 WLAN Network Settings
 - 2.5.1.2.2 LAN Network Settings
 - 2.5.1.3 SOHO Router
 - 2.5.1.3.1 WAN Network Settings
 - 2.5.1.3.2 LAN Network Settings
 - 2.5.1.4 VLAN Network Settings
 - 2.5.1.5 Multicast Routing Settings
 - 2.5.1.6 Firewall Settings
 - 2.5.1.7 Static Routes
 - 2.6 Страница Advanced
 - 2.6.1 Advanced Wireless Setting
 - 2.6.2 Advanced Ethernet Settings
 - 2.6.3 Signal LED Thresholds
 - 2.6.4 Traffic Shaping
 - 2.7 Страница Services

- 2.7.1 Ping WatchDog
- 2.7.2 SNMP Agent
- 2.7.3 Web Server
- 2.7.4 SSH Server
- 2.7.5 Telnet Server
- 2.7.6 NTP Client
- 2.7.7 Dynamic DNS
- 2.7.8 System Log
- 2.8 Страница System
 - 2.8.1 Device
 - 2.8.2 Date Settings
 - 2.8.3 System Accounts
 - 2.8.4 Miscellaneous
 - 2.8.5 Location
 - 2.8.6 Configuration Management
 - 2.8.7 Device Maintenance
 - 2.8.7.1 Firmware upload
- 2.9 Меню Tools
 - 2.9.1 Align Antenna
 - 2.9.2 Site Survey
 - 2.9.3 Device Discovery
 - 2.9.4 Ping
 - 2.9.5 Traceroute
 - 2.9.6 Speed Test
 - 2.9.7 AirView
 - 2.9.7.1 Main View
 - 2.9.7.2 Preferences

1. AirOS v5.3 Введение

AirOS v5.3 является самой новой операционной системой в семействе **Ubiquiti AirOS**, которая включает в себя функции, такие как **AirSelect** и новые версии **AirMax** и **AirView**. Эта современная операционная система обладает мощными беспроводными функциями и функциями маршрутизации, построена на простом пользовательском интерфейсе. **AirOS v5.3** maximizes производительность беспроводных продуктов **Ubiquiti M** серии, которые основаны на [IEEE 802.11n](#).

2. AirOS v5.3 Руководство по конфигурации

Данное руководство представляет подробное описание системы AirOS версии 5.3, которая интегрирована во все продукты серии M производства Ubiquiti Networks, Inc.

AirOS v5.3 поддерживается продуктами новой серии M:

M900 (900MHz) серия:

- [Rocket M900](#)
- [Loco M900](#)

M2 (2.4GHz) серия:

- Bullet M2 HP
- Nano/LoCo M2

- Rocket M2
- PicoStation M2 HP
- AirGrid M2
- NanoBridge M2

M3 (3GHz) серия:

- [Rocket M3](#)
- [Nano M3](#)
- [PowerBridge M3](#)

M365 (3.65GHz) серия:

- [Rocket M365](#)
- [Nano M365](#)
- [PowerBridge M365](#)

M5 (5GHz) серия:

- Bullet M5 HP
- Nano/LoCo M5
- Rocket M5
- PowerBridge M5
- AirGrid M5
- NanoBridge M5

Все устройства на базе AirOS поддерживают следующие режимы работы беспроводной инфраструктуры:

- [Station](#) (Беспроводной клиент);
- [Station WDS](#) (Беспроводной клиент Repeater);
- [Access Point](#) (Точка доступа);
- [Access Point WDS](#) (Точка доступа Repeater).

и следующие сетевые функции:

- [Transparent Layer2 bridge](#);
- [Router](#).
- SOHO Router

В этом руководстве будут рассмотрены все возможные настройки, доступные через Web-интерфейс (настройки зависящие от конкретной модели будут рассмотрены дополнительно)

Примечание: все примеры и иллюстрации в этом документе взяты с интерфейса Nanostation M2, Bullet M2 and Bullet M5, и подобны для всех устройств на базе AirOS v5.3.

AirMax M900 series



Rocket M900



Loco M900

AirMax M2 series



Rocket M2



Nano M2



Loco M2



Pico M2-HP



Bullet M2-HP



NanoBridge M2



AirGrid M2

AirMax M3 series



Rocket M3



Nano M3



PowerBridge M3

AirMax M365 series



Rocket M365



Nano M365



PowerBridge M365

AirMax M5 series



Rocket M5



Nano M5



Loco M5



Bullet M5-HP



NanoBridge M5



PowerBridge M5



AirGrid M5

2.1. Навигация

Все настройки сгруппированы по своему назначению на нескольких страницах (вкладках), перечислим их:



Страница **UBIQUITI** содержит элементы управления для фирменных технологий Ubiquiti, таких как AirMax, AirSelect и AirView.

Страница **MAIN** отображает текущее состояние устройства и статистической информации.

Страница **WIRELESS** содержит элементы управления для настройки беспроводной сети, такие как основные настройки беспроводной сети, которые определяют режим работы, выходную мощность, другие параметры связи и параметры безопасности данных.

Страница **NETWORK** охватывает настройки сетевого режима работы, IP адреса, пакетной фильтрации и сетевыми сервисами (например, DHCP-сервер).

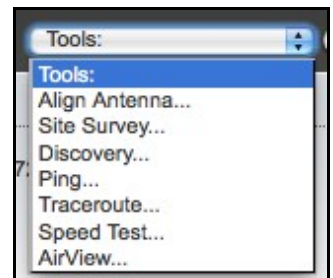
Страница **ADVANCED** предназначена для более тонкой настройки беспроводных функций. На этой странице могут быть настроены специфические параметры AirMax и 802.11n. Также здесь можно управлять сигналами индикации на корпусе и ограничить скорости трафика.

Страница **SERVICES** открывает доступ к настройке сервисных системных утилит, таких как **SNMP**, **NTP**, системный журнал, **Ping Watchdog** и **SSH/Telnet** сервера.

Страница **SYSTEM** содержит элементы управления для обслуживания устройства, управления учетной записью администратора, дополнительные настройки устройства, обновление ОС и резервного копирования настроек. Также здесь можно сменить язык веб интерфейса.

Также с любой страницы доступно меню **TOOLS** в котором есть полезные утилиты для администрирования и мониторинга:

- **Antenna alignment tool** - полезное дополнение для точной подстройки антенны;
- **Site survey tool** - сканирование частот на наличие базовых станций (пункт также доступен в режиме Access Point);
- **Discovery** - сканирование сети беспроводных устройств;
- **Ping** - проверка отклика от заданного узла;
- **Traceroute** - трассировка маршрута до заданного узла;
- **SpeedTest** - утилита проверки скорости между устройствами Ubiquiti;
- **AirView** - сканирование эфира, для определения свободных частот;



2.2. Страница Ubiquiti

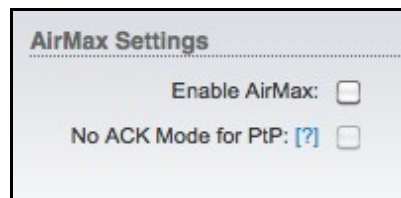
На этой странице оператор может включить и настроить фирменные технологии **Ubiquiti**, такие как **AirMax**, которая обеспечивает великолепную производительность беспроводной связи, больше клиентов на точке доступа и низкую латентность. **AirSelect**, инновационная технология, которая динамически изменяет беспроводной канал, используется для того, чтобы избежать помех, а также **AirView**, анализатор спектра Ubiquiti's.

2.2.1. AirMax Settings

AirMax это запатентованная Ubiquiti технология TDMA поллинга. AirMax обеспечивает лучшую

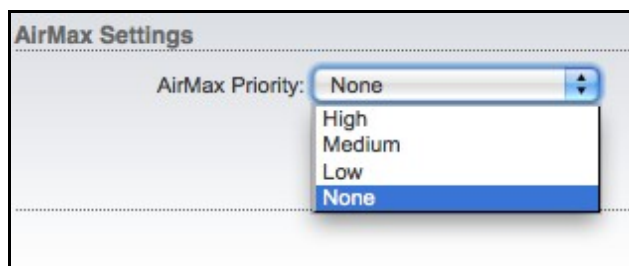
устойчивость от помех и увеличивает максимальное количество пользователей, которые могут быть подключены к точке доступа (при условии, что все устройства поддерживают AirMax). Принцип AirMax в назначении временных интервалов для каждого устройства связи, что избавляет от влияния узлов друг на друга. При работе в режиме Access Point или Access Point WDS с включенным AirMax, к базе смогут подключиться только устройства с поддержкой AirMax. (Для обратной совместимости с устройствами без поддержки AirMax, нужно отключить AirMax на базовой станции). AirMax также поддерживает автоматическое определение некоторых параметров QOS.

Enable AirMax: Если включено, устройство будет работать в режиме AirMax, включая все ее преимущества. Учтите если AirMax включен, то клиенты без поддержки AirMax не смогут подключиться к базовой станции. Этот параметр относится только к точке доступа в режиме Access Point или Access Point WDS режимах. В режиме Station или Station WDS, AirMax будет выбран автоматически при подключении к базовой станции с включенным режимом AirMax.



No ACK Mode for PtP: эта опция позволяет отключить ACK режим на большие расстояния точка-точка (17 км в полосе 40MHz или 51 км в полосе 20MHz). Важно: когда **No ACK Mode for PtP** включен, только один клиент к базовой станции может быть подключен. Если вы хотите подключить более чем 1 клиента, выберите **Auto-ACK** режим.

AirMax Priority: (доступно только в режиме Station и Station WDS) Эта функция определяет размер временных интервалов назначенных каждому клиенту, т.е. станции с более высоким приоритетом получают больше временных интервалов для передачи чем станции с более низким приоритетом. Данная функция имеет смысл если подключено более 1 клиента.



2.2.2. AirSelect

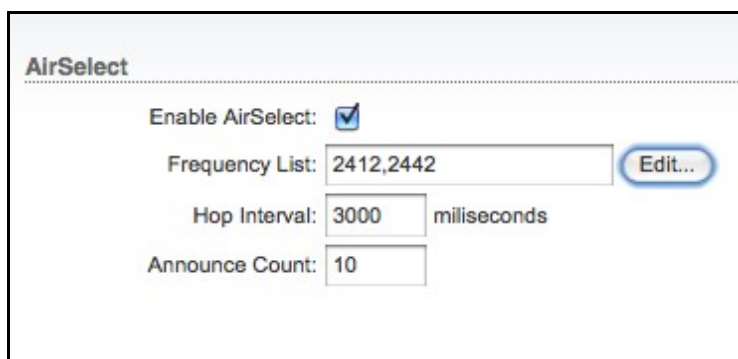
AirSelect это технология, которая динамически изменяет используемый беспроводной канал, для уменьшения помех и увеличения пропускной способности, путем перескока на канал из определенного пользователем списка частот, периодически в течение задаваемого пользователем интервала времени (в миллисекундах).

Enable AirSelect: если включен, устройство будет использовать функцию AirSelect. Эта функция поможет неопытным инсталляторам, т.е. без знаний радио частот; или устройствам, используемым в очень зашумленных средах. Но это не избавляет от тщательного планирования используемых радио частот.

Frequency List: определяет список каналов, из которых AirSelect выберет наименее зашумленный .

Hop Interval: определяет интервал времени между каждой сменой канала, и выражается в миллисекундах. Значение по умолчанию составляет 3000 миллисекунд.

Announce Count: столько раз Базовая Станция объявит своим клиентам служебную информацию перед сменой на следующую частоту . Например, если хоп интервал установлен на 10000 миллисекунд (10 секунд), и количество объявлений равное 10, каждые 1000 миллисекунд (каждую



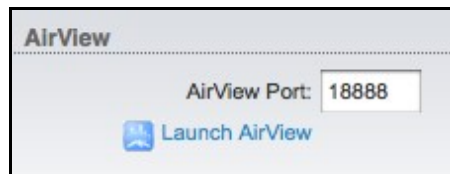
секунду) Базовая Станция будет отправлять объявление своим клиентам о наступающей смене частоты . Чем больше это значение , тем выше риск рассинхронизации с клиентами , поэтому рекомендуется не превышать это отношение более 100 миллисекунд (имежду **Announce Count** и **Hop Interval** должно быть соотношение **1 к 100**).

2.2.3. AirView

AirView это анализатор спектра встроенный в AirOS, позволяет оценить зашумленность радиочастотного спектра.

AirView Port: определяет порт для использования утилиты в этом устройстве. По умолчанию используется порт **18888**.

Launch AirView: нажмите на эту кнопку для запуска утилиты Эйрвью для данного устройства .



2.2.4. AirControl

Enable Discovery: обеспечивает обнаружение устройств, таким образом, устройство может быть обнаружено другими устройствами Ubiquiti через утилиту Discovery Tool встроенную в AirOS.

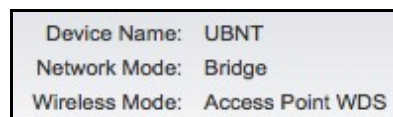


2.3. Страница Main

Главная страница отображает суммарную информацию о состоянии линка, текущие значения основных параметров конфигурации (в зависимости от режима работы), информацию о сети и ее параметры, статистику всех интерфейсов.

2.3.1. Status

Device Name: отображает настраиваемое имя (ID) устройства на базе AirOS v5.3 . Имя устройства (имя хоста) идентифицирует точку доступа при взаимодействии с другими сетевыми устройствами.



Network Mode: отображает сетевой режим в котором работает устройство. AirOS v5.3 обеспечивает устройствам поддержку режима моста, маршрутизатора и SOHO маршрутизатора . Режим работы устройства может быть изменен на странице **Network** .

Wireless Mode: Показывает режим работы радио-интерфейса . AirOS v5.3 обеспечивает устройствам поддержку инфраструктуры беспроводных сетевых решений. Беспроводной режим устройства может быть изменен на странице **Wireless** . Есть пять беспроводных режимов: Station, Station WDS, Access Point, Access Point WDS и Spectral Analyzer (спектральный анализатор AirView). Первые четыре настраиваются на странице **Wireless** . Режим спектрального анализатора может быть выбран, нажав на меню **Tools** (Инструменты), а затем опцию **AirView** . Когда устройство работает в режиме спектрального анализатора, все беспроводные соединения будут прекращены до тех пор, пока **AirView** работает. Закрытие окна **AirView** вернет устройство в прежний режим работы радио-интерфейса.

Все устройства М-серии могут работать только в одном из этих режимов, т.е. если устройство работает в режиме Access Point WDS, то все остальные режимы недоступны .

AirView Status: отображает состояние **AirView** во время работы в режиме спектрального анализатора. Когда точка доступа работает в режиме **AirView** , отображается статус "**Active**". В случае, если вы закроете окно **AirView**, статус изменится на " Switching back to Station " (если до этого точка доступа работала в режиме "Station "), и через несколько секунд, беспроводной режим

изменится.

SSID: идентификатор беспроводной сети (устанавливается на базовой станции и присваивается подключенным клиентам).

При работе точки доступа в режиме **Station**, отображает SSID базовой станции к которой подключен клиент .

При работе в режиме **Access Point**, отображает SSID базовой станции под управлением AirOS v5.3 .

Security: отображает текущие настройки безопасности. "None " значение отображается, если безопасность беспроводной сети отключена. WPA или WPA2 значения отображаются, если соответствующие методы защиты беспроводных сетей используются. Более подробная информация представлена в разделе Wireless.

Version : показывает текущую версию прошивки. Прошивка устройства может быть обновлена на странице System.

Version: v5.3
Uptime: 00:07:30
Date: 2011-01-14 14:49:27

Uptime: показывает общее время работы устройства от момента включения (перезагрузки) или обновления программного обеспечения.

Date : отображает текущую дату и время системы, в виде "год-месяц-день час:мин:сек". Точная дата и время системы извлекаются из Интернет с использованием NTP (Network Time Protocol). Системная дата и время будут неправильные после каждой перезагрузки устройства, если NTP не включен, поскольку большинство из AirOS устройств не имеют автономного питания для внутренних часов.

Channel/Frequency: Это рабочая частота на которой работают базовые станции и клиентские точки доступа. Номер канала соответствует рабочей частоте. Более подробная информация о поддерживаемых каналах содержится в разделе Wireless. Устройства используют указанную радиочастоту для передачи и приема данных. Доступный диапазон частот (каналов) зависит от местного законодательства страны.

Channel/Frequency: 11 / 2462 MHz
Channel Width: 40 MHz (Lower)

Channel Width: это ширина спектра радио канала, используемая в устройстве AirOS v5.3 . Поддерживаются следующие значения ширины спектра канала 5, 10, 20 и 40 МГц . В режиме Station (или Station WDS) по умолчанию устанавливается значение Auto 20/40MHz .

ACK Timeout : отображает текущее значение тайм-аут для ACK кадров. ACK Timeout может быть установлен вручную или настраивается автоматически системой. ACK Timeout (время подтверждения доставки фрейма) определяет, как долго устройство AirOS должно ожидать подтверждения от сопряженного устройства пакета подтверждающего доставку прежде чем признать пересылку ошибочной и требовать повторной передачи. ACK Timeout является очень важным параметром производительности для беспроводной передачи данных. При использовании стандарта 802.11n, рекомендуется установить "Auto adjust" для ACK Timeout. Более подробная информация приводится в разделе Advanced Wireless Setting на странице Advanced.

ACK/Distance: 35 / 0.7 miles (1.2 km)
TX/RX Chains: 2X2

TX/RX Chains: отображает число независимых пространственных потоков данных AirOS v5.3 устройства одновременной приема/передачи в пределах ширины спектрального канала . Эта способность является специфической для 802.11n устройств, которая основана на технологии множественного приема и множественной передачи (MIMO). Несколько цепей передачи данных существенно увеличивают производительность. Количество цепей различается в разных аппаратных моделях устройств Ubiquiti . Каждая цепочка передачи/приема требует отдельной антенны. Bullet устройства M серии используют 1 цепь для передачи/приема (1x1). Nano/LoCo M

серии и Rocket M серии используют 2 цепи для передачи/приема (2x2).

WLAN MAC: показывает MAC-адрес WLAN (Wireless) интерфейса AirOS v5.3 устройства.

WLAN MAC: 00:15:6D:00:05:40
LAN MAC: 00:AA:BB:CC:DD:EE

LAN MAC: показывает MAC-адрес LAN (Ethernet) интерфейса AirOS v5.3 устройства .

LAN1/LAN2: показывает текущее состояние Ethernet порта(ов) связи. Это может предупредить системного администратора , что сетевой кабель не подключен к устройству и нет активного подключения к Ethernet. Если кабель подключен, будет отображаться текущая скорость передачи данных , возможные значения 10 Мбит/с или 100 Мбит/с, полудуплекс или полный дуплекс.


LAN1/LAN2: 100Mbps-Full / Unplugged

AP MAC: показывает MAC-адрес точки доступа, с которой устройство связаны во время работы в режиме Station (или Station WDS). Это собственный MAC-адрес беспроводного интерфейса устройства при работе в режиме точки доступа. AP MAC используется в качестве Basic Service Set Identifier (BSSID) в инфраструктуре беспроводных сетей.

AP MAC: 00:15:6D:00:05:40
Connections: 1

Connections: отображает количество связанных беспроводных клиентов во время работы устройства в режиме точки доступа. Это значение не отображается во время работы в режиме Station.

Signal Strength: отображает полученный беспроводной уровень сигнала (на стороне клиента) во время работы в режиме Station. Представленное значение совпадает с графической полосой. Используйте инструмент "antenna alignment tool" для настройки устройства антенны, чтобы получить лучшую связь с беспроводным устройством. Антенна беспроводного клиента должна быть скорректирована так, чтобы получить максимальный уровень сигнала. Сила сигнала измеряется в дБм (децибелах на 1 милливатт). Соотношение вычисляется как $\text{дБм} = 10 \log_{10} (P/1\text{mW})$. То есть, 0дБм будет 1 мВт и -72дБм будет 0,0000006 мВт. Сигнал -80дБм или лучше (от -50 до -70) рекомендуется для стабильной связи.

Signal Strength:  -64 dBm
Noise Floor: -96 dBm
Transmit CCQ: 100 %
TX/RX Rate: 150.0 Mbps / 150.0 Mbps



Horizontal/Vertical: отображает уровень беспроводного сигнала, принимаемого для каждой полярности, во время работы Station (или Station WDS) режиме MIMO 2x2 устройств. Сила сигнала измеряется в дБм.

Noise Floor: отображает текущее значение уровня шума в дБм. Уровень шума рассматривается при оценке качества сигнала (сигнал-шум SNR, RSSI), его значение определяет отношение силы сигнала к уровню шума.

Transmit CCQ : это индекс, который оценивает качество беспроводного соединения клиента. Значение измеряется в процентах, где 100% соответствует идеальному состоянию линка .

TX Rate and RX Rate : отображает текущую 802,11 скорость передачи данных (TX) и приема данных (RX) при работе в режиме Station. Скорость передачи данных составляет до 150 Мбит/с для 1-чейновых устройств (Bullet M серии) и до 300 Мбит/с для 2-чейновых устройств (NanoStation/LocoStation M и Rocket-M серии). Самые высокие значения обеспечивают максимальную пропускную способность при достаточном уровне сигнала .

Airmax: Показывает текущее состояние AirMax (фирменная технология Ubiquiti TDMA поллинга) . Если AirMax включен, то базовая станция принимает только AirMax клиентские станции. (Отключите AirMax для обратной совместимости с 802.11abg устройствами).

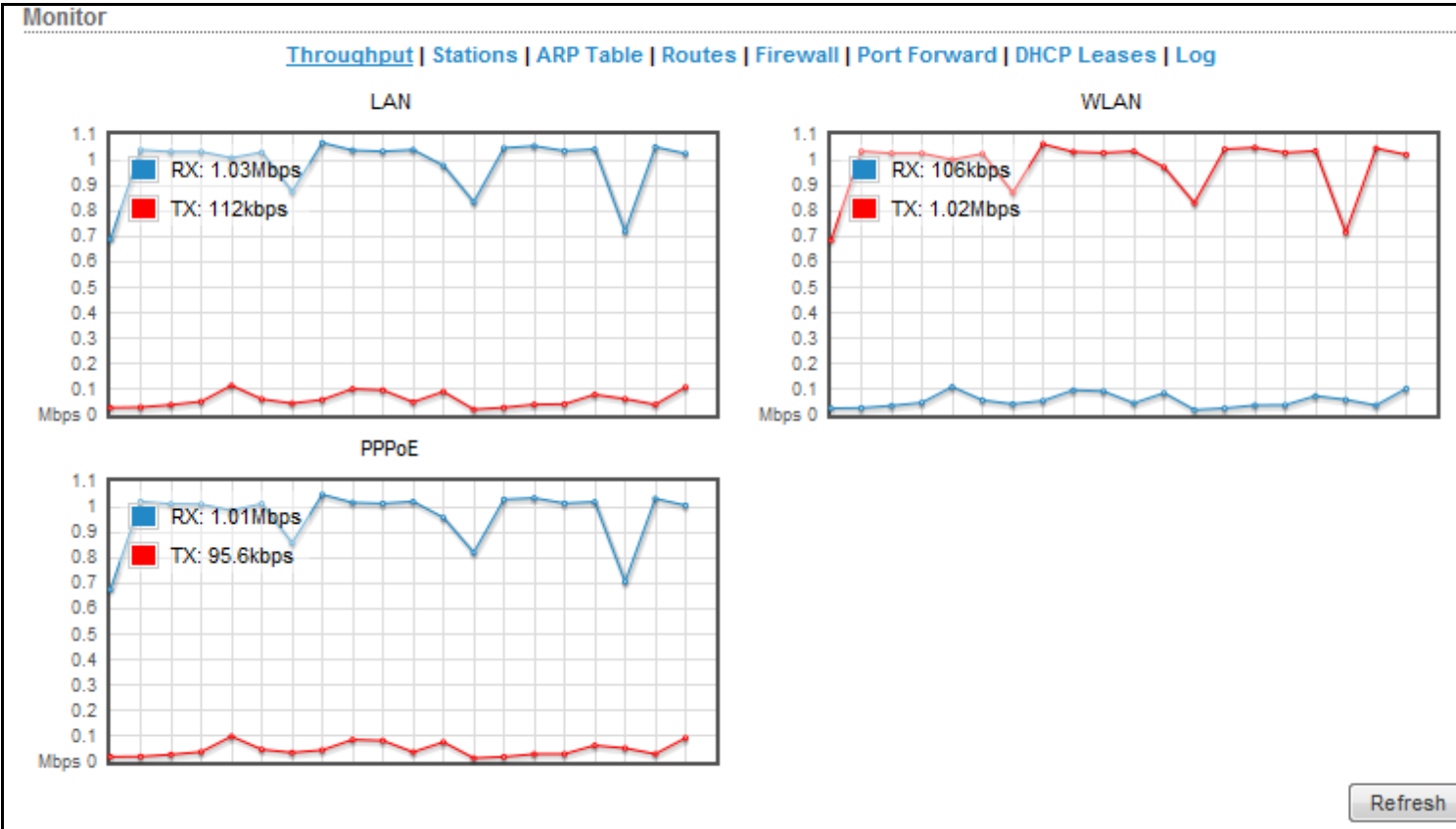
AirMax: Enabled
AirMax Quality:  99 %
AirMax Capacity:  98 %

Airmax Quality : это индекс, который вычисляет качество связи AirMax. Значение измеряется в процентах, где 100% соответствует идеальному состоянию линка .

Airmax Capacity : это показатель максимальной скорости передачи данных для линка . Маленькое значение указывает на то, что устройство не сможет развить максимальную скорость .

2.3.2. Monitor

Throughput: отображает графики, которые в реальном времени представляют текущие данные о трафике на LAN, WLAN и PPPoE интерфейсах как в графическом так и в цифровом формате. Масштаб графика и единица измерения пропускной способности (б/с, Кбит/с, Мбит/с) динамически изменяется в зависимости от среднего значения пропускной способности. Статистика обновляется автоматически. Статистика может быть обновлена вручную, используя кнопку "Refresh".



Stations: отображает список станций, которые связаны с устройством во время работы в режиме Access Point (или Access Point WDS).

Throughput Stations ARP Table Bridge Table Log								
Station MAC	Device Name	Signal / Noise, dBm	ACK	TX/RX, Mbps	CCQ, %	Connection Time	Last IP	Action
00:15:6D:AD:8A:01	CPE_AD8A01	-49 / -90	37	54 / 2	100	1 day 03:58:20	192.168.0.12	kick
00:15:6D:AD:8A:08	CPE_AD8A08	-49 / -90	37	54 / 2	100	01:52:25	192.168.0.89	kick

Для каждого клиентского устройства отображается следующая информация :

- **Station MAC** - MAC адрес связанного устройства ;
- Device Name**: отображает имя хоста клиентского устройства ;
- Signal/Noise, dBm**: уровень сигнала / шума полученного от клиента;
- ACK**: эти значения указывают ACK Timeout и соответствующее расстояние до станции.
- Tx/Rx, Mbps**: значение Tx представляет скорость передачи данных в Мбит/с , а Rx значение скорость приема данных в Мбит/с ;

CCQ,%: это индекс, который оценивает качество связи беспроводного клиента.

Connection time: это значение представляет общее время работы станции, связанной с AP.

Last IP: отображает IP-адрес станции, связанной с AP.

Action: показывает доступные действия для этой станции, например: дисконнект на нескольких секунд, для диагностики проблемных станций.

Информацию, отображаемую в блоке **Stations** можно обновить с помощью кнопки "Refresh".

Более подробную информацию о каждой присоединенной станции можно получить нажав на ее MAC адрес:

UBNT: [NanoStation M2] - Station Info: 00:15:6D:72:42:19

http://192.168.1.21/stainfo.cgi?ifname=ath0&sta_mac=00:15:6D:72:42:19

Station	00:15:6D:72:42:19	[1]
Device Name: UBNT	Negotiated Rate Last Signal, dBm	
Connection Time: 00:00:50	MCS0	N/A
Signal Strength: -32 dBm	MCS1	N/A
Noise Floor: -88 dBm	MCS2	N/A
ACK/Distance: 34 / 0.7 miles (1.1 km)	MCS3	N/A
CCQ: 100%	MCS4	N/A
AirMax Priority: High	MCS5	N/A
AirMax Quality: 86%	MCS6	N/A
AirMax Capacity: 55%	MCS7	N/A
Last IP: 192.168.1.20	MCS8	N/A
TX/RX Rate: 78.0 Mbps / 78.0 Mbps	MCS9	N/A
TX/RX Packets: 4360 / 4399	MCS10	N/A
TX/RX Packet Rate, pps: 14 / 12	MCS11	-30
Bytes Transmitted: 1733006 (1.65 MBytes)	MCS12	-34
Bytes Received: 1884638 (1.80 MBytes)	MCS13	N/A
	MCS14	N/A
	MCS15	N/A

Kick Refresh Close

Terminado

Информация, содержащаяся в окне "Station info" обновляется автоматически, ее также можно обновить в любой момент кнопкой "Refresh".

AP Information: выбор этого пункта открывает окно статистики связи во время работы в режиме **Station**.

Чтобы переподключиться к базовой станции (AP) нажмите кнопку "Reconnect", данную информацию также можно обновить в любой момент кнопкой "Refresh".

Throughput AP Information ARP Table Bridge Table Routes Log			
Access Point 00:15:6D:72:42:2C			
Device Name: UBNT		Negotiated Rate	Last Signal, dBm
Connection Time: 00:01:01		MCS0	N/A
Signal Strength: -48 dBm		MCS1	N/A
Noise Floor: -89 dBm		MCS2	N/A
ACK/Distance: 34 / 0.7 miles (1.1 km)		MCS3	N/A
CCQ: 100%		MCS4	N/A
Last IP: 192.168.1.21		MCS5	N/A
TX/RX Rate: 78.0 Mbps / 78.0 Mbps		MCS6	N/A
TX/RX Rate: 5534 / 5534		MCS7	N/A

DHCP Client :
(Применимо для режима Router - при включенном DHCP) показывает служебную информацию - IP-адрес WAN интерфейса , маску, DNS-серверов и шлюза во время работы в режиме DHCP Router .

Throughput AP Information DHCP Client ARP Table Routes Port Forward DHCP Leases Log			
DHCP Client Information			
IP Address: 192.168.0.91		DHCP Server: 192.168.0.1	
Netmask: 255.255.255.0		Domain:	
Gateway: 192.168.0.1		Total Lease Time: 10:00:00	
Primary DNS IP: 192.168.0.1		Remaining Lease Time: 09:55:42	
Secondary DNS IP: 192.168.0.1			
		Renew Release Refresh	
		Reconnect Refresh	

ARP Table : отображает список всех элементов ARP (Address Resolution Protocol) таблицы, зафиксированных устройством .

Список можно обновить с помощью кнопки Refresh.

ARP используется для связи каждого IP-адреса в уникальным аппаратным адресом (MAC) устройств. Важно иметь уникальные адреса IP для каждого MAC иначе будут неоднозначные маршруты в сети.

Bridge Table : отображает список всех записей в системной таблице "мост" , во время работы устройства в режиме "Bridge".

Список можно обновить в любой момент кнопкой "Refresh" .

Таблица "мост" отображает к какому порту бриджа привязан клиент , другими словами, через какой интерфейс (Ethernet или беспроводной) сетевое клиентское устройство (с соответствующим адресом MAC) обменивается пакетами с системой AirOS (это предотвращает избыточную передачу данных).

Throughput Stations ARP Table Bridge Table Routes Log			
IP Address	MAC Address	Interface	
192.168.0.49	00:0C:76:F5:86:27	BRIDGE	
192.168.0.69	00:25:00:41:26:85	BRIDGE	
192.168.0.1	00:09:A3:00:4B:8E	BRIDGE	
192.168.0.67	00:18:39:98:D4:8A	BRIDGE	
192.168.0.6	00:0D:87:BB:86:E5	BRIDGE	
			Refresh

"Ageing timer" показывает время старения для каждой записи (в секундах) - если в течении этого времени не было обмена данными со станцией с данным MAC адресом, запись удаляется из таблицы "мост".

Routes: отображает все записи в системной таблице маршрутизации, при работе устройства в режиме "Router".

Список можно обновить в любой момент кнопкой "Refresh".

Throughput Stations ARP Table Bridge Table Routes Log			
Destination	Gateway	Netmask	Interface
192.168.0.0	0.0.0.0	255.255.255.0	BRIDGE
169.254.0.0	0.0.0.0	255.255.0.0	BRIDGE
0.0.0.0	192.168.0.200	0.0.0.0	BRIDGE
			Refresh

AirOS анализирует IP адрес назначения каждого пакета данных, проходящего через систему, и выбирает подходящий интерфейс для пересылки пакета. Выбор системы зависит от правил статических маршрутов, которые зарегистрированы в системной таблице маршрутизации. Статические маршруты для определенных хостов, сетей или шлюзов по умолчанию устанавливаются автоматически в зависимости от конфигурации IP всех интерфейсов системы AirOS.

Firewall: во время работы устройства в режиме "Bridge", отображает список правил в цепочке брандмауэра, согласно стандарта таблицы фильтров [ebtables](#).

Во время работы устройства в режиме "Router", отображает список правил в цепочке брандмауэра, согласно стандарта таблицы фильтров [iptables](#).

Список можно обновить в любой момент кнопкой "Refresh".

IP и MAC-уровень контроля доступа и фильтрации пакетов в AirOS реализуется с помощью iptables (routing) и ebtables (bridging) брандмауэра, который защищает ресурсы частной сети от внешних угроз путем предотвращения несанкционированного доступа и фильтрации нежелательных соединений.

Более подробная информация представлена в разделе Wireless.

Port Forward : отображает список активных записей в цепочке PortForward из таблицы NAT стандарта Iptables, во время работы устройства работает в режиме "Router". Список можно обновить в любой момент кнопкой "Refresh".

Port Forwarding создает прозрачный туннель через брандмауэр или NAT, это делает доступными через WAN интерфейс частные сетевые сервисы, работающие на стороне LAN.

DHCP Leases : показывает текущее состояние арендованных адресов IP от DHCP-сервера. Эта опция доступна, если DHCP-сервер включен, когда устройство работает в режиме **Router**.

Throughput AP Information DHCP Client ARP Table Routes Port Forward DHCP Leases Log				
MAC Address	IP Address	Remaining Lease	Hostname	Interface
00:25:4B:A9:7B:5A	192.168.4.143	00:55:32		LAN
				Refresh

"MAC address" показывает MAC-адрес клиента, который подключен к точке доступа.

"IP address" показывает IP-адрес клиента аренду DHCP-сервер устройства.

"Remaining Lease time" показывает, как долго арендованный IP-адрес будет действительным и зарезервирован для конкретного клиента DHCP.

"*Hostname*": отображает имя устройства (хоста) клиента получающего аренду IP.

"*Interface*" показывает через какой интерфейс связан DHCP клиент с указанным MAC-адресом.

Список можно обновить в любой момент кнопкой "**Refresh**".

Более подробная информация представлена в разделе *Wireless*.

Log показывает список всех событий, зарегистрированных системой.

Кнопкой "Clear" можно очистить системный журнал. Кнопкой "Refresh" можно в любой момент обновить содержимое системного журнала.

Если системный журнал отключен, то выводится сообщение "Syslog is disabled, unable to show system messages".

Настройка системного журнала описана в разделе *Services*.

2.4. Страница *Wireless*

Страница *Wireless* содержит все необходимые оператору настройки для беспроводной части. Такие как нормативные требования, SSID, канал и частоты, режим работы устройства, скорость передачи данных и беспроводная безопасность.

The screenshot shows the configuration interface for a Ubiquiti Bullet M2 device running AirOS. The top navigation bar includes tabs for MAIN, WIRELESS (selected), NETWORK, ADVANCED, SERVICES, and SYSTEM. A 'Tools' dropdown and a 'Logout' button are also present. The main content area is titled 'Basic Wireless Settings' and contains various configuration options:

- Wireless Mode:** Set to 'Access Point'.
- SSID:** Set to 'Ubiquiti'. There is a 'Hide SSID' checkbox.
- Country Code:** Set to 'Chile'. There is a checked 'Obey Regulatory Rules' checkbox.
- IEEE 802.11 Mode:** Set to 'B/G/N mixed'.
- Channel Width:** Set to '20 MHz'.
- Channel Shifting:** Set to 'Disabled'.
- Frequency, MHz:** Set to '2447'.
- Extension Channel:** Set to 'None'.
- Frequency List, MHz:** A checkbox for 'Enabled' is present.
- Antenna Gain:** Set to '0 dBi'.
- Cable Loss:** Set to '0 dB'.
- Output Power:** A slider is shown, with a value of '12 dBm' displayed.
- Max TX Rate, Mbps:** Set to 'MCS 7 - 65'. There is a checked 'Automatic' checkbox.

Below the 'Basic Wireless Settings' section is the 'Wireless Security' section:

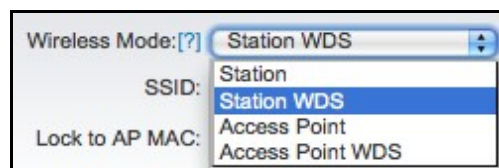
- Security:** Set to 'WPA2'.
- WPA Authentication:** Set to 'PSK'.
- WPA Preshared Key:** A field with masked characters (dots) and a 'Show' checkbox.
- MAC ACL:** A checkbox for 'Enabled' is present.

A 'Change' button is located at the bottom right of the configuration area. The footer of the page reads '© Copyright 2006-2011 Ubiquiti Networks, Inc.'

2.4.1. Basic Wireless Settings

Базовые беспроводные настройки, такие как идентификатор беспроводной сети SSID, код страны, выходная мощность, 802.11 режим и скорость передачи данных могут быть настроены в этом разделе.

Wireless Mode: определяет режим работы устройства. Режим зависит от требований топологии сети. Всего 4 режима поддерживается системой AirOS V5.3:



1. **Station:** Это режим клиента, который может подключиться к точке доступа. Он является общепринятым для подключения к базовой станции. В режиме *Station* устройства работают как абонентские станции при подключении к точке доступа в режиме *Access Point* с уникальным SSID, которая перенаправляет весь входящий/исходящий трафик на Ethernet интерфейс. Спецификой этого режима является то, что абонентская станция использует arpnat технологию, которая может привести к отсутствию прозрачности при прохождении широковещательных пакетов в режиме *bridge*.

2. **Station WDS:** WDS расшифровывается как Wireless Distribution System. Режим *Station WDS* должен использоваться при подключении к базовой станции, которая работает в режиме *Access Point WDS*. Этот режим совместим с WPA/WPA2 шифрованием. Режим *Station WDS* позволяет пересылку пакетов на *layer2* уровне. Преимущество режима *Station WDS* в улучшенной производительности и более высокой пропускной способности. Режим *Station WDS - Bridge* является полностью прозрачным для всех *Layer2* протоколов.

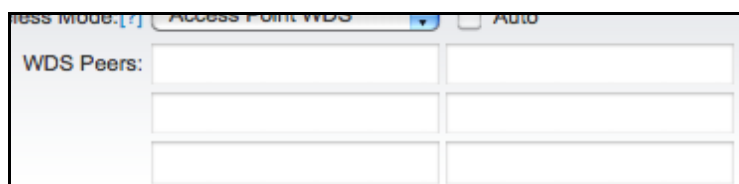
3. **Access Point:** Это точка доступа согласно стандарта 802.11 (Базовая станция).

4. **Access Point WDS:** Это 802.11 точка доступа, которая позволяет организовать прозрачный мост *layer2* уровня со станцией в режиме *Station WDS* с использованием протокола WDS. Режим *Access Point WDS* не полностью совместим с WPA/WPA2 шифрованием. WDS режим также позволяет реализовать беспроводной мост для обмена трафиком между устройствами, которые работают в режиме *Access Point WDS*. Точка доступа в режиме *Access Point WDS* обычно подключается к проводной сети (Ethernet LAN), чтобы организовать беспроводное подключение к ресурсам сети. При подключении беспроводных базовых станций друг к другу с использованием WDS, их порты Ethernet могут быть объединены мостом в один порт LAN. Очень важно следить, чтобы не создать в сети петлю, при использовании мостов WDS или комбинации проводной (Ethernet) соединений и WDS мостов. Нужно использовать древовидную или звездообразную топологию сети при создании WDS мостов (например, если AP2 и AP3 указаны как повторители WDS станции AP1, то AP2 не должна быть указана как повторитель WDS станции AP3, и AP3 не должно быть указано как WDS повторитель AP2 в любом случае). Топологии Mesh (сеть) и Ring (кольцо) не поддерживают WDS, это надо учитывать при построении сети с использованием данных топологий.

Примечание: Важно знать, что протокол WDS, не определен как стандарт, поэтому должен быть использован только с устройствами, поддерживающими режимы *Station WDS* и *Access Point WDS*, при использовании WDS с оборудованием сторонних производителей могут возникнуть проблемы с совместимостью.

Примечание: При подключении устройства в режиме AP-WDS к AP-WDS, WPA/WPA2 метод безопасности не будет работать, используйте либо WEP шифрование либо вообще отключите шифрование (что не рекомендуется, т.к. это может поставить под угрозу безопасность вашей сети). В случае подключения STA-WDS клиентов к устройству AP-WDS, все методы защиты доступны и работают нормально.

WDS Peers: WDS станции и/или WDS базовые станции, подключенные к базовой станции WDS под управлением AirOS




должны быть указаны в этом списке в целях создания инфраструктуры беспроводных сетей - Wireless Distribution System (применяется только в режиме AP WDS).

Введите MAC-адреса сопряженных WDS устройства в поле ввода *WDS Peers*. Один MAC-адрес должен быть указан для режима соединения точка-точка, до шести сопряженных WDS могут быть указаны для использования случае соединения точка-многоточка .

Опция **Auto** должна быть включена для того, чтобы установить WDS связь между точками доступа, если *WDS peers* не указаны (применимо только в режиме AP WDS). Если опция *Auto* включена, точки доступа будут выбирать WDS пиров (точки доступа) в соответствии с настройкой SSID. Точка доступа работающая в режиме WDS должна иметь такой же SSID как WDS Peer для того, чтобы автоматически установить связь при включенной опции *Auto* . Данная конфигурация также известна как репитер (повторитель, ретранслятор. Эта опция также не совместима с WPA или WPA2 режимами безопасности .

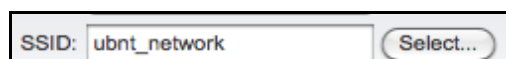
Примечание: Базовая станция, работающая в режиме WDS и все WDS пиры должны работать на одной частоте , при одинаковой ширине спектра канала и при одинаковых настройках безопасности.

SSID: Service Set Identifier используется для идентификации 802.11 беспроводной локальной сети, устанавливается в режиме *Access Point* или *Access Point WDS* . Все клиентские устройства, сопряженные с базовой станцией, будут получать широковещательные сообщения от точки доступа с данным SSID. Также допускается несколько базовых станций с одинаковыми SSID.



Hide SSID отключит вещание SSID базовой станцией . И наоборот сделает видимым SSID во время сканирования сети . Данный пункт доступен только при работе в режиме *Access point* .

В режиме работы *Station* или *Station WDS* вы должны указать SSID базовой станции, к которой должны подключаться клиентские точки доступа.



Примечание: Если в SSID задать значение "**Any**", то станция будет подключаться к любой доступной базе.

Список доступных точек доступа можно получить с помощью кнопки "**Select**" (не относится к режиму *Access Point*), она открывает доступ к утилите "**Site Survey**", которая используется для выбора подходящей точки доступа. Site Survey будет искать все доступные беспроводные сети в диапазоне поддерживаемых каналов и позволит вам выбрать одну для подключения к ней. В случае если в выбранной сети используется шифрование, то вы должны будете установить параметры безопасности в разделе Безопасность беспроводных сетей. Выберите точку доступа из списка и нажмите кнопку "**Select**" для подключения к ней .

Нажмите кнопку "**Scan**", чтобы обновить список доступных беспроводных сетей. Список сканируемых каналов может быть изменен с помощью пункта *Channel Scan List*.

Hide SSID позволит скрыть SSID точки доступа (идентификатор сети) от беспроводных станций при сканировании доступных сетей. При отключенной опции - SSID будет виден во время сканирования беспроводных сетей. Эта функция доступна только в режиме работы точки доступа (*Acess Point*).



Lock to AP MAC : устанавливается на клиентской точке доступа *Station* и *Station WDS*, если есть несколько базовых станций с одинаковым именем SSID, и нужно подключиться к одной из них с заданным MAC адресом, чтобы избежать от автоматического перескакивания на другую базу с таким же SSID.



Country Code: Разные страны мира имеют различные ограничения в использовании уровня мощности и выбора частот для беспроводных сетей. Для того, чтобы убедиться, что устройство работает согласно всем нормативным актам, убедитесь в том, что правильно выбрали страну, где планируется использовать это устройство. Список каналов, ограничение выходной мощности, IEEE 802.11 стандарт и ширина спектра канала будут установлены согласно нормативам выбранной страны. Таблица соответствия частот стран мира доступна по [адресу](#).

IEEE 802.11 mode: выбор радиостандарта, используемого для работы устройства под управлением AirOS. 802.11b, 802.11a and 802.11g - устаревшие режимы работы, при используемой частоте 2,4ГГц; 802.11n - более новый стандарт, основанный на более быстром алгоритме ортогонального частотного разделения каналов с мультиплексированием (OFDM), которое подходит как и к 2,4ГГц так и для 5ГГц диапазона.



Country Code: Chile
IEEE 802.11 Mode: B/G/N mixed

Используемые стандарты:

A/N mixed используется для подключения к сетям по стандартам 802.11a или 802.11n. Поддерживающие устройства серии: M900, M5, M3 и M365.

B/G/N mixed используется для подключения к сетям по стандартам 802.11b, 802.11g или 802.11n. Поддерживающие устройства серии: M2.

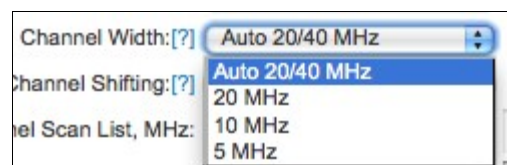
Channel Width: эта ширина спектра канала. Поддерживаемая ширина спектра канала:

5MHz - спектр канала с шириной 5МГц

10MHz – спектр канала с шириной 10МГц

20MHz - спектр канала с шириной 20МГц (установлен по умолчанию)

40MHz - спектр канала с шириной 40МГц



Channel Width: Auto 20/40 MHz
Channel Shifting: Auto 20/40 MHz
Channel Scan List, MHz: 20 MHz, 10 MHz, 5 MHz

Auto 20MHz/40MHz - доступно только в режиме Station (или Station WDS). Обеспечивает улучшенную совместимость.

Уменьшение ширины спектра обеспечивает 2 преимущества и 1 недостаток:

+ увеличит список непересекающихся каналов, что облегчает масштабируемость сети;

+ увеличивает спектральную плотность мощности канала и позволяет увеличить расстояние соединения;

- уменьшает пропускную способность пропорционально сокращению ширины спектра. То есть, если турбо режим (40MHz) увеличивает максимальную скорость соединения вдвое, то режим 10MHz - сократит ее в два раза.

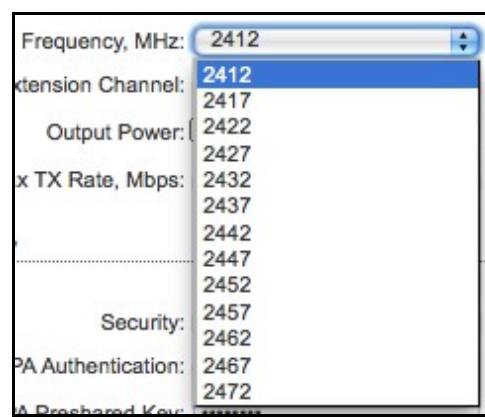
Channel Shifting: позволяет сместить частоту канала относительно стандартной для протоколов 802.11b/g/n и 802.11a. Эта функция является собственной разработкой Ubiquiti. В то время как сети стандарта 802.11 работают на стандартных каналах, например, Channel 36 (5180МГц), Channel 40 (5200МГц) и т.д., с интервалом в 5МГц, channel shifting позволяет работать на новых, смещенных относительно стандартных каналах. Смещены могут быть все каналы относительно стандартной частоты основного канала в интервале 5МГц (802.11na) или 2/3МГц (802.11bgn).



Channel Shifting: Disabled
Frequency, MHz: Disabled, Enabled

Преимущества данной функции это существенное увеличение безопасности сети. Используя channel-shifting, сети могут по настоящему становиться невидимыми для миллионов Wi-Fi устройств во всем мире.

Frequency, MHz: выбор беспроводного канала в режиме работы



Frequency, MHz: 2412
Extension Channel: 2412, 2417, 2422, 2427
Output Power: 2432, 2437, 2442, 2447, 2452, 2457, 2462, 2467, 2472
Security: 2472
PA Authentication: 2472
A Prepared Key: 2472

Access Point. На выбор доступно множество частот для избежания воздействия помех от рядом стоящих точек доступа. Список каналов может отличаться в зависимости от выбранной страны, стандарта IEEE 802.11, ширины спектра канала и опции Channel Shifting. Сейчас AirOS 5.3 включает в себя опцию "Auto", которая выбирает канал основываясь на текущем использовании и уровне шума на момент включения или перезагрузки устройства. После выбора канала он будет использоваться до тех пор пока устройство не будет перезагружено или не будут внесены дополнительные изменения в настройки.

Extension Channel: (применимо только в режиме AP или AP WDS, при ширине канала 40МГц) указывает использование канала в связке позволяющего AirMax использовать два канала одновременно. Использование двух каналов позволяет увеличить производительность Wi-Fi соединения. Канал выбирается системой автоматически.



Channel Scan List, MHz: эта функция ограничивает сканирование только выбранными каналами (применимо только в режиме Station и Station WDS). Эта функция значительно ускоряет сканирование путем фильтрации не нужных точек доступа в результатах. Site Survey будет искать точки доступа только на выбранных каналах.

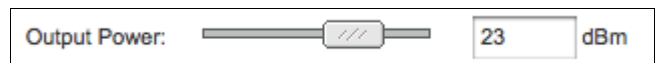
Frequency List, MHz: будучи активированной, эта опция может быть использована в двух случаях: в первую очередь, если частота установлена в режим "Auto", сканироваться и анализироваться будут только перечисленные в списке частоты (список значений может быть в ручную введен через запятую или выбраны через функцию "Edit"). Во-вторых при запуске AirSelect, будут использованы только те каналы которые указаны в списке.

Управлять списком каналов для выбранного режима IEEE 802.11 и ширины спектра можно только если функция включена. Есть два способа установить список каналов: перечислив нужные каналы через запятую в поле ввода или выбрать нужные каналы в окне Channel Scan List, которое открывается при нажатии на кнопку **Edit**. Утилита Site Survey будет искать точки доступа только на заданных каналах только если поиск или site survey запущен в режиме *Station*.

Antenna Gain: определяет усиление антенны точки доступа (применяется только для устройств с подключением к внешней антенне, таких как Rocket и Bullet). Когда опция "Obey Regulatory Rules" включена, усиление антенны вычисляет мощность передатчика для соответствия местным нормативным актам. Эта опция аналогична функции "Cable Loss" и так же влияет на мощность передатчика устройства.

Cable Loss: если функция "Obey Regulatory Rules" включена, Cable Loss влияет на мощность передатчика устройства. В случае если у вас большие потери при передаче сигнала по проводам, максимальная мощность передатчика может быть увеличена вплоть до максимально допустимой, разрешенной местными властями. Эта функция аналогична "Antenna Gain".

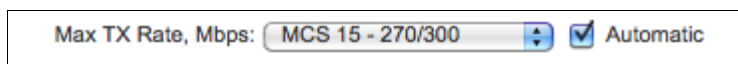
Output Power: эта функция устанавливает максимальный уровень мощности (в dBm) беспроводного устройства. Выходная мощность каждого беспроводного модуля может регулироваться при помощи этого слайдера. При вводе значения мощности вручную, слайдер автоматически устанавливается в нужном положении. Максимальная мощность ограничивается согласно местным нормативным актам. В случае использования устройства со встроенной антенной (например, NanoStation M/LocoStation M), функция регулирует выходную мощность подаваемую на встроенную антенну.



Obey regulatory Rules: эта функция должна оставаться включенной для принудительной установки выходной мощности передатчика для соответствия нормам выбранной страны. В этом случае будет невозможно установить эквивалентную изотропно-излучаемую мощность (EIRP) выше значения разрешенного нормативами региона (в отличие от максимальной выходной мощности и усиления

антенны допустимых для стандартов IEEE 802.11a/b/g/n).

Max Data Rate, Mbps: эта функция устанавливает скорость передачи данных (в Mbps) с которой устройство должно передавать беспроводные пакеты. Так же вы можете установить определенную скорость между MCS 0 и MCS 7 (или MCS15 при соединении устройств с поддержкой функции 2x2). Рекомендуется использовать функцию "Automatic", особенно если у вас возникают трудности при соединении или потери данных на высокой скорости. В этом случае устройство будет автоматически использовать более низкую скорость передачи. Если вы установите ширину спектра канала на 20МГц то максимальная скорость передачи данных будет равна MCS7 (65Mbps) или MCS15 (130Mbps). Если вы установите ширину спектра канала на 40МГц то максимальная скорость передачи данных будет равна MCS7 (150Mbps) или MCS15 (300Mbps).



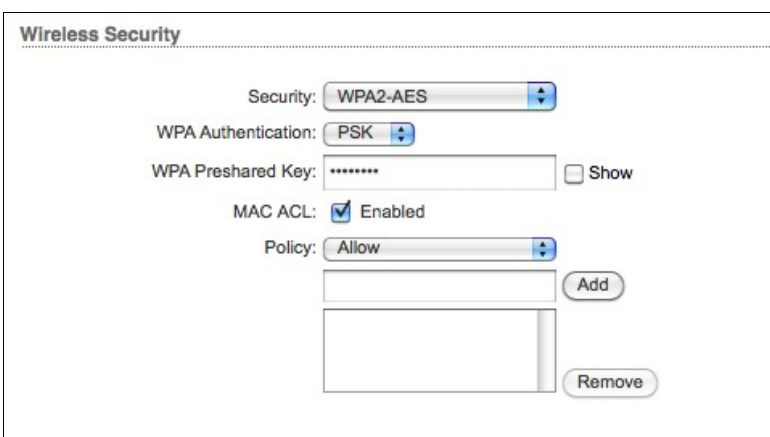
Примечание: Если вы устанавливаете режим шифрования WEP, WPA-TKIP или WPA2-TKIP, максимальная скорость передачи будет MCS12. Это аппаратное ограничение. Если необходимо увеличить скорость передачи, используйте WPA-AES или WPA2-AES.

Automatic: если функция включена, скоростной алгоритм будет выбирать наилучшую скорость передачи, в зависимости от качества соединения. Рекомендуется использовать эту функцию особенно если у вас возникают трудности при соединении или потери данных на высокой скорости. Перейдите к разделу *Advanced* для получения более подробной информации о скоростных алгоритмах.

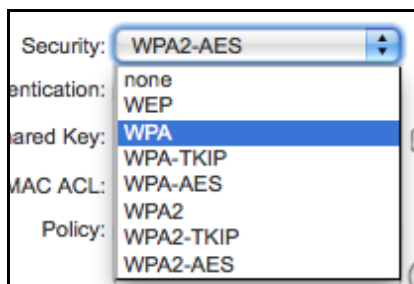
2.4.2. Wireless Security

Этот раздел расскажет вам о том как настроить параметры которые контролируют то как абонентская точка будет подключаться к базовой станции и шифровать/дешифровать данные.

Установите алгоритм безопасности клиентского устройства аналогичный алгоритму используемому базовой станцией. Пользовательская станция должна быть авторизована точкой доступа для получения доступа в сеть, все передаваемые данные будут зашифрованы с применением выбранного алгоритма.



Security:
AirOS



поддерживает режимы шифрования none(без шифрования), WEP, WPA и WPA2. Выберите метод шифрования используемый в вашей беспроводной сети:

WEP (Wired Equivalent Privacy) - метод шифрования основанный на стандарте IEEE 802.11 и использующий алгоритм шифрования RC4. Включение режима WEP позволяет увеличить безопасность передачи данных в беспроводных сетях. WEP самый старый алгоритм и есть несколько программ способный взломать его мене чем за 10 минут. Рекомендуется использовать методы шифрования WPA™/WPA2™ если возможно.

WPA (Wi-Fi Protected Access) - WPA™ (IEEE 802.11i/D3.0) и WPA2™ (IEEE 802.11i) - протоколы с применением общедоступного ключа, позволяют увеличить безопасность передачи данных, поскольку это новые протоколы созданные по стандарту 802.11i предназначенные для преодоления недостатков WEP.

WPA™ и WPA2™ поддерживают следующие шифры для зашифровки данных:

TKIP (Temporal Key Integrity Protocol) - использует алгоритм шифрования RC4.

AES (так же известен как CCMP) - протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счётчика, который использует алгоритм Advanced Encryption Standard (симметричный алгоритм блочного шифрования).

Устройство по умолчанию будет использовать самый надежный шифр (AES) как в режиме станции так и в режиме точки доступа. Если AES не поддерживается на другой стороне соединения, то будет использоваться шифр TKIP - как в случае если устройство работает в режиме точки доступа с использованием метода WPA и как минимум одна станция (не имеющая поддержки AES) подключена к ней.

WPA – включение режима шифрования WPA™.

WPA-TKIP – включение режима шифрования WPA™ с поддержкой только шифра TKIP.

WPA-AES – включение режима шифрования WPA™ с поддержкой только шифра AES.

WPA2 – enable WPA2™ security mode.

WPA2-TKIP – включение режима шифрования WPA2™ с поддержкой только шифра TKIP.

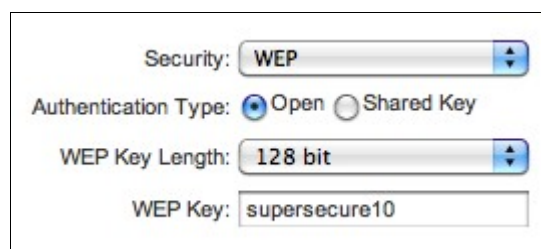
WPA2-AES – включение режима шифрования WPA2™ с поддержкой только шифра AES.

2.4.2.1 WEP

Authentication Type: доступно только при выборе режима безопасности WEP. В этом режиме необходимо выбрать один из режимов аутентификации:

Open Authentication (выбрано по умолчанию) – станция авторизуется точкой доступа автоматически

Shared Authentication – станция авторизуется по запросу генерируемому точкой доступа.



WEP Key Length: длина ключа WEP 64-bit (выбрано по умолчанию) или 128-bit. 128-ми битный ключ обеспечивает более высокий уровень защиты для вашей беспроводной сети.

Key Type: *HEX* (выбрано по умолчанию) или *ASCII*, эта опция определяет формат символов для WEP ключа, при использовании этого метода шифрования.

WEP Key: ключ для шифровки / дешифровки данных:

Для **64-bit** – установите WEP ключ в виде 10 HEX (0-9, A-F или a-f) символов (например, 00112233AA) или 5 ASCII символов.

Для **128-bit** – установите WEP ключ в виде 26 HEX (0-9, A-F или a-f) символов (например, 00112233445566778899AABBCC) или 13 ASCII символов.



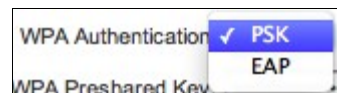
Key Index: позволяет установить индекс ключа WEP. Можно установить 4 различных ключа, но работать будет только один из них. Активный ключ устанавливается путем выбора индекса 1,2,3 или 4.

2.4.2.2 WPA/WPA2

WPA - AES – включение режима WPA™ с поддержкой только шифра AES. Протоколы безопасности "Wi-Fi Protected Access" - WPA™ (IEEE 802.11i/D3.0) с общедоступным ключом, являются улучшенными протоколами безопасности, поскольку это новые протоколы созданные по стандарту 802.11i с учетом всех слабых мест протокола WEP.

WPA2 - AES – включение режима WPA2™ с поддержкой только шифра AES. Протоколы безопасности "Wi-Fi Protected Access 2" - WPA2™ (IEEE 802.11i) с общедоступным ключом, являются улучшенными протоколами безопасности, поскольку это новые протоколы созданные по стандарту 802.11i с учетом всех слабых мест протокола WEP.

WPA Authentication: меню выбора одного из доступных методов WPA-ключа:



PSK – метод с применением общедоступного ключа для WPA™ или WPA2™ (выбрано по умолчанию).

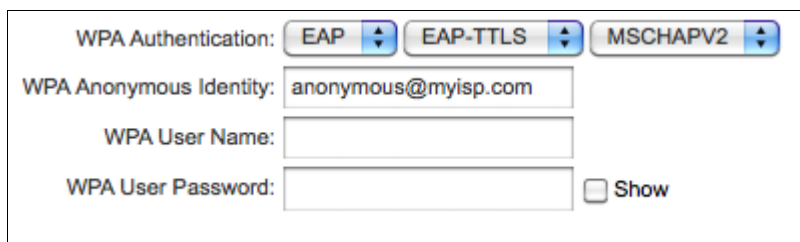
EAP – метод для WPA™ или WPA2™ с использованием EAP (Extensible Authentication Protocol - протокол расширенной проверки подлинности) - метод аутентификации разработанный по стандартам IEEE 802.1x. Этот метод обычно используется в сетях крупных предприятий.

WPA Pre-shared Key: пароль, который необходимо задать при использовании метода безопасности WPA™ или WPA2. Пароль может содержать от 8 до 63 знаков ASCII.



2.4.2.2.1 EAP Authentication - в режиме станции

WPA Identity: учетная запись используемая для аутентификации в режиме EAP (применимо только в режиме Station и Station WDS).



WPA User Name: учетная запись используемая в режиме EAP для туннельной аутентификации (EAP-TTLS) в нешифрованном виде (применимо только в режиме Station и Station WDS).

WPA User Password: пароль учетной записи для аутентификации в режиме EAP (применимо только в режиме Station и Station WDS).

2.4.2.2.2 EAP Authentication - в режиме точки доступа

Radius Server IP: IP адрес RADIUS-сервера. RADIUS - это сетевой протокол позволяющий организовать централизованное управление аутентификацией, авторизацией и системой аккаунтов для компьютеров в сети.



Radius Server Port: UDP порт RADIUS-сервера. Обычно используется порт 1812, но это зависит от RADIUS-сервера который вы используете.

Radius Server Secret: пароль RADIUS-сервера. Чувствительный к регистру текст, используемый для авторизации между двумя RADIUS-устройствами.

Примечание: При подключении устройства работающего в режиме AP-WDS к другому устройству в режиме AP-WDS, методы шифрования WPA/WPA2 не будут работать. Устройства будут использовать только WEP режим или работать без шифрования. Это может понизить безопасность в вашей сети. При подключении устройства работающего в режиме STA-WDS к устройству в режиме AP-WDS, все методы шифрования будут работать корректно.

2.4.2.3. MAC ACL

Максимальное число записей в списке MAC ACL, которое может быть введено посредством веб интерфейса AirOS v5.3, составляет 32 MAC адреса. Чтобы управлять большим количеством адресов доступа, нужно сохранить файл конфигурации устройства, отредактировать его в текстовом редакторе, загрузить на устройство и применить измененную конфигурацию (веб интерфейс будет отображать только первые 32 адреса, и если вы отредактировали конфигурацию без ошибок, то все будет работать как надо).

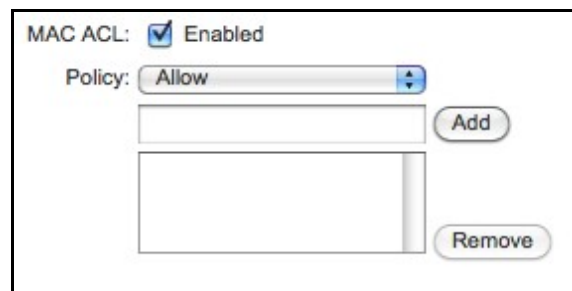
```
...
wireless.1.mac_acl.33.mac=XX:XX:XX:XX:XX:XX
wireless.1.mac_acl.33.status=enabled
wireless.1.mac_acl.34.mac=XX:XX:XX:XX:XX:XX
wireless.1.mac_acl.34.status=enabled
wireless.1.mac_acl.35.mac=XX:XX:XX:XX:XX:XX
wireless.1.mac_acl.35.status=enabled
wireless.1.mac_acl.36.mac=XX:XX:XX:XX:XX:XX
wireless.1.mac_acl.36.status=enabled
...
```

MAC ACL: MAC Access Control List (ACL) дает возможность запретить или разрешить клиентским устройствам подключаться к базовой станции в режимах AP и AP WDS.

Чтобы включить MAC ACL установите переключатель **Enabled**.

Есть два способа управлять списком Access Control List:

- задать конкретных клиентов, которым разрешен доступ, при этом всем остальным устройствам доступ будет запрещен - установите в поле Policy значение **Allow**.
- и наоборот перечислить запрещенных клиентов, а всем остальным будет разрешен доступ - установите **Policy** в значение **Deny**.



Мак адреса клиентских устройств добавляются и удаляются с помощью кнопок **Add** и **Remove** соответственно.

Примечание: MAC Access Control имеет самый низкий уровень защиты, для серьезной защиты доступа используйте шифрование WPA™ or WPA2™.

Нажмите кнопку **Change** чтобы сохранить изменения.

2.5 Страница Network

Вкладка Network позволяет администратору настраивать функции моста или роутера.

Устройства на базе AirOS v5.3 могут работать в режиме моста, роутера и SOHO роутера. IP адрес может быть получен от DHCP сервера или настроен в ручную. Используйте Раздел меню *Network* для настройки IP адреса.

Network Mode: выберите режим работы устройства. Всего три режима работы: мост (bridge), роутер (router) и SOHO роутер (SOHO router). Выбор режима зависит от технологий используемых в вашей сети:

[Bridge] режим работы выбран по умолчанию так как этот режим чаще всего используется в клиентских станциях, при соединении с точками доступа или при использовании WDS. В этом режиме устройство выступает в роли прозрачного моста. Не будет никакой сегментации сети пока широковещательный домен будет тот же. В режиме моста не блокируется широковещательный трафик. Дополнительно может быть сконфигурирован фаервол для фильтрации пакетов и контроля доступа в режиме моста.

[Router] режим роутера может быть использован для обеспечения маршрутизации и сегментации сети - беспроводные клиенты будут находиться в другой подсети. Режим роутера будет блокировать широковещательный трафик.

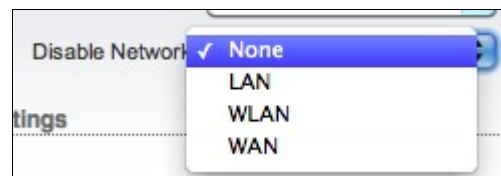
AirOS v5.3 поддерживает функцию пропускания многоадресных пакетов в режиме роутера.

Роутеры на основе AirOS v5.3 могут выступать в роли DHCP сервера и использовать NAT, который очень часто используется точками доступа. NAT будет выступать в роли фаервола между LAN и WLAN сетями. Так же дополнительно может быть сконфигурирован фаервол для фильтрации пакетов и контроля доступа в режиме роутера.

[SOHO Router]: SOHO (= Small Office and Home Office) роутер - этот режим расширяет режим возможности обычного роутера и позволяет превратить LAN порт в WAN, при этом беспроводная сеть (WLAN) становится локальной.

Устройства с одним Ethernet портом (в режиме AP или AP-WDS) в этом режиме работают как обычный роутер, однако LAN порт становится WAN портом, а беспроводная сеть (WLAN) становится локальной. Устройства с двумя и более Ethernet портами, главный Ethernet порт становится WAN портом, а беспроводная сеть (WLAN) и остальные LAN порты становятся локальными

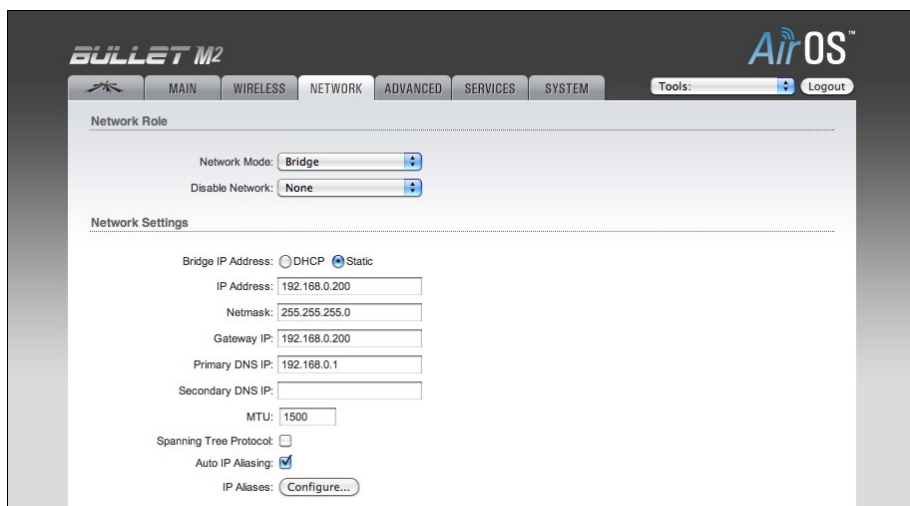
Disable Network: опция которая может быть использована для отключения *WLAN*, *LAN* или *WAN* интерфейса. Эту функцию следует использовать осторожно, так как по отключенному интерфейсу не может быть установлено ни одного соединения. Так же будет невозможно подключиться и перенастроить AirOS через отключенный интерфейс. Опция *Disable WAN* доступна только в режиме *SOHO* роутера.



2.5.1 Network settings

2.5.1.1 Bridge Mode

В режиме моста устройства на базе AirOS v5.3 пропускают все пакеты данных от одного сетевого интерфейса к другому без какой либо интеллектуальной маршрутизации. Для простейших задач, это эффективное и полностью прозрачное решение. WLAN (беспроводная сеть) и LAN (Ethernet) интерфейсы принадлежат к одному сегменту сети, который имеет одинаковый диапазон IP адресов.



Мост имеет свой IP адрес для управления:

Bridge IP Address: устройству можно назначить статический адрес или получать его автоматически по DHCP.

Должен быть выбран один из способов присвоения IP адреса:

DHCP –выберите эту опцию для получения динамического IP адреса, шлюза и DNS сервера от BPC3 сервера в вашей сети.

Static – выберите эту опцию для назначения статического IP адрес.

IP Address: IP адрес устройства (доступно только в режиме **Static**). Этот адрес будет использоваться для подключения и управления устройством с AirOS.

IP адрес и маска подсети должны соответствовать адресному пространству сегмента сети в котором находится устройство. Если IP адрес устройства и IP адрес компьютера администратора (подключенного по проводной или беспроводной связи) будут находиться в разных адресных пространствах, то устройство будет недоступно.

Netmask (маска сети): эта величина определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети. Маска сети определяет адресное пространство сегмента сети в котором располагается устройство с AirOS.

Маска сети 255.255.255.0 (или /24), часто используется среди множества IP сетей С-класса.

Network Settings

Bridge IP Address: ☐ DHCP ☒ Static

IP Address:

Netmask:

Gateway IP:

Primary DNS IP:

Secondary DNS IP:

MTU:

Spanning Tree Protocol: ☐

Auto IP Aliasing: ☒

IP Aliases:

Gateway IP: Обычно это IP адрес роутера через который осуществляется доступ в интернет. Это может быть DSL или кабельный модем, или шлюз вашего провайдера. Устройство с AirOS будет направлять пакеты данных на шлюз, если адресат находится за пределами локальной сети.

IP адрес шлюза должен быть из того же сегмента сети что и устройство AirOS.

Primary/Secondary DNS IP: The Domain Name System (DNS) - это "телефонная книга" интернета, которая переводит имена доменов в IP адреса. Эти поля определяют IP адреса серверов к которым AirOS обращается как к источникам перевода.

Primary DNS - IP адрес DNS сервера.

Secondary DNS - IP адрес дополнительного DNS сервера.

Используется в случае отказа основного DNS.

UBNT: [NanoStation M2] - Bridge IP Aliases

http://192.168.1.20/ipalias.cgi?iface=br0

	IP	Netmask	Comment	Enabled
1.	192.168.1.45	255.255.255.0	pc	<input checked="" type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

MTU: определяет максимальный размер блока (в байтах), который может быть передан на канальном уровне. При использовании медленного соединения, большие пакеты могут вызывать задержки.

DHCP Fallback IP: IP адрес используемый в случае невозможности получения IP адреса от DHCP сервера (при работе в режиме *DHCP*).

Вслучае если IP адрес устройства с AirOS v5.3 неизвестен, он может быть получен с помощью [Ubiquiti Discovery Utility](#). Мультиплатформная утилита должна быть запущена с компьютера администратора, который расположен в

Network Settings

Bridge IP Address: ☒ DHCP ☐ Static

DHCP Fallback IP:

DHCP Fallback Netmask:

MTU:

Spanning Tree Protocol: ☐

Auto IP Aliasing: ☒

IP Aliases:

том же сегменте сети что и устройство с AirOS.

AirOS v5.3 будет сброшена к заводским настройкам IP (192.168.1.20/255.255.255.0), если *осуществить процедуру "Reset to defaults"*.

DHCP Fallback Netmask: маска сети используемая в случае невозможности получения IP адреса от DHCP сервера (при работе в режиме *DHCP*).

Spanning Tree Protocol: множество взаимосвязанных мостов образуют сети используя IEEE 802.1d *Spanning Tree Protocol (STP)*, который используется для нахождения кратчайшего пути и ликвидации петель в топологии сети.

Если STP включен, мост с AirOS будет взаимодействовать с другими устройствами в сети посылая и принимая *Bridge Protocol Data Units (BPDU)*.

Spanning Tree Protocol: ☒

STP должен быть выключен (по умолчанию), когда устройство с AirOS является единственным мостом в сети или когда в топологии сети отсутствуют петли. В этом случае использование STP не имеет смысла.

Auto IP Aliasing конфигурирует автоматически генерируемый IP адрес для соответствия WLAN/LAN интерфейсу, если активирован. Генерируемый IP адрес - это уникальный адрес класса B из диапазона 169.254.X.Y (маска сети 255.255.0.0), который предназначен для использования внутри только такого же сегмента сети. Этот адрес всегда начинается с 169.254.X.Y, где X и Y - это последние два разряда MAC адреса устройства (то есть если MAC равен 00:15:6D:A3:04:FB, генерируемый IP будет равен 169.254.4.251).

IP Aliases (IP псевдонимы) - могут быть настроены как для внутренней так и для внешней сети. Настройка производится в окне конфигурации, которое доступно после нажатия кнопки "Configure".

IP Address - альтернативный IP адрес для LAN или WLAN интерфейса, используемый для маршрутизации или управления устройством ;

Netmask - идентификатор адресного пространства для конкретного IP псевдонима;

Comments - информационное поле для комментария к IP псевдониму. Несколько слов о назначении псевдонима;

Enabled - флажок включающий или выключающий определенный IP алиас. Все IP алиасы сохраняются в системном конфигурационном файле. Однако только включенные будут работать.

Данные о новых IP псевдонимах могут быть сохранены кнопкой **Save** или отменены кнопкой **Cancel** в окне конфигурации.

Нажмите на кнопку **Change** для сохранения изменений произведенных на вкладке *Network*.

2.5.1.2 Router Mode

Во время работы в режиме роутера, роли LAN и WLAN интерфейсов изменятся согласно режиму **Wireless**:

В режиме AP/AP WDS: Беспроводной интерфейс и все беспроводные клиенты считаются локальными, а Ethernet интерфейс подключается к внешней сети;

В режиме Station/Station WDS: Беспроводной интерфейс и все беспроводные клиенты считаются внешней сетью, а Ethernet интерфейс и все подключенные к нему устройства - внутренней сетью.

Проводные/беспроводные клиенты маршрутизируются из внутренней сети во внешнюю по умолчанию. Network Address Translation (NAT)- так же работает.

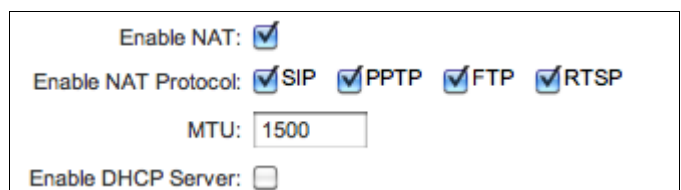
2.5.1.2.1 WLAN Network Settings

IP Address: этот IP адрес назначается WLAN интерфейсу, который подключен к внутренней сети согласно одному из режимов работы описанных выше. Этот IP будет использоваться как IP адрес шлюза для маршрутизации всех устройств во внутренней сети, а так же для настройки AirOS.

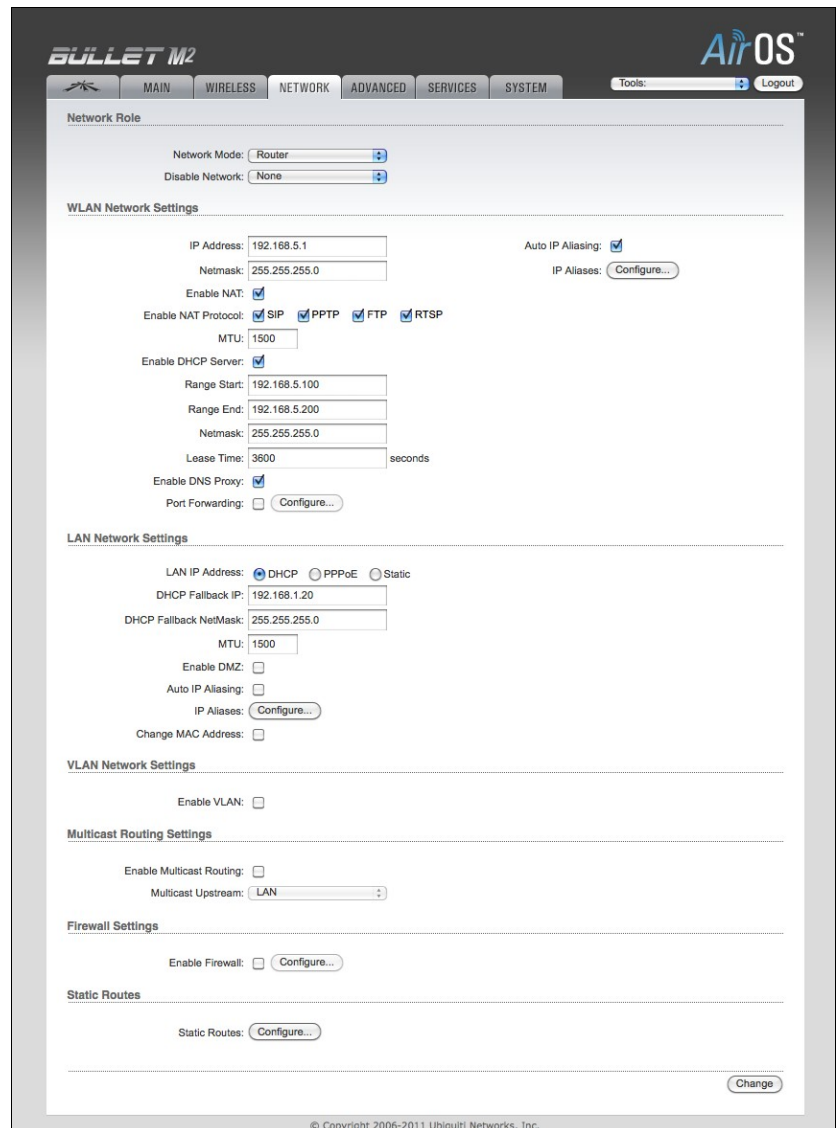
Netmask: используется для определения класса используемого адресного пространства. Значение 255.255.255.0 - типично для сетей класса C, которые поддерживают диапазон адресов от 192.0.0.x до 223.255.255.x. Сети класса C используют 24 бита для идентификации сети (альтернативное обозначение "/24") и 8 бит для идентификации хоста.

Enable NAT: Network Address Translation (NAT) - позволяет пересылать пакеты с LAN интерфейса на IP адрес беспроводного интерфейса, а затем осуществлять суб-маршрутизацию на клиентские устройства расположенные в локальной сети, при работе AirOS в режиме *AP/AP WDS* и в обратном направлении при работе в режиме "Station/Station WDS".

Enable NAT Protocol: если NAT активирован, пакеты данных могут быть модифицированы для прохождения через роутер. Для того чтобы предотвратить модификацию некоторых специфических пакетов (например: SIP, PPTP, FTP, RTSP), снимите отметку с чекбокса(-ов).



NAT реализован с использованием правил маскарadingа. В режиме Router его настройки хранятся в таблице NAT в iptables. Для более детальной информации о функциях NAT обратитесь к инструкции



iptables

Если NAT отключен, то необходимо настроить статические маршруты для того чтобы пакеты могли пройти через устройство на базе AirOS v5.3.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) сервер присваивает IP адреса клиентам подключенным к беспроводному интерфейсу, при работе в режиме *AP/AP WDS* или клиентам подключенным к LAN интерфейсу, при работе в режиме *Station/Station WDS*.

Range Start/End: этот диапазон определяет список IP адресов выдаваемых DHCP сервером устройствам во внутренней сети настроенным на получение динамического IP.

Netmask: используется для определения класса используемого адресного пространства. Значение 255.255.255.0 - типично для сетей класса C, которые поддерживают диапазон адресов от 192.0.0.x до 223.255.255.x. Сети класса C используют 24 бита для идентификации сети (альтернативное обозначение "/24") и 8 бит для идентификации хоста.

Lease Time: IP адрес выдаваемый DHCP сервером будет действителен только в течении срока аренды. Увеличение этого времени обеспечивает непрерывную работу клиента, но увеличивает потенциальную возможность возникновения конфликтов. Уменьшение времени аренды поможет избежать потенциального конфликта адресов, но может вызвать множество небольших задержек у клиента пока он получит новый IP адрес от DHCP сервера. Значение устанавливается в секундах. Максимальный срок аренды 172800 секунд.

MTU: определяет размер (в байтах) наибольшего пакета данных. При медленном соединении, большие пакеты могут вызвать задержки в обмене данных.

Enable DNS Proxy: функция позволяет пересылать запросы DNS от хостов находящихся в интрасети к DNS серверу. Для ее работы нужно указать IP адрес работающего DNS сервера. В настройках хостов в качестве IP адреса первичного DNS сервера следует указывать IP адрес устройства с AirOS, для того чтобы DNS прокси получал запросы DNS и переводил их в IP адреса.

Port Forwarding: данная функция позволяет перенаправлять отпределенные порты из внутренней сети во внешнюю. Это полезно для многих приложений, например, FTP серверов, игр и пр. где разные хосты должны рассматриваться как использующие один общий IP адрес/порт.

Правила перенаправления портов могут быть настроены в окне "Port Forwarding", которое открывается кнопкой **Configure**, доступной после активации функции **Port Forwarding**.

Enable DHCP Server: ☒

Range Start: 192.168.1.100

Range End: 192.168.1.200

Netmask: 255.255.255.0

Lease Time: 3600 seconds

Enable DNS Proxy: ☒

Enable DNS Proxy: ☒

Port Forwarding: ☒ [Configure...](#)

UBNT: [Bullet M2] – Port Forwarding

Port Forwarding

	Private IP	Private Port	Type	Source IP/mask	Public Port	Comment	Enabled
1.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
17.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
18.	<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Перенаправление портов может быть настроено с использованием следующих критериев:

Private IP - IP адрес хоста подключенного к внутренней сети к которому нужно получить доступ из внешней сети;

Private Port - TCP/UDP порт приложения работающего на хосте подключенном к внутренней сети;

Type - тип протокола который должен перенаправляться из внутренней сети.

Public Port - TCP/UDP порту устройства с AirOS v5.3, которое будет принимать и перенаправлять подключение из внешней сети на хост во внутренней сети.

Comments - текстовое поле для краткого комментария.

Enabled - флажок включающий или выключающий правило перенаправления. Все добавленные правила будут созранятся в настройках. Однако только включенные правила будут работать.

Добавленные правила могут быть сохранены нажатием кнопки **Save** или отменены кнопкой **Cancel** в окне конфигурации.

Auto IP Aliasing - конфигурирует автоматически генерируемый IP адрес для соответствия WLAN/LAN интерфейсу, если активирован. Генерируемый IP адрес - это уникальный адрес класса B из диапазона 169.254.X.Y (маска сети 255.255.0.0), который предназначен для использования внутри только такого же сегмента сетии. Этот адрес всегда начинается с 169.254.X.Y, где X и Y - это последние два разряда MAC адреса устройства (то есть если MAC равен 00:15:6D:A3:04:FB, генерируемый IP будет равен 169.254.4.251).

IP Aliases (IP псевдонимы) - могут быть настроены как для внутренней так и для внешней сети. Настройка производится в окне конфигурации, которое доступно после нажатия кнопки "Configure".

IP Address - альтернативный IP адрес для LAN или WLAN интерфейса, используемый для маршрутизации или управления устройством ;

Netmask - идентификатор адресного пространства для конкретного IP псевдонима;

Comments - информационное поле для комента к IP псевдониму. Несколько слов о назначении псевдонима;

Enabled - флажок включающий или выключающий определенный IP алиас. Все IP алиасы сохраняются в системном конфигурационном файле. Однако только влюченные будут работать.

	IP	Netmask	Comment	Enabled
1.	192.168.0.105	255.255.255.0		<input checked="" type="checkbox"/>
2.				<input type="checkbox"/>
3.				<input type="checkbox"/>
4.				<input type="checkbox"/>
5.				<input type="checkbox"/>
6.				<input type="checkbox"/>
7.				<input type="checkbox"/>
8.				<input type="checkbox"/>

Save Cancel

Данные о новых IP псевдонимах могут быть сохранены кнопкой **Save** или отменены кнопкой **Cancel** в окне конфигурации.

2.5.1.2.2 LAN Network Settings

LAN IP Address: этот IP адрес назначается LAN или WLAN интерфейсу, который подключен к внешней сети согласно одному из ражимов работы описанных выше. Этот IP будет использоваться как IP адрес шлюза для маршрутизации всех устройств во внутренней сети, а так же для настройки AirOS.

Интерфейсу подключенному к внешней сети, IP адрес может быть назначен в ручную, или присваиваться DHCP сервером, который должен располагаться во внешней сети. Необходимо выбрать один из режимов присвоения IP адреса:

DHCP – выберите эту опцию для получения IP адреса, шлюза и адреса DNS сервера динамически от внешнего DHCP сервера.

PPPoE – выберите эту опцию для получения IP адреса, шлюза и адреса DNS сервера динамически от внешнего PPPoE сервера.

Static – выберите эту опцию для назначения статических настроек IP для внешнего интерфейса.

IP адрес и маска сети должны соответствовать адресному пространству сегмента сети в котором расположено устройство с AiOS. Если настройки IP устройства и компьютера администратора подключенного к устройству, будут отличаться - устройство будет недоступно. Применимо только в режиме *Static*.

Netmask: используется для определения класса используемого адресного пространства. Значение 255.255.255.0 - типично для сетей класса C, которые поддерживают диапазон адресов от 192.0.0.x до 223.255.255.x. Сети класса C используют 24 бита для идентификации сети (альтернативное обозначение "/24") и 8 бит для идентификации хоста. Применимо только в режиме *Static*.

Gateway IP: IP адрес шлюза расположенного во внешней сети, который предоставляет доступ в интернет. Это может быть DSL или кабельный модем, или шлюз вашего провайдера. Устройство с AirOS будет направлять пакеты данных на шлюз, если адресат находится за пределами локальной сети. Применимо только в режиме *Static*.

IP адрес шлюза должен быть из того же сегмента сети что и сетевой интерфейс устройства подключенный к внешней сети (беспроводной интерфейс в режиме *Station* и LAN интерфейс в режиме *AP*). Применимо только в режиме *Static*.

Primary/Secondary DNS IP: The Domain Name System (DNS) - это "телефонная книга" интернета, которая переводит имена доменов в IP адреса. Эти поля определяют IP адреса серверов где DNS запросы перенаправляются устройством с AirOS v5.3. Применимо только в режиме *Static*.

Primary DNS - IP адрес DNS сервера.

Secondary DNS - IP адрес дополнительного DNS сервера. Используется в случае отказа основного DNS.

LAN Network Settings

LAN IP Address: ☐ DHCP ☐ PPPoE ☒ Static

IP Address:

Netmask:

Gateway IP:

Primary DNS IP:

Secondary DNS IP:

MTU:

Enable DMZ: ☐

Auto IP Aliasing: ☐

IP Aliases: [Configure...](#)

Change MAC Address: ☐

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) - это виртуальное частное и безопасное подключение между двумя системами, которое включает инкапсулированную передачу данных. Часто используется как средство для подключения клиентов к интернет провайдеру.

Выберите опцию *PPPoE* чтобы настроить PPPoE туннель для подключения к провайдеру. Как PPPoE может быть настроен только тот интерфейс, который подключен к внешней сети, так как весь трафик будет передаваться через этот туннель.

IP адрес, шлюз и IP DNS сервера будут получены от PPPoE сервера после установки соединения. Широковещательный адрес используется для обнаружения PPPoE сервера и создания туннеля.

Для создания PPPoE соединения необходимы корректные данные авторизации:

PPPoE Username – имя пользователя для подключения к серверу (на PPPoE сервере должны быть соответствующие настройки);

PPPoE Password – пароль для подключения к серверу (на PPPoE сервере должны быть соответствующие настройки);

Show: Установите этот флажок для отображения символов пароля PPPoE.

PPPoE MTU/MRU – максимальный размер (в байтах) передаваемого (MTU) и принимаемого (MRU) блока данных инкапсулируемого трафика проходящего через PPP туннель; (значение MTU/MRU по умолчанию: 1492)

PPPoE Encryption – включение использования протокола шифрования MPPE (Microsoft Point-to-Point Encryption).

IP адрес интерфейса PPP будет показан на вкладке *Main* после статистики PPP интерфейса, если он получен по установленному PPPoE соединению, в противном случае будет выводиться сообщение "Not Connected".

Процедура преподключения PPPoE туннеля может быть инициирована кнопкой *Reconnect*, которая расположена на вкладке *Main* после статистики PPPoE интерфейса.

Enable DMZ: демилитаризованная зона может быть включена и использоваться как место, где можно разместить такие сервисы как Web серверы, Proxy серверы, and E-mail серверы таким образом, чтобы они могли обслуживать локальную сеть и при этом быть изолированными от нее для увеличения безопасности. DMZ обычно используется вместе с NAT как альтернативой для *Port Forwarding*, так как делает все порты хоста в сети видимыми из внешней сети.

DMZ Management Port: порт веб управления для устройства на базе AirOS v5.3 (TCP/IP порт 80 по умолчанию), используемый для хост устройства если опция *DMZ Management Port* активирована. В этом случае устройство с AirOS будет отвечать на запросы из внешней сети так как если бы они исходили от хоста указанного в DMZ IP. Рекомендуется оставить функцию *Management Port* отключенной, так как при ее активации устройство с AirOS станет недоступной из внешней сети.

DMZ IP: подключенный к внутренней сети хост, указанный в поле *DMZ IP* адрес будет доступен из внешней сети.

LAN Network Settings

LAN IP Address: ☐ DHCP ☒ PPPoE ☐ Static

PPPoE Username:

PPPoE Password: ☐ Show

PPPoE MTU/MRU: /

PPPoE Encryption: ☒

Enable DMZ: ☐

Auto IP Aliasing: ☐

IP Aliases:

Change MAC Address: ☐

DHCP Fallback IP: в случае работы внешнего сетевого интерфейса роутера в режиме динамического получения IP адреса и невозможности получить его от DHCP сервера, будет назначен IP указанный в этом поле.

DHCP Fallback Netmask: маска сети используемая в случае невозможности получения IP адреса от DHCP сервера (при работе в режиме *DHCP*).

Вслучае если IP адрес устройства с AirOS v5.3 неизвестен, он может быть получен с помощью [Ubiquiti Discovery Utility](#). Мультиплатформенная утилита должна быть запущена с компьютера администратора, который расположен в том же сегменте сети что и устройство с AirOS.

AirOS v5.3 будет сброшена к заводским настройкам IP (192.168.1.20/255.255.255.0), если *осуществить процедуру "Reset to defaults"*.

LAN Network Settings

LAN IP Address: ☒ DHCP ☐ PPPoE ☐ Static

IP Address:

Netmask:

Gateway IP:

Primary DNS IP:

Secondary DNS IP:

PPPoE Username:

PPPoE Password:

PPPoE MTU/MRU: 1492 / 1492

PPPoE Encryption: ☐

Enable DMZ: ☐

DMZ Management Port: ☐

DMZ IP:

DHCP Fallback IP: 192.168.1.20

Auto IP Aliasing - конфигурирует автоматически генерируемый IP адрес для соответствия WLAN/LAN интерфейсу, если активирован. Генерируемый IP адрес - это уникальный адрес класса B из диапазона 169.254.X.Y (маска сети 255.255.0.0), который предназначен для использования внутри только такого же сегмента сети. Этот адрес всегда начинается с 169.254.X.Y, где X и Y - это последние два разряда MAC адреса устройства (то есть если MAC равен 00:15:6D:A3:04:FB, генерируемый IP будет равен 169.254.4.251).

IP Aliases (IP псевдонимы) - могут быть настроены как для внутренней так и для внешней сети. Настройка производится в окне конфигурации, которое доступно после нажатия кнопки "Configure".

IP Address - альтернативный IP адрес для LAN или WLAN интерфейса, используемый для маршрутизации или управления устройством ;

Netmask - идентификатор адресного пространства для конкретного IP псевдонима;

Comments - информационное поле для комментария к IP псевдониму. Несколько слов о назначении псевдонима;

Enabled - флажок включающий или выключающий определенный IP алиас. Все IP алиасы сохраняются в системном конфигурационном файле. Однако только включенные будут работать.

Данные о новых IP псевдонимах могут быть сохранены кнопкой **Save** или отменены кнопкой **Cancel** в окне конфигурации.

UBNT: [Bullet M5] - WLAN IP Aliases - Mozilla Firefox

http://192.168.1.20/ipalias.cgi?iface=ath0

WLAN IP Aliases

	IP	Netmask	Comment	Enabled
1.	192.168.0.105	255.255.255.0		<input checked="" type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Save Cancel

Listo

Change MAC Address: данная функция позволяет легко изменить MAC адрес соответствующего интерфейса.

Особенно это полезно когда ваш провайдер назначает только один действительный IP адрес, связанный с конкретным MAC адресом;

обычно используется кабельными операторами или некоторыми интернет провайдерами.

Change MAC Address: ☒

MAC Address: 00:25:00:41:26:85

2.5.1.3 SOHO Router

Station or Station WDS SOHO (= Small Office and Home Office) router - этот режим расширяет режим возможности обычного роутера и позволяет превратить LAN порт в WAN, при этом беспроводная сеть (WLAN) становится локальной.

Корректная работа в режиме SOHO роутера возможна только при работе в режиме AP или AP-WDS, так как он не предназначен для работы как беспроводной клиент.

Устройства с одним Ethernet портом (в режиме AP или AP-WDS) в этом режиме работают как обычный роутер, однако LAN порт становится WAN портом, а беспроводная сеть (WLAN) становится локальной. Устройства с двумя и более Ethernet портами, главный Ethernet порт становится WAN портом, а беспроводная сеть (WLAN) и остальные LAN порты становятся локальными.

The screenshot shows the 'BULLET M2' web interface with the 'AirOS' logo. The 'NETWORK' tab is selected. Under 'Network Role', 'Network Mode' is set to 'SOHO Router' and 'Disable Network' is 'None'. The 'WAN Network Settings' section shows 'WAN IP Address' set to 'DHCP' (selected), with 'DHCP Fallback IP' at '192.168.1.20' and 'DHCP Fallback NetMask' at '255.255.255.0'. Other options like 'MTU', 'Enable DMZ', 'Auto IP Aliasing', and 'IP Aliases' are visible. The 'LAN Network Settings' section shows 'IP Address' at '192.168.1.1', 'Netmask' at '255.255.255.0', and 'Enable NAT' checked. 'Enable NAT Protocol' has checkboxes for SIP, PPTP, FTP, and RTSP, all of which are checked. 'MTU' is set to '1500'.

Примечание: Не используйте режим SOHO роутер в комбинации с беспроводным режимом Station или Station WDS на устройствах с одним Ethernet портом, это может сделать устройство недоступным. В подобном случае сбросьте настройки устройства на заводские, для этого нажмите кнопку Reset на 8 секунд а потом отпустите.

2.5.1.3.1 WAN Network Settings

WAN IP Address: этот IP адрес назначается WLAN интерфейсу, который подключен к внешней сети. Этот IP будет использоваться для маршрутизации, а так же для настройки AirOS.

IP адрес WAN интерфейсу может быть назначен в ручную, или присваиваться DHCP сервером, который должен располагаться во внешней сети. Необходимо выбрать один из режимов присвоения IP адреса:

DHCP – выберите эту опцию для получения IP адреса, шлюза и адреса DNS сервера динамически от внешнего DHCP сервера.

PPPoE – выберите эту опцию для получения IP адреса, шлюза и адреса DNS сервера динамически от внешнего PPPoE сервера.

Static – выберите эту опцию для назначения статических настроек IP для внешнего

интерфейса.

Netmask: используется для определения класса используемого адресного пространства. Значение 255.255.255.0 - типично для сетей класса C, которые поддерживают диапазон адресов от 192.0.0.x до 223.255.255.x. Сети класса C используют 24 бита для идентификации сети (альтернативное обозначение "/24") и 8 бит для идентификации хоста.

Gateway IP: IP адрес шлюза расположенного во внешней сети, который предоставляет доступ в интернет. Это может быть DSL или кабельный модем, или шлюз вашего провайдера. Устройство с AirOS будет направлять пакеты данных на шлюз, если адресат находится за пределами локальной сети.

Primary/Secondary DNS IP: The Domain Name System (DNS) - это "телефонная книга" интернета, которая переводит имена доменов в IP адреса. Эти поля определяют IP адреса серверов где DNS запросы перенаправляются устройством с AirOS

MTU: определяет размер (в байтах) наибольшего пакета данных. При медленном соединении, большие пакеты могут вызвать задержки в обмене данными.

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) - это виртуальное частное и безопасное подключение между двумя системами, которое включает инкапсулированную передачу данных. Часто используется как средство для подключения клиентов к интернет провайдеру.

Выберите опцию *PPPoE* чтобы настроить PPPoE туннель для подключения к провайдеру. Как PPPoE может быть настроен только тот интерфейс, который подключен к внешней сети, так как весь трафик будет передаваться через этот туннель. IP адрес, шлюз и IP DNS сервера будут получены от PPPoE сервера после установки соединения. Широковещательный адрес используется для обнаружения PPPoE сервера и создания туннеля.

Для создания PPPoE соединения необходимы корректные данные авторизации:

PPPoE Username – имя пользователя для подключения к серверу (на PPPoE сервере должны быть соответствующие настройки);

PPPoE Password – пароль для подключения к серверу (на PPPoE сервере должны быть соответствующие настройки);

The screenshot shows the 'WAN Network Settings' window. At the top, 'WAN IP Address' has three radio buttons: 'DHCP', 'PPPoE', and 'Static'. The 'Static' button is selected. Below this, there are input fields for 'IP Address' (192.168.0.1), 'Netmask' (255.255.255.0), 'Gateway IP' (192.168.0.200), 'Primary DNS IP' (192.168.0.1), and 'Secondary DNS IP' (empty). There is also an 'MTU' field set to 1500. Below these are checkboxes for 'Enable DMZ' and 'Auto IP Aliasing', both of which are unchecked. There is a 'Configure...' button next to 'IP Aliases' and a 'Change MAC Address' checkbox which is also unchecked.

The screenshot shows the 'WAN Network Settings' window. At the top, 'WAN IP Address' has three radio buttons: 'DHCP', 'PPPoE', and 'Static'. The 'PPPoE' button is selected. Below this, there are input fields for 'PPPoE Username' (username) and 'PPPoE Password' (masked with dots). There is a 'Show' checkbox next to the password field. Below these are 'PPPoE MTU/MRU' fields set to 1492 / 1492. There is a 'PPPoE Encryption' checkbox which is checked. Below these are checkboxes for 'Enable DMZ' and 'Auto IP Aliasing', both of which are unchecked. There is a 'Configure...' button next to 'IP Aliases' and a 'Change MAC Address' checkbox which is also unchecked.

Show: Установите этот флажок для отображения символов пароля PPPoE.

PPPoE MTU/MRU – максимальный размер (в байтах) передаваемого (MTU) и принимаемого (MRU) блока данных инкапсулируемого трафика проходящего через PPP туннель; (значение MTU/MRU по умолчанию: 1492)

PPPoE Encryption – включение использования протокола шифрования MPPE (Microsoft Point-to-Point Encryption).

IP адрес интерфейса PPP будет показан на вкладке *Main* после статистики PPP интерфейса, если он получен по установленному PPPoE соединению, в противном случае будет выводиться сообщение "Not Connected".

Процедура преподключения PPPoE туннеля может быть инициирована кнопкой *Reconnect*, которая расположена на вкладке *Main* после статистики PPP интерфейса.

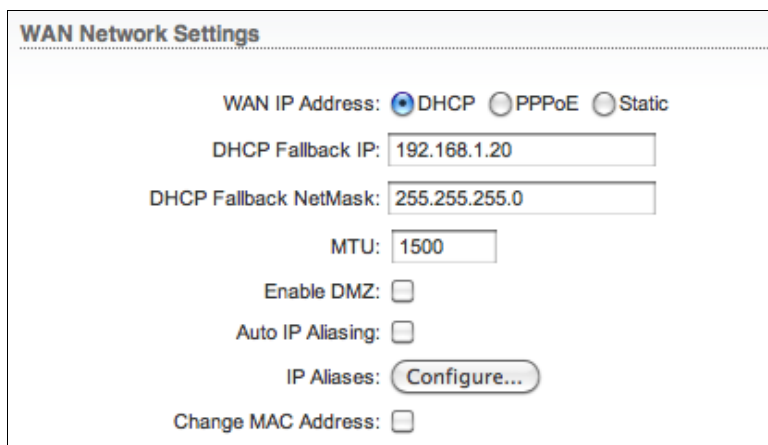
Enable DMZ: демилитаризованная зона может быть включена и использоваться как место, где можно разместить такие сервисы как Web серверы, Proxy серверы, and E-mail серверы таким образом, чтобы они могли обслуживать локальную сеть и при этом быть изолированными от нее для увеличения безопасности. DMZ обычно используется вместе с NAT как альтернативой для *Port Forwarding*, так как делает все порты хоста в сети видимыми из внешней сети.

DMZ Management Port: порт веб управления для устройства на базе AirOS v5.3 (TCP/IP порт 80 по умолчанию), используемый для хост устройства если опция *DMZ Management Port* активирована. В этом случае устройство с AirOS будет отвечать на запросы из внешней сети так как если бы они исходили от хоста указанного в DMZ IP. Рекомендуется оставить функцию *Management Port* отключенной, так как при ее активации устройство с AirOS станет недоступной из внешней сети.

DMZ IP: подключенный к внутренней сети хост, указанный в поле *DMZ IP* адрес будет доступен из внешней сети.

DHCP Fallback IP: при работе WAN интерфейса SOHO роутера в режиме динамического получения IP адреса и невозможности получить его от DHCP сервера, будет назначен IP указанный в этом поле.

DHCP Fallback Netmask: маска сети используемая в случае невозможности получения IP адреса от DHCP сервера (при работе в режиме *DHCP*).



Auto IP Aliasing: конфигурирует автоматически генерируемый IP адрес для соответствия WLAN/LAN интерфейсу, если активирован. Генерируемый IP адрес - это уникальный адрес класса B из диапазона 169.254.X.Y (маска сети 255.255.0.0), который предназначен для использования внутри только такого же сегмента сети. Этот адрес всегда начинается с 169.254.X.Y, где X и Y - это последние два разряда MAC адреса устройства (то есть если MAC равен 00:15:6D:A3:04:FB, генерируемый IP будет равен 169.254.4.251).

IP Aliases: (IP псевдонимы) - могут быть настроены как для внутренней так и для внешней сети. Настройка производится в окне конфигурации, которое доступно после нажатия кнопки "Configure".

IP Address - альтернативный IP адрес для LAN или WLAN интерфейса, используемый для маршрутизации или управления устройством ;

Netmask - идентификатор адресного пространства для конкретного IP псевдонима;

Comments - информационное поле для комментария к IP псевдониму. Несколько слов о назначении псевдонима;

Enabled - флажок включающий или выключающий определенный IP алиас. Все IP алиасы сохраняются в системном конфигурационном файле. Однако только включенные будут работать.

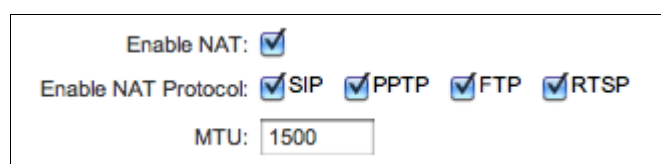
Change MAC Address: данная функция позволяет легко изменить MAC адрес соответствующего интерфейса. Особенно это полезно когда ваш провайдер назначает только один действительный IP адрес, связанный с конкретным MAC адресом; обычно используется кабельными операторами или некоторыми интернет провайдерами.

2.5.1.3.2 LAN Network Settings

IP Address: этот IP адрес назначается LAN (включая WAN) интерфейсу подключенному к внутренней сети. Он будет использоваться для маршрутизации внутренней сети (будет служить шлюзом для всех устройств в интра сети). Так же этот IP адрес может быть использован для управления устройством с AirOS 5.3.

Netmask: используется для определения класса используемого адресного пространства. Значение 255.255.255.0 - типично для сетей класса C, которые поддерживают диапазон адресов от 192.0.0.x до 223.255.255.x. Сети класса C используют 24 бита для идентификации сети (альтернативное обозначение "/24") и 8 бит для идентификации хоста.

Enable NAT: позволяет пересылать пакеты из внешней сети (WAN) на IP адрес локального интерфейса, а затем осуществлять суб-маршрутизацию на клиентские устройства расположенные в локальной сети, при работе AirOS в режиме *AP/AP WDS*.



Enable NAT: ☒

Enable NAT Protocol: ☒ SIP ☒ PPTP ☒ FTP ☒ RTSP

MTU:

Enable NAT Protocol: если NAT активирован, пакеты данных могут быть модифицированы для прохождения через роутер. Для того чтобы предотвратить модификацию некоторых специфических пакетов (например: SIP, PPTP, FTP, RTSP), снимите отметку с чекбокса(-ов).

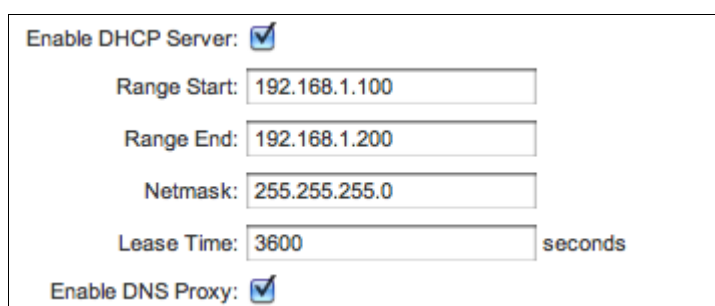
NAT реализован с использованием правил маскарadingа. В режиме Router его настройки хранятся в таблице NAT в iptables. Для более детальной информации о функциях NAT обратитесь к инструкции iptables

Если NAT отключен, то необходимо настроить статические маршруты для того чтобы пакеты могли пройти через устройство на базе AirOS v5.3.

MTU: определяет размер (в байтах) наибольшего пакета данных. При медленном соединении, большие пакеты могут вызвать задержки в обмене данных.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) сервер присваивает IP адреса клиентам подключенным к беспроводному интерфейсу, при работе в режиме *AP/AP WDS* или клиентам подключенным к LAN интерфейсу, при работе в режиме *Station/Station WDS*.

Range Start/End: этот диапазон определяет список IP адресов выдаваемых DHCP сервером устройствам во внутренней сети настроенным на



Enable DHCP Server: ☒

Range Start:

Range End:

Netmask:

Lease Time: seconds

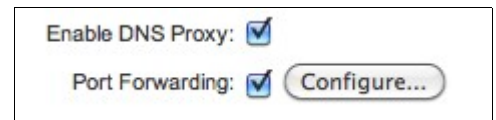
Enable DNS Proxy: ☒

получение динамического IP.

Netmask: используется для определения класса используемого адресного пространства. Значение 255.255.255.0 - типично для сетей класса C, которые поддерживают диапазон адресов от 192.0.0.x до 223.255.255.x. Сети класса C используют 24 бита для идентификации сети (альтернативное обозначение "/24") и 8 бит для идентификации хоста.

Lease Time: IP адрес выдаваемый DHCP сервером будет действителен только в течении срока аренды. Увеличение этого времени обеспечивает непрерывную работу клиента, но увеличивает потенциальную возможность возникновения конфликтов. Уменьшение времени аренды поможет избежать потенциального конфликта адресов, но может вызвать множество небольших задержек у клиента пока он получит новый IP адрес от DHCP сервера. Значение устанавливается в секундах.

Enable DNS Proxy: функция позволяет пересылать запросы DNS от хостов находящихся в интрасети к DNS серверу. Для ее работы нужно указать IP адрес работающего DNS сервера. В настройках хостов в качестве IP адреса первичного DNS сервера следует указывать IP адрес устройства с AirOS, для того чтобы DNS прокси получал запросы DNS и переводил их в IP адреса.



Port Forwarding: данная функция позволяет перенаправлять определенные порты из внутренней сети во внешнюю. Это полезно для многих приложений, например, FTP серверов, игр и пр. где разные хосты должны рассматриваться как использующие один общий IP адрес/порт.

Правила перенаправления портов могут быть настроены в окне "Port Forwarding", которое открывается кнопкой **Configure**, доступной после активации функции **Port Forwarding**.

Перенаправление портов может быть настроено с использованием следующих критериев:

Private IP - IP адрес хоста подключенного к внутренней сети к которому нужно получить доступ из внешней сети;

Private Port - TCP/UDP порт приложения работающего на хосте подключенном к внутренней сети;

Type - тип протокола который должен перенаправляться из внутренней сети.

Public Port - TCP/UDP порту устройства с AirOS v5.3, которое будет принимать и перенаправлять подключение из внешней сети на хост во внутренней сети.

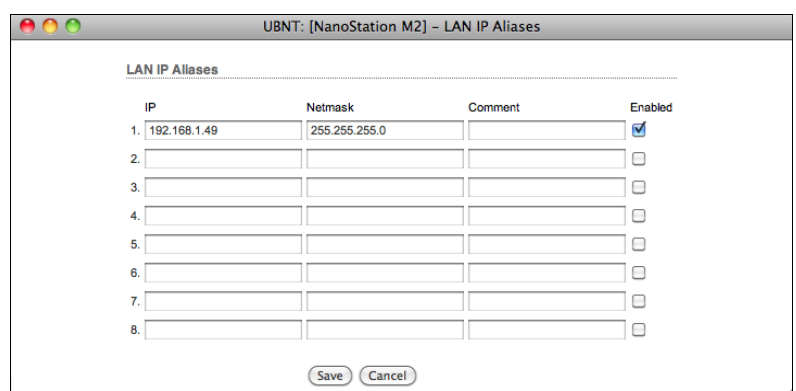
Comments - текстовое поле для краткого комментария.

Enabled - флажок включающий или выключающий правило перенаправления. Все добавленные правила будут созранятся в настройках. Однако только включенные правила будут работать.

Добавленные правила могут быть сохранены нажатием кнопки **Save** или отменены кнопкой **Cancel** в окне конфигурации.

Auto IP Aliasing конфигурирует автоматически генерируемый IP адрес для соответствия WLAN/LAN интерфейсу, если активирован. Генерируемый IP адрес - это уникальный адрес класса B из диапазона 169.254.X.Y (маска сети 255.255.0.0), который предназначен для использования внутри только такого же сегмента сети. Этот адрес всегда начинается с 169.254.X.Y, где X и Y - это последние два разряда MAC адреса устройства (то есть если MAC равен 00:15:6D:A3:04:FB, генерируемый IP будет равен 169.254.4.251).

IP Aliases (IP псевдонимы) - могут быть



настроены как для внутренней так и для внешней сети. Настройка производится в окне конфигурации, которое доступно после нажатия кнопки "Configure".

IP Address - альтернативный IP адрес для LAN или WLAN интерфейса, используемый для маршрутизации или управления устройством ;

Netmask - идентификатор адресного пространства для конкретного IP псевдонима;

Comments - информационное поле для комментария к IP псевдониму. Несколько слов о назначении псевдонима;

Enabled - флажок включающий или выключающий определенный IP алиас. Все IP алиасы сохраняются в системном конфигурационном файле. Однако только включенные будут работать.

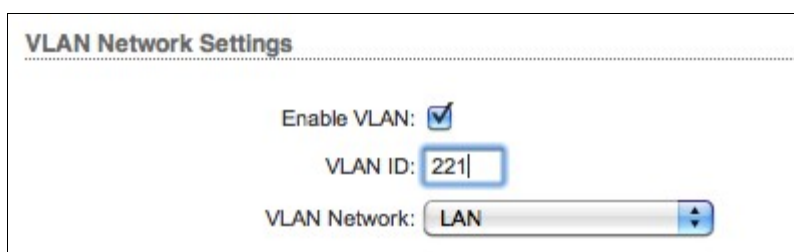
Данные о новых IP псевдонимах могут быть сохранены кнопкой **Save** или отменены кнопкой **Cancel** в окне конфигурации.

2.5.1.4 VLAN Network Settings

Enable VLAN: определяет максимальный размер (в байтах) пропускаемого пакета данных. При использовании медленного соединения, большие пакеты могут вызвать задержки.

VLAN ID: это уникальное значение присваиваемое каждому устройству. Каждый VLAN ID представляет собой отдельную виртуальную сеть. В AirOS 5.3 диапазон значений VLAN ID равен от 2 до 4094. Возможно присвоить только один VLAN ID на каждое устройство.

VLAN Network: определяет какому интерфейсу будет назначен присвоенный VLAN ID.

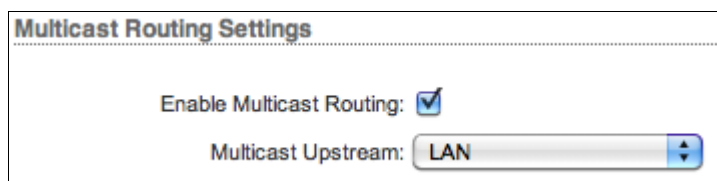


2.5.1.5 Multicast Routing Settings

При поддержке мультикаста (многоадресной отправки), приложения могут посылать одну копию каждого пакета данных группе компьютеров которые хотят его принять. Эта технология посылает пакеты группе получателей лучше чем одному получателю. Это зависит от сети для пересылки пакетов хостам которые должны их принимать. Обычные маршрутизаторы изолируют весь широковещательный (в том числе и многоадресный) трафик между внутренней и внешней сетью, однако AirOS имеет функцию пропуска мультикаста.

Enable Multicast Routing - эта опция активирует пропускание многоадресных пакетов между внешней и внутренней сетями в режиме при работе устройства в режиме роутера. Работа мультикаста основана на IGMP (Internet Group Management Protocol) протоколе.

Multicast Upstream: указывает источник многоадресного трафика.



2.5.1.6 Firewall Settings

Firewall (брандмауэр) может быть активирован на любом роутере с помощью функции "Enable Firewall". Настроить фаервол можно в окне конфигурации доступном по нажатию кнопки "Configure".

Настройки фаервола могут быть определены по следующим критериям:

Action - выбор между двумя правилами фаервола: ACCEPT или DROP. Если выбрано “Асцепт”, пакеты будут проходить через фаервол бел

изменений. Если выбрано “DROP”, пакеты будут отклоняться;

Interface - интерфейс на котором осуществляется фильтрация пакетов (WLAN, LAN или PPP);

IP Type - указание конкретного протокола на котором работает правило фильтрации (IP, ICMP, TCP, UDP, P2P);

Source IP/mask - источник фильтруемых пакетов, обычно это IP хоста который посылает пакеты;

Source Port - TCP/UDP порт источника пакета, обычно это порт приложения хоста-источника пакетов;

Destination IP/mask - IP адрес точки назначения пакета, обычно это IP адрес системы которой адресован пакет;

Destination Port - порт назначения TCP/UDP пакета, обычно это порт приложения хоста-адресата.

Comments - текстовое поле для короткого комментария к правилу фильтрации.

On - флажок включающий или выключающий правило фаервола. Все добавленные правила сохраняются в конфигурационном файле, однако только отмеченные этим флажком будут работать.

No - операторы инвертирующие значения полей *Source IP/mask*, *Source Port*, *Destination IP/mask* и *Destination Port* (т.е. если включен *not* для значения 443 поля *Destination Port*, фильтрация будет применяться ко всем пакетам посланным на любой другой порт кроме 443, который обычно используется протоколом HTTPS).

Action	Interface	IP Type	Not	Source IP/Mask	Not	Src Port	Not	Destination IP/Mask	Not	Dst Port	Comment	On
✓ DROP	ANY	IP	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>
ACCEPT	ANY	IP	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>
DROP	ANY	IP	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>
DROP	ANY	IP	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>
DROP	ANY	IP	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>
DROP	ANY	IP	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>
DROP	ANY	IP	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>
DROP	ANY	IP	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>

Изменения в правилах фаервола могут быть созданы кнопкой **Save** или отменены кнопкой **Cancel** в окне конфигурации.

В режиме Router, все активные правила фаервола хранятся в цепочке FIREWAL, в таблице *iptables filter*.

Для более подробного описания функционала фаервола в режиме роутера, обращайтесь к инструкции *iptables*

Нажмите на кнопку save для того чтобы изменения на вкладке Network вступили в силу.

2.5.1.7 Static Routes

В этом разделе вы можете в ручную добавить статические правила маршрутизации в таблицу System Routing, это позволит указать конкретный IP адрес(а), которые проходят через определенный шлюз.

Для каждой записи должен быть указан валидный *Target Network IP*, *Netmask*, *Gateway IP*, а так же если необходимо комментарий, и отмечен чекбокс “ON” для включения этого правила. После чего нажмите кнопку “Save” для сохранения изменений или “Cancel” для отмены.

	Target Network IP	Netmask	Gateway IP	Comment	On
1.	192.168.10.0	255.255.255.0	192.168.0.1	Static Route 1	<input checked="" type="checkbox"/>
2.					<input type="checkbox"/>
3.					<input type="checkbox"/>
4.					<input type="checkbox"/>
5.					<input type="checkbox"/>
6.					<input type="checkbox"/>
7.					<input type="checkbox"/>
8.					<input type="checkbox"/>
9.					<input type="checkbox"/>
10.					<input type="checkbox"/>
11.					<input type="checkbox"/>
12.					<input type="checkbox"/>
13.					<input type="checkbox"/>
14.					<input type="checkbox"/>
15.					<input type="checkbox"/>
16.					<input type="checkbox"/>
17.					<input type="checkbox"/>
18.					<input type="checkbox"/>
19.					<input type="checkbox"/>
20.					<input type="checkbox"/>

Save Cancel

2.6 Страница Advanced

Эта вкладка содержит расширенные настройки маршрутизации и беспроводного интерфейса. Вкладка Advanced позволяет конфигурировать функции влияющие на производительность и поведение устройства. Эти настройки рассчитаны на продвинутого пользователя имеющего достаточный объем знаний в постоении беспроводных сетей. Эти настройки не следует менять, если вы не знаете к каким последствиям это приведет.

2.6.1 Advanced Wireless Setting

Стандарт 802.11n поддерживает скоростные режимы MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6, MCS7 для устройств с цепочками 1x1 и MCS8, MCS9, MCS10, MCS11, MCS12, MCS13, MCS14, MCS15 для устройств с цепочками 2x2. Параметр ACK timeout оказывает решающее влияние на производительность в беспроводных подключениях на

BULLET M2

AirOS™

MAIN WIRELESS NETWORK ADVANCED SERVICES SYSTEM

Tools: Logout

Advanced Wireless Settings

RTS Threshold: 2346 ☒ Off

Fragmentation Threshold: 2346 ☒ Off

Distance: 0.4 miles (0.6 km)

ACK Timeout: 31 ☒ Auto Adjust

Aggregation: ☒ Enable

32 Frames 50000 Bytes

Multicast Data: ☒ Allow All

Enable Extra Reporting: ☒

Enable Client Isolation: ☐

Sensitivity Threshold, dBm: -96 ☒ Off

Advanced Ethernet Settings

Enable Autonegotiation: ☒

Link Speed, Mbps: 100

Enable Full Duplex: ☒

Signal LED Thresholds

LED1	LED2	LED3	LED4
94	80	73	65

Traffic Shaping

Enable Traffic Shaping: ☐

Change

© Copyright 2006-2011 Ubiquiti Networks, Inc.

открытом пространстве.

RTS Threshold: определяет размер передаваемого пакета и за счет использования точки доступа, помогает управлять потоками трафика. Устанавливается диапазон значений от 0 до 2346 байт, или флажок "off". Значение по умолчанию равно 2346, что означает, что RTS будет отключена.



RTS Threshold:	2346	<input checked="" type="checkbox"/> Off
Fragmentation Threshold:	2346	<input checked="" type="checkbox"/> Off

RTS/CTS (англ. *Request To Send / Clear To Send*, **Запрос на отправку/Разрешение отправки**) механизм, используемый в беспроводных сетях IEEE 802.11 для исключения т. н. «коллизий» фреймов; способ решения проблем «скрытого узла» и «незащищенного узла». Предельные значения размера RTS/CTS пакета равны 0-2346 байт. Если размер пакета который хочет передать узел, больше порогового значения, срабатывает механизм RTS/CTS. Если размер пакета равен или меньше порогового значения, фрейм отправляется немедленно.

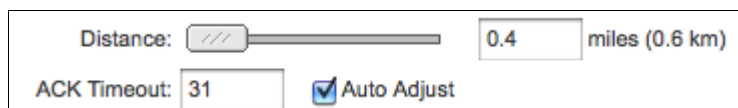
Система использует фреймы Request to Send/Clear to Send для взаимодействия, которое обеспечивает снижение коллизий точек доступа со скрытыми станциями. Станции сначала посылают RTS фрейм, данные же посылаются только после ответа точки доступа. Станция посылает CTS фрейм в ответ на RTS, что обеспечивает освобождение линии на запрос станции о передаче данных. Контроль взаимодействия с использованием CTS фреймов имеет временной интервал во время которого все другие станции прекращают трансляцию до тех пор пока запрашивающая станция не окончит трансляцию.

Fragmentation Threshold: определяет максимальный размер пакета до его фрагментации на несколько пакетов. Диапазон равен 256-2346 байт, или флажок "off". Установка параметра *Fragmentation Threshold* на слишком низкое значение может вызвать ухудшения производительности сети.

Использование фрагментации может увеличить надежность передачи фреймов. Поскольку отправка меньших фреймов вызывает меньшую вероятность возникновения коллизий. Однако меньшие значения фрагментации понизят пропускную способность. Рекомендуется вносить минимальные изменения в значения *Fragmentation Threshold* или оставить значене по умолчанию, так как 2346, является оптимальным для большинства беспроводных сетей.

AirOS v5.3 имеет в своем арсенале новый авто-распознающий алгоритм, который динамически оптимизирует таймаут распознавания фреймов без вмешательства человека. Это критическое свойство предназначено для стабилизации соединений стандарта 802.11n на больших расстояниях. Пользователь так же имеет возможность установить величину вручную, однако рекомендуется этого не делать.

Distance: установите расстояние в милях (или километрах) используя слайдер или введите значение вручную. Мощность сигнала и пропускная способность слабеют на расстоянии. Изменение расстояния изменит значение параметра ACK Timeout для соответствия значению дистанции.



Distance:	<input type="text" value="0.4"/>	miles (0.6 km)
ACK Timeout:	<input type="text" value="31"/>	<input checked="" type="checkbox"/> Auto Adjust

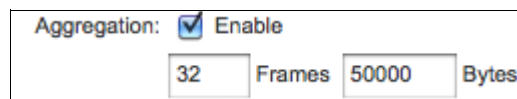
ACK Timeout: установите значение параметра *ACK Timeout* (временной промежуток распознавания). Каждый раз когда станция получает фрейм данных она посылает ACK фрейм точке доступа (если отсутствуют ошибки в передаче). Если станция не получает ACK фрейм от точки доступа на протяжении установленного промежутка времени, она повторяет отправку фрейма. Производительность падает так как очень много фреймов отправляется повторно, поэтому если *timeout* слишком короткий или слишком длинный, это приведет к ухудшению соединения и снижению пропускной способности.

Изменение параметра "*ACK Timeout*" изменит параметр *Distance* для соответствия дистанции параметра ACK Timeout.

Auto Adjust - этот флажок включает автоконфигурирование параметра ACK Timeout. Если активировано - ACK Timeout будет устанавливаться динамически с использованием алгоритма аналогичного "Conservative Rate" (используемого в AirOS v3.4). Настоятельно рекомендуется использовать опцию *Auto Adjust* для сетей 802.11n.

Если две или более станции расположены на значительном расстоянии от привязанной к ним точки доступа, наибольшее значение *ACK Timeout* для наибольшего расстояния должен быть установлен на точке доступа. AirOS v5.3 содержит улучшенный алгоритм вычисления ACK Timeout.

Aggregation: часть стандарта 802.11n (или проект стандарта). Он позволяет посылать несколько фреймов при однократном подключении к среде, объединяя фреймы вместе в один большой фрейм. Он создает большой фрейм соединяя меньшие фреймы с одинаковым физическим источником, точкой назначения и классом трафика (т. е. QoS) в один большой фрейм с общим MAC заголовком.

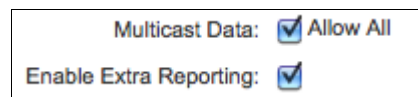


Frames – количество фреймов объединяемых в большой фрейм.

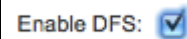
Bytes – размер (в байтах) большого фрейма.

Multicast Data: эта опция позволяет включить пропускание многоадресного трафика. По умолчанию эта опция отключена.

Enable Extra Reporting: функция позволяет выводить дополнительную информацию (например имя хоста) в управляющих фреймах 802.11. Эта информация обычно используется для идентификации системы и данных о статусе в утилитах для обнаружения и операционных систем роутеров.

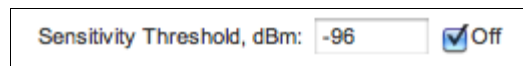


Enable DFS: DFS - это часть беспроводного стандарта IEEE 802.11h. Функция *Enable DFS* позволяет включать/отключать поддержку DFS (только в устройствах серии M5). DFS может быть обязателен в некоторых регулирующих доменах и должен быть настроен согласно регламенту выбранной страны.



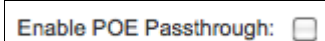
Enable Client Isolation: эта опция позволяет посылать пакеты только из внешней сети на оборудование клиента и обратно (возможно только в режиме *AP/AP WDS*). Если функция активирована беспроводные станции подключенные к той же точке доступа, не смогут связываться на уровне MAC и IP. Это эффективно для связанных станций и WDS.

Sensitivity Threshold, dBm: определяет минимальный уровень сигнала для клиента с которым можно подключиться к точке доступа. Любой клиент с уровнем сигнала ниже указанной величины будет отключен. Эта опция полезна для поддержания хорошего уровня сигнала между подключенными станциями, обеспечивая лучшую производительность. Снятие галочки "OFF" отключает функцию.

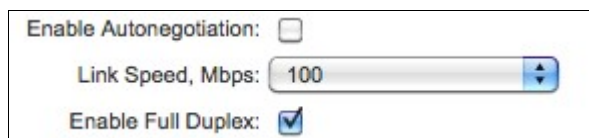


2.6.2 Advanced Ethernet Settings

Enable PoE Passthrough (только для серии Nano M): когда функция включена, устройство позволяет передать питание POE с главного порта на второстепенный, тем самым позволяя запитать другое устройство, например совместимую IP камеру.



Enable Autonegotiation: когда функция активна, устройство будет автоматически производить



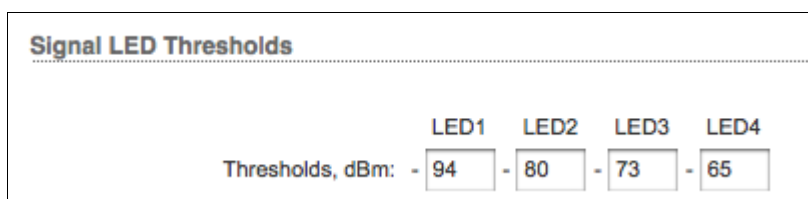
согласование параметров передачи с противной стороной, таких как скорость и дуплекс. В этом процессе устройства обмениваются информацией о своих параметрах и после выбирают быстрее режим передачи, который оба поддерживают. Если вы хотите установить эти параметры вручную, отключите эту функцию и выберите необходимые значения:

Link Speed, Mbps: выберите максимальную скорость передачи данных. Есть два варианта : 10Mbps или 100Mbps. Если вы используете очень длинный Ethernet кабель, скорость соединения в 10Mbps должна обеспечить лучшую стабильность.

Enable Full Duplex: выбор режима дуплекса; если включено устройство работает в полном дуплексе (позволяет двустороннюю передачу данных в обоих направлениях одновременно). Если отключено, устройство будет работать в режиме полу-дуплекса (позволяет двустороннюю передачу данных в обоих направлениях, но не одновременно, а только в одном направлении в одно и то же время).

2.6.3 Signal LED Thresholds

Индикаторы на задней панели устройств с AirOS v5.3 могут загораться, когда величины получаемого сигнала указаны в соответствующих полях. Это позволяет техникам устанавливать клиентские устройства без необходимости подключения к нему (например выставлять положение антенны).



Signal LED Thresholds				
	LED1	LED2	LED3	LED4
Thresholds, dBm:	- 94	- 80	- 73	- 65

Signal LED Thresholds укажите предельное значение уровня сигнала (dBm), которая будет включать индикатор:

LED 1 (красный) будет включаться если уровень сигнала достигнет значения указанного в этом поле. Значение по умолчанию -94dBm.

LED 2 (желтый) будет включаться если уровень сигнала достигнет значения указанного в этом поле. Значение по умолчанию -80dBm.

LED 3 (зеленый) будет включаться если уровень сигнала достигнет значения указанного в этом поле. Значение по умолчанию -73dBm.

LED 4 (зеленый) будет включаться если уровень сигнала достигнет значения указанного в этом поле. Значение по умолчанию -65dBm.

Пример конфигурации: если уровень сигнала (отображаемый на вкладке *Main*) колеблется в пределах -63 dBm, пороговые значения индикаторов лучше установить такие: -70, -65, -62, -60. **Примечание:** значения указываются без знака "-".

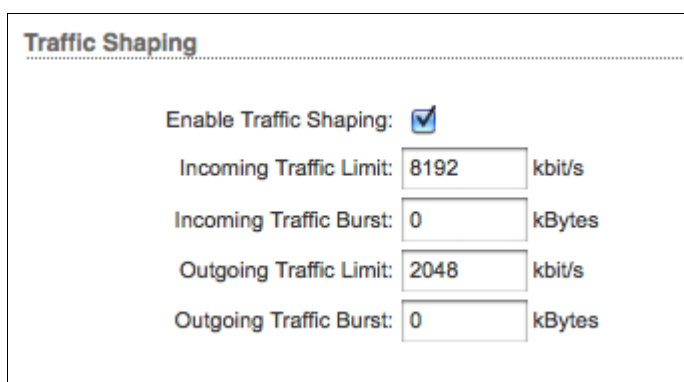
2.6.4 Traffic Shaping

Шейпинг (ограничение скорости) беспроводного трафика - функция предназначенная для контроля входящего и исходящего трафика с клиентской стороны (при подключении по Ethernet интерфейсу).

Устройства с AirOS могут ограничивать отдачу и загрузку основываясь на пользовательских ограничениях.

Enable Traffic Shaping: включает контроль пропускной способности устройства.

Incoming Traffic Limit: укажите максимальную пропускную способность (в килобитах в секунду) для трафика пропускаемого с беспроводного интерфейса



Traffic Shaping	
Enable Traffic Shaping:	<input checked="" type="checkbox"/>
Incoming Traffic Limit:	8192 kbit/s
Incoming Traffic Burst:	0 kBytes
Outgoing Traffic Limit:	2048 kbit/s
Outgoing Traffic Burst:	0 kBytes

на Ethernet.

Incoming Traffic Burst: укажите объем данных (в килобитах) которые будут проходить после инициации соединения без ограничений указанных в поле *Incoming Traffic Limit*.

Outgoing Traffic Limit: укажите максимальную пропускную способность (в килобитах в секунду) для трафика пропускаемого с Ethernet на беспроводной интерфейс.

Outgoing Traffic Burst: укажите объем данных (в килобитах) которые будут проходить после инициации соединения без ограничений указанных в поле *Outgoing Traffic Limit will*.

2.7 Страница Services

На этой вкладке доступна конфигурация сервисов таких как: SNMP, SSH, System Log и Ping Watchdog.

2.7.1 Ping WatchDog

Ping watchdog переводит устройство с AirOS v5.3 в режим постоянного пинга указанного пользователем IP адреса (например адрес интернет шлюза). Если указанный адрес запинговать, устройство автоматически перезагрузится. Это опция создает своего рода защитный механизм.

Ping Watchdog предназначен для длительного мониторинга конкретного соединения к удаленному хосту с использованием команды Ping. Ping работает посредством отправки ICMP пакета "эхо запроса" указанному хосту и ждет получения "эхо ответа". Если указанное количество ответов не приходит - устройство перезагружается.

Enable Ping Watchdog: включение инструмента Ping Watchdog.

IP Address To Ping: поле ввода IP адреса хоста для мониторинга.

Ping Interval: интервал (в секундах) между посылаемыми "эхо" запросами. Значение по умолчанию 300 секунд.

Startup Delay: временной интервал задержки (в секундах) до отправки первого "эхо" запроса. Значение по умолчанию 300 секунд.

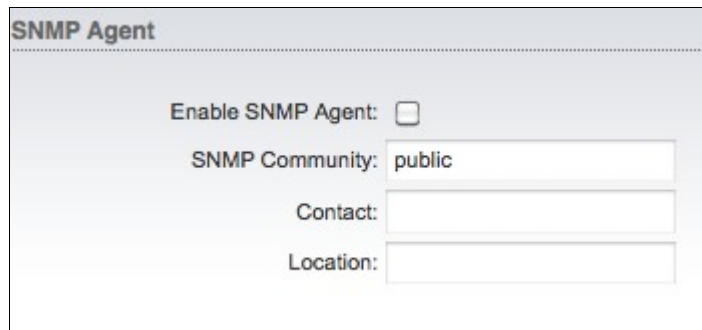
Величина Startup Delay должна быть не менее 60 секунд, так как инициализация соединения сетевого и беспроводного интерфейсов занимает некоторое время при перезагрузке устройства.

Failure Count to Reboot: количество "эхо" ответов ожидаемых устройством. Если указанное количество не будет получено в течении одного промежутка времени, Ping Watchdog перезагрузит устройство. Значение по умолчанию 3 пакета.

2.7.2 SNMP Agent

Simple Network Monitor Protocol (SNMP) используется для мониторинга подключаемых к сети устройств которые требуют внимания администратора. AirOS содержит SNMPагент, который позволяет ей взаимодействовать с SNMP программами для контроля сети.

SNMP агент обеспечивает интерфейс для мониторинга устройства используя Simple Network Management Protocol (протокол облегчающий обмен информацией для управления сетевыми устройствами). SNMP агент позволяет сетевому администратору следить за производительностью сети, находить и устранять сетевые неполадки. Для удобной идентификации оборудования следует сконфигурировать SNMP агент, указав в нем информацию о расположении оборудования и контактную информацию:



SNMP Agent

Enable SNMP Agent: ☐

SNMP Community: public

Contact:

Location:

Enable SNMP Agent: включение SNMP агента.

SNMP Community: укажите строку SNMP-группы. Это необходимо для авторизации доступа к объектам MIB (базы данных информации управления) и функциям таким как встроенный пароль. Устройство поддерживает общественную группу только для чтения, которая дает доступ авторизованным управляющим станциям ко всем объектам MIB кроме общественных групп. AirOS поддерживает SNMP v1. SNM-группа по умолчанию "public".

Contact: контактная информация для связи при возникновении экстренной ситуации.

Location: место расположения устройства.

2.7.3 Web Server

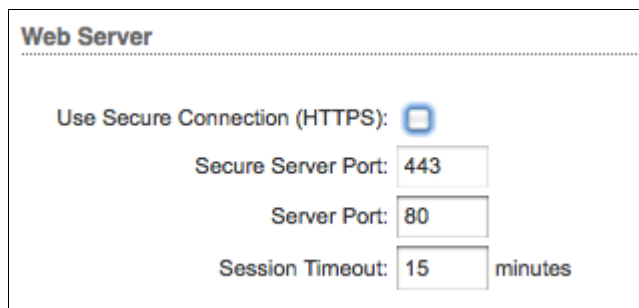
Web Server: в этом разделе можно настроить web сервер устройства с AirOS v5.3:

Use Secure Connection (HTTPS): если установлен флажок web сервер будет использовать режим безопасности HTTPS. По умолчанию этот режим отключен.

Secure Server Port: TCP/IP порт web сервера при использовании HTTPS.

Server Port: TCP/IP порт web сервера при использовании HTTP.

Session timeout: максимальная пауза до окончания сессии. После окончания сессии, для внесения изменений или просмотра главной страницы, вы должны заново авторизоваться используя учетные данные устройства.



Web Server

Use Secure Connection (HTTPS): ☒

Secure Server Port: 443

Server Port: 80

Session Timeout: 15 minutes

2.7.4 SSH Server

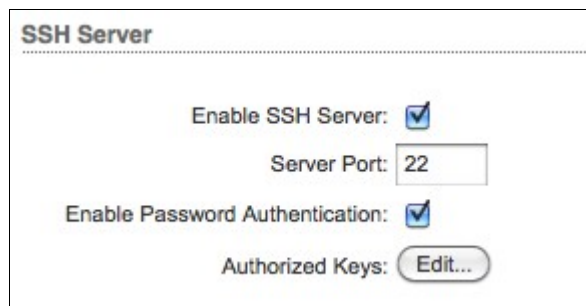
SSH Server: здесь могут быть сконфигурированы параметры SSH (англ. *Secure SHell* — «безопасная оболочка») сервера:

Enable SSH Server: включение опции позволяющей осуществлять доступ через SSH протокол.

Server Port: TCP/IP порт SSH сервиса.

Enable Password Authentication: если включено, для доступа к устройству по SSH необходимо использовать учетную запись администратора, в противном случае будет необходим ключ авторизации.

Authorized Keys: для импорта общего файла ключа для доступа по SSH без использования пароля администратора, нажмите кнопку “Browse” и выберите файл ключ, после нажмите “Import” и в завершении нажмите кнопку “Save”.



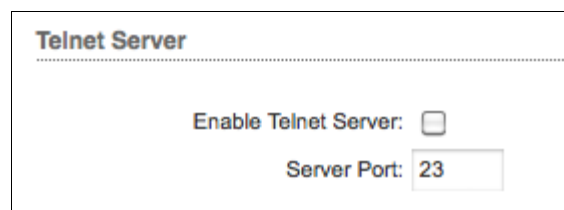
The screenshot shows the 'SSH Server' configuration window. It has a title bar 'SSH Server' and a dotted line separator. Below the separator, there are three settings: 'Enable SSH Server' with a checked checkbox, 'Server Port' with a text box containing '22', and 'Enable Password Authentication' with a checked checkbox. At the bottom, there is 'Authorized Keys' with an 'Edit...' button.

2.7.5 Telnet Server

Telnet Server: здесь могут быть сконфигурированы параметры Telnet сервера:

Enable Telnet Server: эта опция включает Telnet доступ к устройству.

Server Port: TCP/IP порт сервиса.



The screenshot shows the 'Telnet Server' configuration window. It has a title bar 'Telnet Server' and a dotted line separator. Below the separator, there are two settings: 'Enable Telnet Server' with an unchecked checkbox and 'Server Port' with a text box containing '23'.

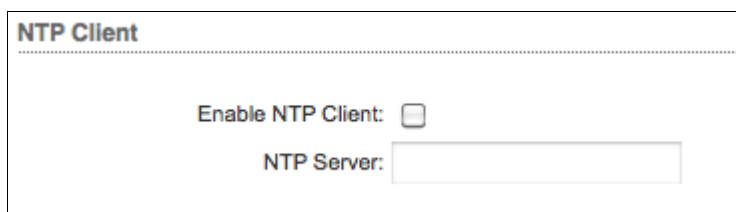
2.7.6 NTP Client

NTP Client: The Network Time Protocol (NTP) - сетевой протокол для синхронизации часов компьютера с использованием сетей с пакетной коммутацией, переменной латентностью. Это может быть использовано для установки системного времени AirOS.

Системное время указывается в каждой записи системного журнала событий, если включена опция журналирования.

Enable NTP Client: включение NTP клиента.

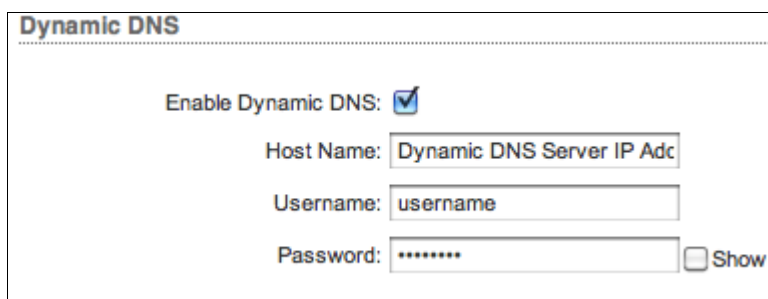
NTP Server: IP адрес или доменное имя NTP сервера.



The screenshot shows the 'NTP Client' configuration window. It has a title bar 'NTP Client' and a dotted line separator. Below the separator, there are two settings: 'Enable NTP Client' with an unchecked checkbox and 'NTP Server' with an empty text box.

2.7.7 Dynamic DNS

Enable Dynamic DNS: отметьте этот чекбокс для включения динамического DNS сервиса для устройства с AirOS. Динамический DNS - это сетевой сервис обеспечивающий уведомление DNS сервера в реальном времени о любых изменениях IP адреса устройства, тем самым обеспечивая доступ через доменное



The screenshot shows the 'Dynamic DNS' configuration window. It has a title bar 'Dynamic DNS' and a dotted line separator. Below the separator, there are four settings: 'Enable Dynamic DNS' with a checked checkbox, 'Host Name' with a text box containing 'Dynamic DNS Server IP Adc', 'Username' with a text box containing 'username', and 'Password' with a text box containing '*****' and a 'Show' checkbox.

имя даже если IP адрес устройства изменился.

Host Name: имя хоста динамического DNS.

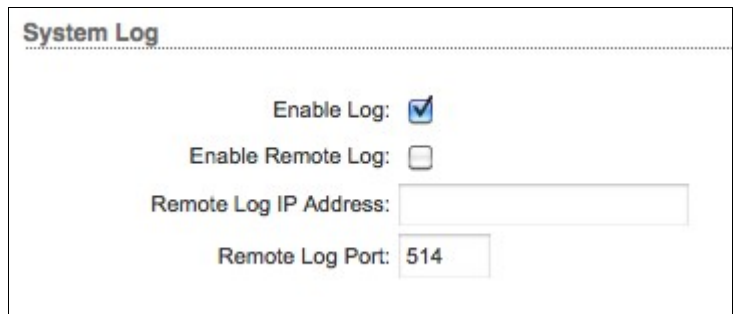
Username: имя пользователя динамического DNS.

Password: пароль динамического DNS. Пометка “show” позволяет отобразить пароль.

2.7.8 System Log

Enable Log: эта опция включает ведение системного журнала. По умолчанию опция отключена.

Enable Remote Log: включение функции отправки сообщений системного журнала на удаленный сервер, указанный в параметрах *Remote Log IP Address* и *Remote Log Port*.



Remote Log IP Address IP адрес хоста на который необходимо посылать сообщения системного журнала. Удаленный хост должен быть настроен на получение этих сообщений.

Remote Log Port: TCP/IP порт хоста на который необходимо посылать сообщения системного журнала. Порт по умолчанию для большинства утилит журналирования "514".

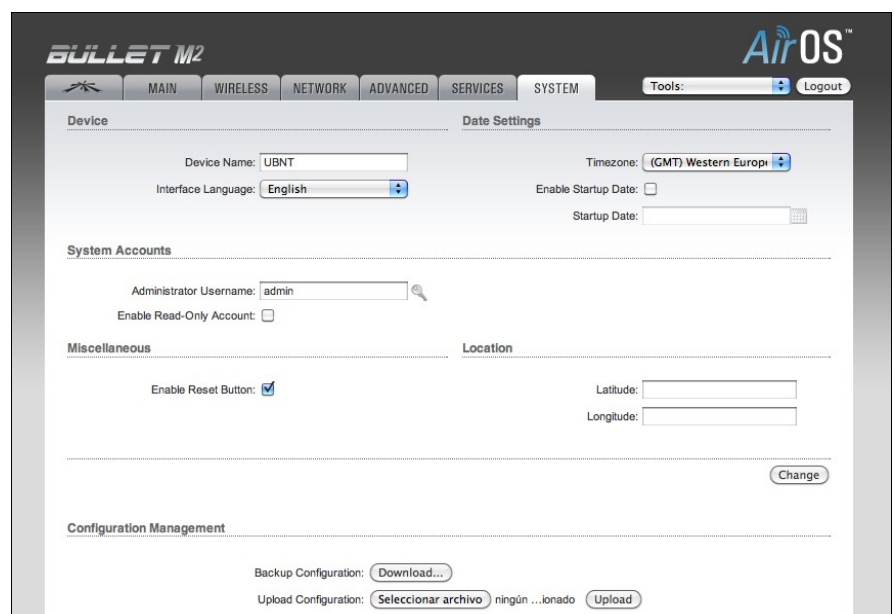
Каждое сообщение журнала содержит как минимум данные о системном времени и имя хоста. Обычно добавляется еще и имя службы которая создает запись в журнале. Сообщения от разных служб имеют различный контекст и содержание. Обычно выводятся сообщения об ошибках, предупреждения или информационные системные сообщения, однако могут выводиться и более детализированные сообщения по отладке. Чем больше детализированных сообщений выводится, тем больше объем журнала.

2.8 Страница System

Вкладка System содержит административные опции. Эта вкладка позволяет администратору перезагружать устройство, восстанавливать заводские настройки, обновлять ПО или конфигурацию, а так же управлять учетными данными администратора.

2.8.1 Device

Имя устройства (хоста) - идентификатор устройства в сети. SNMP агент сообщает его авторизованным управляющим станциям. Имя устройства будет



отображаться в большинстве операционных систем различных роутеров и утилитах обнаружения.

Device Name: идентификатор системы.

Interface Language: опция изменяет язык веб интерфейса устройства. Язык по умолчанию английский. Цвета и отображение всех элементов не изменяется.

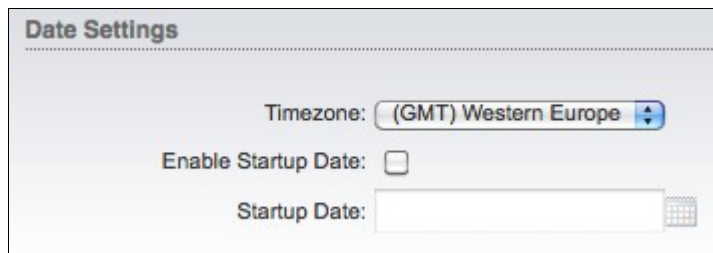
Кнопка **Change** сохраняет изменения в поле *Device Name*.

Так же могут быть загружены дополнительные языковые пакеты.

2.8.2 Date Settings

Timezone: выбор временной зоны относительно GMT (по Гринвичу).

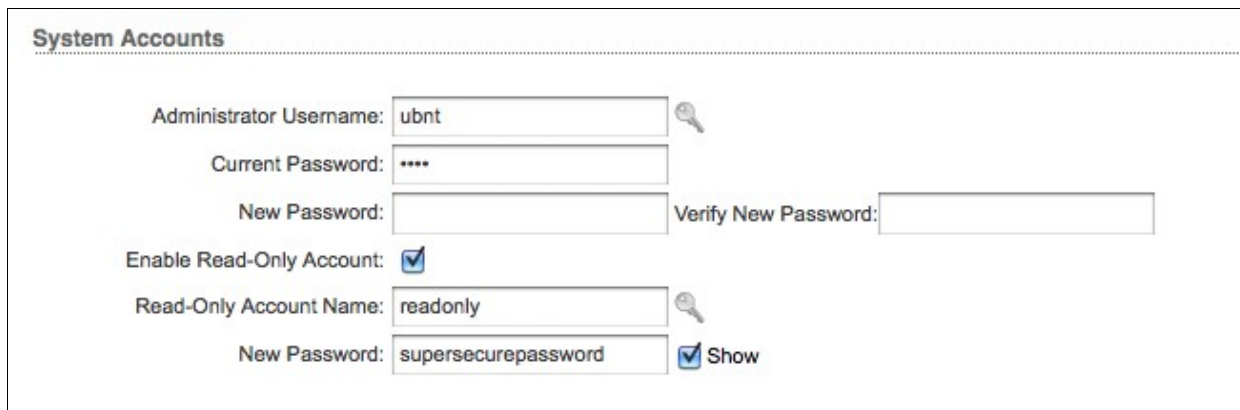
Enable Startup Date: когда опция активна, она позволяет редактировать дату запуска устройства. Это дата возврата устройства после каждой перезагрузки. Для поддержания времени и даты актуальными, настройте NTP клиент на вкладке Services.



Startup Date: установка даты запуска устройства. Дату можно выбрать нажав на иконку календаря или введя вручную в следующем формате: 2 цифры месяца, 2 цифры числа, 4 цифры года (например, для 6 мая 2010 года дата должна иметь такой вид - 05/06/2010).

2.8.3 System Accounts

В этом разделе вы можете



изменить пароль администратора для защиты вашего устройства от несанкционированного доступа. Пароль администратора по умолчанию должен быть изменен при первом запуске каждого устройства:

Administrator Username: имя пользователя с правами администратора.

Key button: нажмите на эту кнопку для смены пароля администратора.

Current Password: ввод текущего пароля администратора. это необходимо для изменения пароля и имени пользователя администратора.

Учетные данные администратора по-умолчанию:

- * Имя пользователя: ubnt
- * Пароль: ubnt

New Password: поле ввода нового пароля;

Verify Password: поле для повторного ввода пароля для избежания ошибок.

Примечание: пароль должен состоять из 8 символов максимум.

Enable Read-Only Account: включение аккаунта с правами только для чтения, и настройка имени пользователя и пароля для защиты устройства от несанкционированного доступа. По умолчанию эта опция отключена.

Read-Only Username: имя пользователя.

Key button: нажмите эту кнопку для смены пароля.

New Password: новый пароль для учетной записи с правами чтения.

Show: включение отображения символов пароля.

Нажмите на кнопку **Change** для сохранения изменений.

2.8.4 Miscellaneous

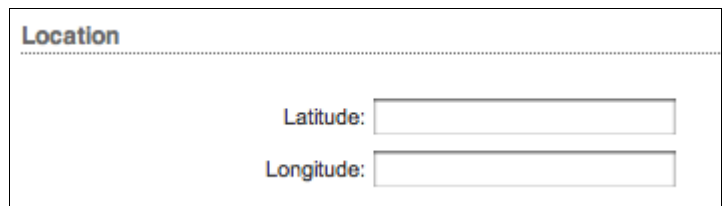
Enable Reset Button: эта опция позволяет включать или отключать кнопку reset. Это помогает избежать случайного сброса устройства к заводским настройкам. Если кнопка reset отключена, сброс настроек устройства возможен при помощи процедуры [TFTP Recovery](#).



The screenshot shows a section titled "Miscellaneous" with a dotted line separator. Below the separator, there is a label "Enable Reset Button:" followed by a checked checkbox icon.

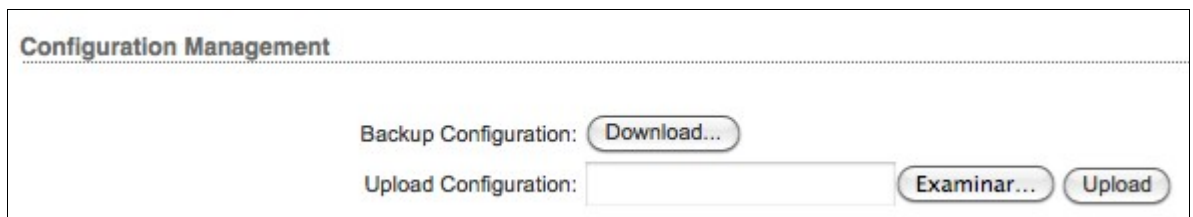
2.8.5 Location

Latitude (широта) и **Longitude** (долгота) - величины определяющие местоположения устройства. Они используются для автоматического обновления местоположения устройств в утилите AirControl.



The screenshot shows a section titled "Location" with a dotted line separator. Below the separator, there are two input fields. The first is labeled "Latitude:" and the second is labeled "Longitude:". Both fields are empty.

2.8.6 Configuration Management



The screenshot shows a section titled "Configuration Management" with a dotted line separator. Below the separator, there are two rows of controls. The first row is labeled "Backup Configuration:" and has a "Download..." button. The second row is labeled "Upload Configuration:" and has a text input field, followed by "Examinar..." and "Upload" buttons.

Конфигурация AirOS v5.3 хранится в виде обыкновенного текстового файла (cfg). При помощи раздела *Configuration Management* можно сохранить резервную копию, восстановить или обновить конфигурационный файл системы:

Backup Configuration: нажмите кнопку **Download** для загрузки резервной копии конфигурационного файла.

Upload Configuration: нажмите кнопку **Browse** для выбора файла конфигурации с вашего компьютера.

Нажатием на кнопку **Upload** загрузит новый конфигурационный файл в систему. Настройки новой конфигурации будут видны на вкладках *Wireless*, *Network*, *Advanced*, *Services* и *System*.

Новая конфигурация будет применена после нажатия кнопки *Apply* и полной перезагрузки системы. Предыдущая конфигурация будет удалена после нажатия на кнопку *Apply*. Строго рекомендуется сделать резервную копию текущей конфигурации перед загрузкой новой.

Используйте резервные копии конфигураций устройств только от устройств того же типа - созданные на устройствах Bullet M2 (или M5), Rocket M2 (или M5), NanoStation M2 (или M5)! Последствия от смешивания конфигураций различного типа устройств могут быть непредсказуемыми. Резервные копии AirOS v3.4 не совместимы с AirOS v5.3.

2.8.7 Device Maintenance

Настройки



расположенные в этом разделе предназначены для рутинных задач: перезагрузка, сброс, генерирование информационного отчета.

Firmware Version: отображает текущую версию программного обеспечения.

Build Number: отображение номера сборки версии программного обеспечения.

Update

Используйте этот раздел для обновления программного обеспечения устройства. Обновление программного обеспечения совместимо со всеми настройками устройства. Настройки системы сохраняются при обновлении.

2.8.7.1 Firmware upload

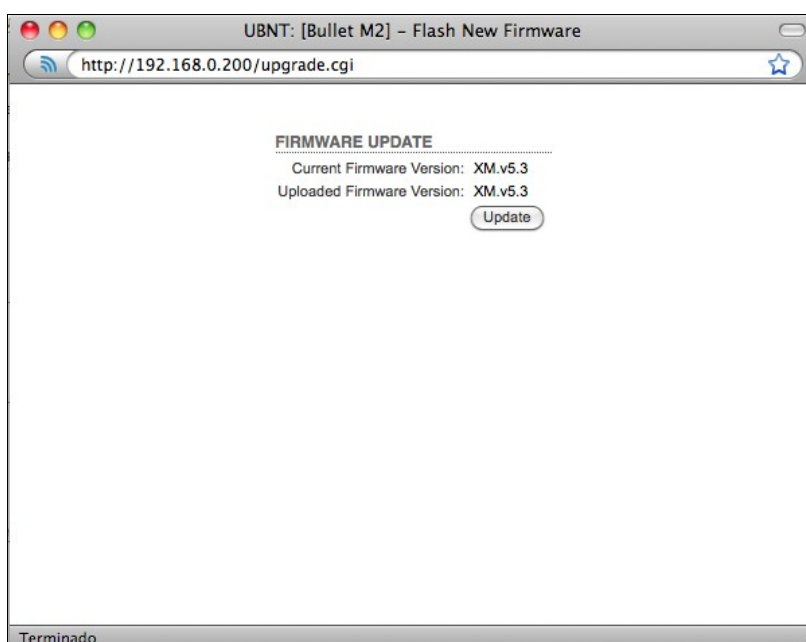
Current Firmware:

отображает текущую версию программного обеспечения.

Firmware File: нажмите на кнопку **Browse** для выбора файла обновления программного обеспечения. Новый файл будет загружен в систему после нажатия на кнопку **Upload**.

Close this window – отменяет загрузку программного обеспечения.

Кнопка **Update** позволяет загрузить файл обновления. Процесс обновления системы может занимать от 3 до 7 минут. Устройство будет недоступно до завершения процесса



обновления.

Не отключайте питание, не перезагружайте и не отсоединяйте устройство до завершения процесса обновления, это может повредить устройство!

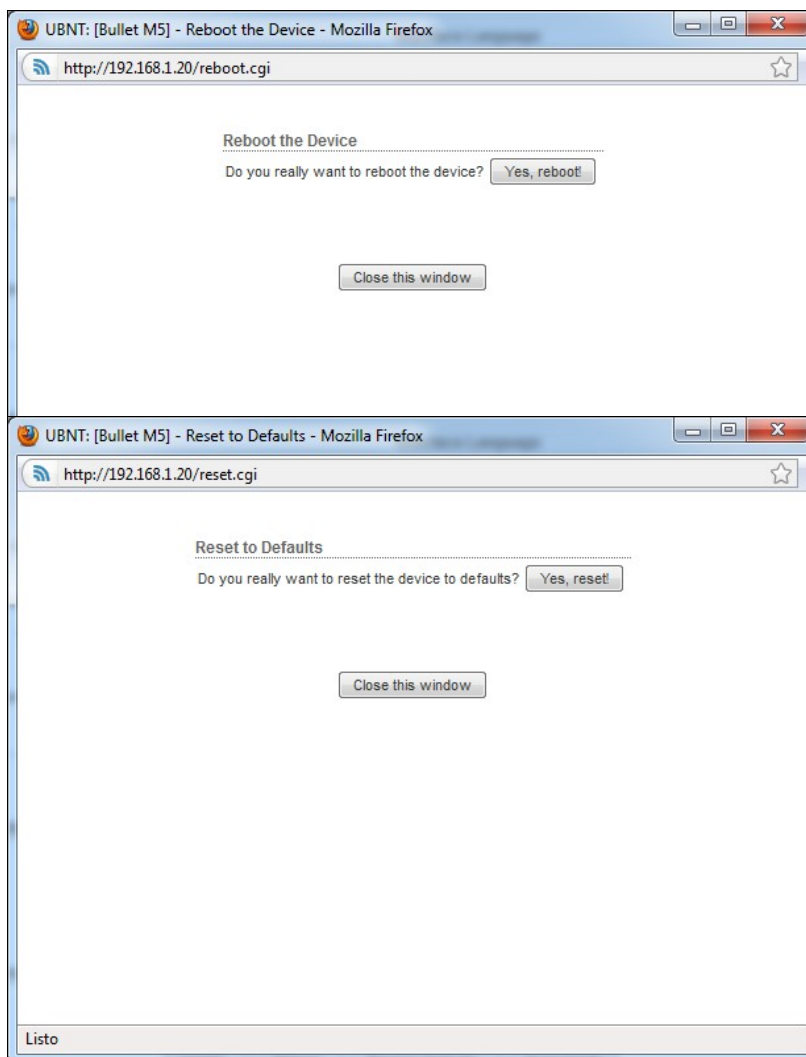
Настоятельно рекомендуется сделать резервную копию конфигурации информации о поддержке перед обновлением.

Close this window – эта кнопка закрывает окно обновления, но не отменяет его если процесс уже запущен.

Reboot: нажатие кнопки *Reboot* позволяет инициировать полную перезагрузку устройства. Процесс аналогичен нажатию на кнопку перезагрузки на самом устройстве или отключению/включению питания. Система не изменяется после перезагрузки. Все не сохраненные изменения будут утеряны.

Reset to Defaults: эта кнопка позволяет сбросить настройки устройства к заводским. Текущая конфигурация будет удалена и заменена на конфигурацию по умолчанию.

После завершения процесса сброса настроек устройство вернется к заводской конфигурации IP адреса (192.168.1.20/255.255.255.0) и будет работать в режиме *Station-Bridge*. Настоятельно рекомендуется сделать резервную копию конфигурации перед тем как сбросить все настройки.

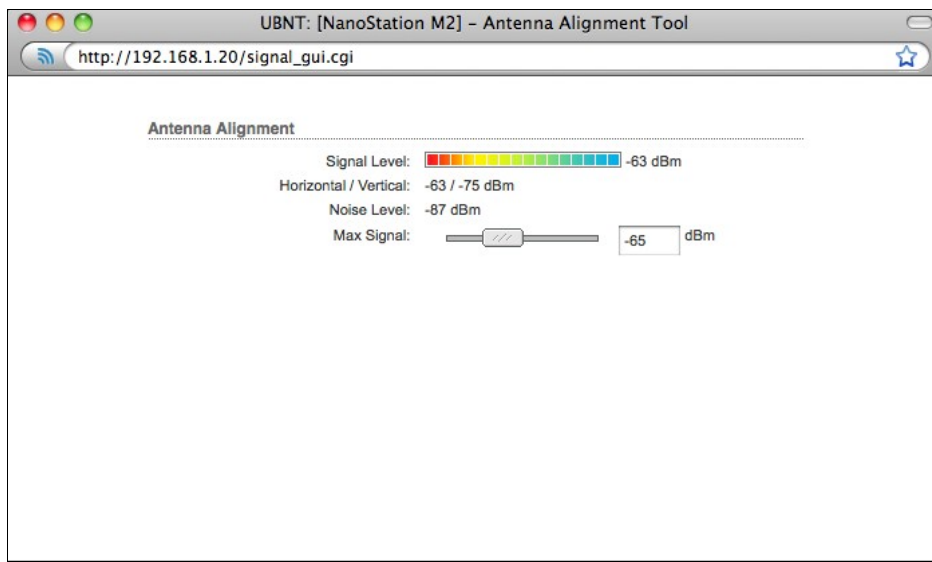


Support Info: нажатие на эту кнопку выводит файл информации о системе. Этот файл предоставляется инженерам Ubiquiti (по запросу) при возникновении неполадок в конфигурации.

2.9 Меню Tools

2.9.1 Align Antenna

Align Antenna - утилита помогающая направить антенну для получения максимального сигнала.



Выбор инструмента **Align Antenna** откроет новое окно с индикатором мощности. Оно обновляет каждую секунду отображаемую силу сигнала по последнему принятому пакету.

Horizontal/Vertical: отображает принимаемый сигнал для каждой поляризации, при работе в режиме Station (или Station WDS) устройств MIMO 2x2. Сигнал отображается в dBm.

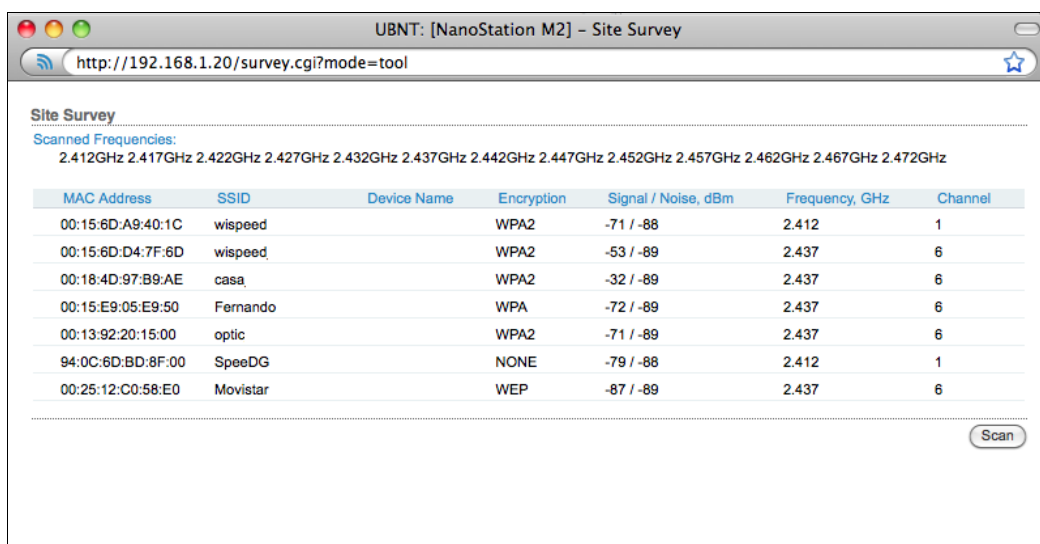
"Noise Level"(уровень шумов) - эта величина отображает уровень шумов при получении сигнала.

Слайдер "Max Signal" позволяет определить границы измерения. Если граница будет снижена цветовая шкала станет более чувствительна к колебаниям сигнала так как слайдер **Max Signal** фактически изменяет максимальное значение индикатора.

Окно *Align Antenna* может быть закрыто нажатием кнопки **Close this window**.

2.9.2 Site Survey

Site Survey: утилита для поиска всех доступных сетей в радиусе досягаемости на всех каналах при работе устройства в режиме *Access Point* или *Station*. В режиме *Station* список каналов можно изменить. См. раздел *Link Setup* для получения подробной информации об изменении списка каналов.



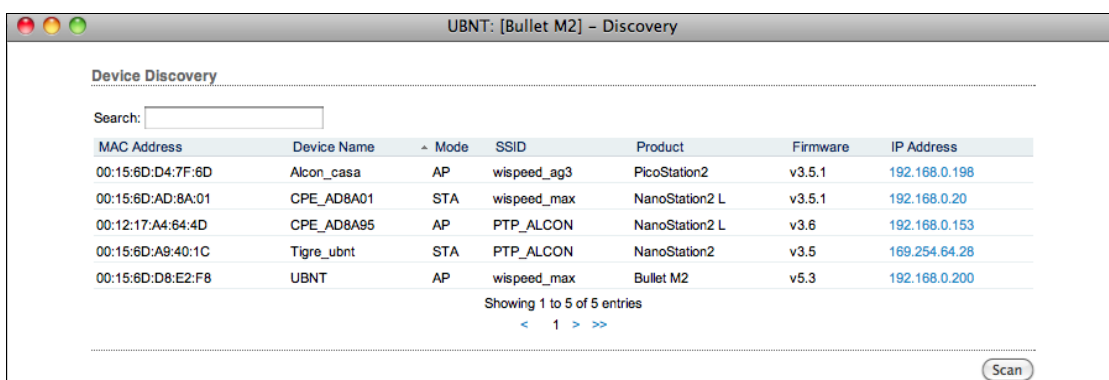
MAC Address	SSID	Device Name	Encryption	Signal / Noise, dBm	Frequency, GHz	Channel
00:15:6D:A9:40:1C	wispeed		WPA2	-71 / -88	2.412	1
00:15:6D:D4:7F:6D	wispeed		WPA2	-53 / -89	2.437	6
00:18:4D:97:B9:AE	casa		WPA2	-32 / -89	2.437	6
00:15:E9:05:E9:50	Fernando		WPA	-72 / -89	2.437	6
00:13:92:20:15:00	optic		WPA2	-71 / -89	2.437	6
94:0C:6D:BD:8F:00	SpeedG		NONE	-79 / -88	2.412	1
00:25:12:C0:58:E0	Movistar		WEP	-87 / -89	2.437	6

Site Survey выводит MAC адреса, SSID, имена устройств, тип шифрования (если используется), уровень сигнала/шума в *dBm*, частоту в *GHz* и используемый канал на всех точках доступа в зоне досягаемости устройства.

Утилита *Site Survey* может быть обновлена нажатием кнопки **Scan**. Окно утилиты закрывается кнопкой **Close this window**.

2.9.3 Device Discovery

Эта утилита сканирует сеть на присутствие всех устройств Ubiquiti Network в сети в которой находится устройство. В поле поиска



MAC Address	Device Name	Mode	SSID	Product	Firmware	IP Address
00:15:6D:D4:7F:6D	Alcon_casa	AP	wispeed_ag3	PicoStation2	v3.5.1	192.168.0.198
00:15:6D:AD:8A:01	CPE_AD8A01	STA	wispeed_max	NanoStation2 L	v3.5.1	192.168.0.20
00:12:17:A4:64:4D	CPE_AD8A95	AP	PTP_ALCON	NanoStation2 L	v3.6	192.168.0.153
00:15:6D:A9:40:1C	Tigre_ubnt	STA	PTP_ALCON	NanoStation2	v3.5	169.254.64.28
00:15:6D:D8:E2:F8	UBNT	AP	wispeed_max	Bullet M2	v5.3	192.168.0.200

можно задать фильтрацию по символам или цифрам.

Device Discovery: выводит MAC адрес, имя устройства, беспроводной режим, SSID, тип устройства, версию программного обеспечения и IP адрес. Для доступа к web интерфейсу устройства кликните на его Ip адрес.

Утилита Discovery может быть обновлена нажатием кнопки **Scan**.

2.9.4 Ping

Ping: эта утилита предназначена для пинга устройств в сети непосредственно с устройства под управлением AirOS.

Утилита Ping может быть использована для проверки качества соединения непосредственно между двумя устройствами в сети при помощи ICMP пакетов.

Host	Time	TTL
192.168.1.34	4.11 ms	64
192.168.1.34	4.08 ms	64
192.168.1.34	4.05 ms	64
192.168.1.34	4.05 ms	64
192.168.1.34	3.96 ms	64
192.168.1.34	4.05 ms	64

6 of 6 packets received, 0% loss

Min: 3.96 ms Avg: 4.05 ms Max: 4.11 ms

Start

IP адрес удаленного устройства может быть выбран из автоматически генерируемого списка или указан вручную.

Размер ICMP пакетов может быть указан в поле **Packet size**. Оценка производится после отправки/получения указанного в поле **Packet count** количества пакетов.

Статистика потери пакетов и время задержек выводится после завершения теста.

Запуск теста производится нажатием кнопки **Start**.

2.9.5 Traceroute

TraceRoute: позволяет отследить пререходы с устройства с AirOS к внешнему IP адресу. Это можно использовать для нахождения пути следования ICMP пакетов по сети к хосту назначения.

Разрешение IP-адресов (символически, а не численно) можно

#	Host	IP	Responses
1	192.168.1.20	192.168.1.20	10.193 ms · 2.281 ms · 2.836 ms

Start

включить, выбрав опцию **Resolve IP address**.

Запуск теста производится нажатием кнопки **Start**.

2.9.6 Speed Test

Эта утилита позволяет протестировать скорость соединения с любым устройством в сети. Ее можно использовать для измерения пропускной способности непосредственно между двумя устройствами.

Select Destination IP: IP адрес удаленной системы может быть выбран из автоматически генерируемого списка или указан вручную.

UBNT: [NanoStation M2] - Speed Test

http://192.168.1.21/sptest.cgi

Network Speed Test

Select Destination IP: 192.168.1.20

User: ubnt

Password: ****

Remote WEB Port: 80

☒ Show Advanced Options

Direction: duplex

Test Results

RX: 121.55 Mbps
TX: 47.09 Mbps
Total: 168.64 Mbps

Run Test

Так же необходимо иметь данные учетной записи (логин и пароль администратора) для связи двух устройств на базе AirOS. Это необходимо для проведения теста пропускной способности на основе протокола TCP/IP.

Remote WEB port: необходимо указать удаленный порт устройства с AirOS для проведения теста (например, 443 порт должен быть указан если на удаленном устройстве включена поддержка HTTPS). Если порт указан не верно, будет запущен тест на основе протокола ICMP.

Show advanced options: включение дополнительных настроек утилиты Speed Test. Всего три опции доступны для направления трафика при оценке максимальной пропускной способности:

Direction:

- Оценка входящей (Rx) пропускной способности при выборе варианта "получить";
- Оценка исходящей (Tx) пропускной способности при выборе варианта "передать";
- Оценка входящей (Rx) и исходящей (Tx) пропускной способности одновременно при выборе варианта "дуплекс".

Результаты теста

Rx: отображает входящую скорость.

Tx: отображает исходящую скорость.

Total: отображает суммарную скорость.

2.9.7 AirView

AirView это анализатор частоты встроенный в AirOS V5.3, который позволяет увидеть загрязненность радио спектра.

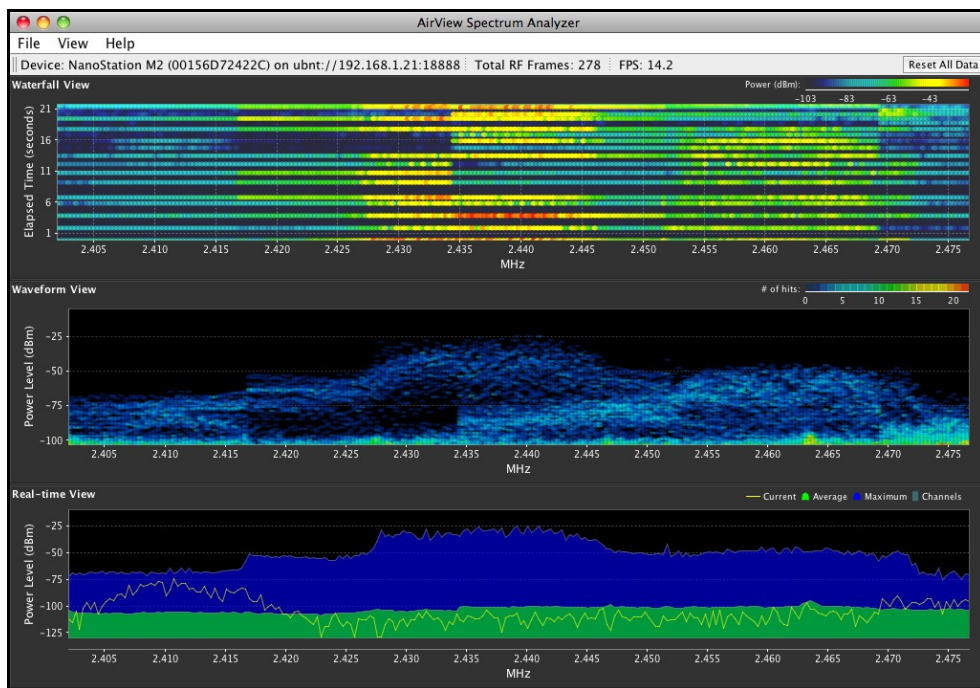
Вид:

Показать диаграмму 1 (верхняя): когда опция включена, отображается верхняя диаграмма, **Waterfall** или **Channel Usage**, в зависимости от выбранных настроек. Это временные графики отображают собранную энергию в совокупности или использование канала для каждой частоты за все время работы AirView.

Показать диаграмму 2 (средняя): когда опция включена, отображается средняя диаграмма **Waveform**. Это повременной график, показывающий совокупность собранной энергии для каждой частоты в течение всего времени работы. Цвет излучения определяет его амплитуду: холодные цвета выступают за более низкие уровни (с синее самого низкого уровня), в то время как теплые цвета (желтый, оранжевый или красный) означает более высокие энергетические уровни на этой частоте.

Показать диаграмму 3 (нижняя): когда опция включена, эта диаграмма отображает традиционный анализ спектра, в котором энергия (в dBm) показана в режиме реального времени как функция частоты.

Clear All Markers: нажмите эту кнопку для сброса всех установленных маркеров. Маркеры устанавливаются кликом на точке соответствующей частоте на третьей диаграмме.



2.9.7.1 Main View

Device: отображает имя, MAC и IP адрес устройства на котором запущена AirView.

Total RF Frames: отображает общее число RF фреймов собранных за время работы AirView с момента последнего нажатия кнопки "Reset All Data".

FPS: отображает общее количество фреймов собираемых за секунду. Чем больше интервал в амплитуде тем меньше фреймов в секунду будет собрано.

Reset All Data: нажмите на эту кнопку для сброса всех собранных данных. Используете эту функцию когда хотите проанализировать спектр в другом месте.

2.9.7.2 Preferences

В этом разделе вы можете изменить настройки AirView, такие как включение/отключение диаграмм или указать частотный интервал.

Диаграммы

Показать верхнюю диаграмму: выберете диаграмму отображаемую в верхней части. Всего два варианта: Waterfall или Channel Usage.

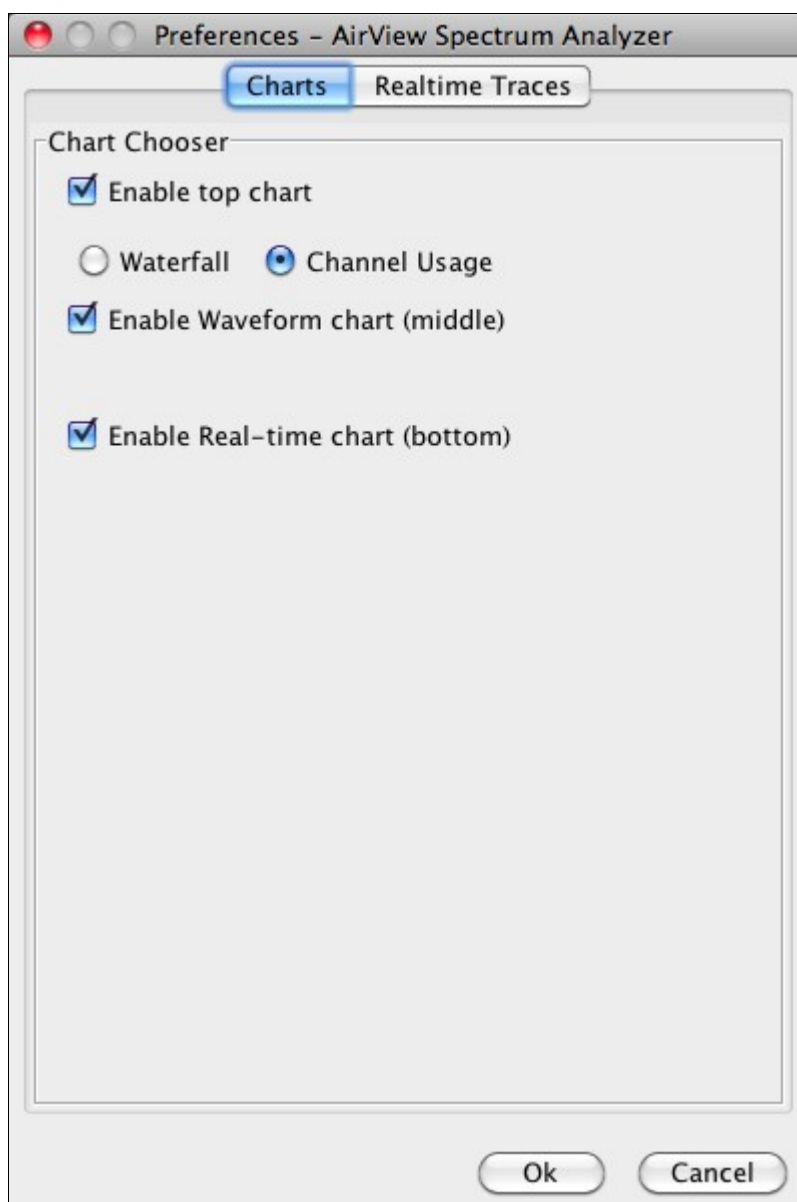
Waterfall: Это повременной график, который показывает совокупность энергии накопленной за время работы AirView на каждой частоте. Цвет энергии определяет его амплитуду: холодные цвета выступают за более низкие энергетические уровни (синее самого низкого уровня) на этой частоте, в то время как теплые цвета (желтый, оранжевый или красный) означают более высокие энергетические уровни.

Легенда (в правом верхнем углу) обеспечивает численную привязку различных цветов к различным уровням мощности (dBm). Низкий уровень этой легенды (слева) всегда соответствует расчетному уровню шума, а высокий уровень (справа) установлен на наивысший уровень мощности сигнала обнаруженного с начала сессии.

Channel Usage: на этом графике, каждый 2,4 GHz (или 5 GHz для устройств серии M5) Wi-Fi канал представлен в виде процентного графика относительной "плотности" этого конкретного канала. Этот процент рассчитывается на основе анализа количества источников и мощности излучения радиочастот в этом канале с начала сессии AirView.

Показать диаграмму Waveform (средняя): как и Waterfall, это повременной график, показывающий совокупность собранной энергии для каждой частоты в течение всего времени работы AirView. Цвет излучения определяет его амплитуду: холодные цвета выступают за более низкие уровни (с синее самого низкого уровня), в то время как теплые цвета (желтый, оранжевый или красный) означает более высокие энергетические уровни на этой частоте. Длительный анализ спектра помогает определить постоянные источники радио сигнала в данной среде.

Показать диаграмму Real-time (нижняя): эта диаграмма отображает традиционный анализ спектра, в котором энергия (в dBm) показана в режиме реального времени в зависимости от



частоты. На диаграмме отображаются три различных графика : Max Hold – этот график будет обновлять и удерживать максимальный уровень мощности на частоте с момента запуска AirView. Average – показывает среднее значение энергии на частоте. Real-time - показывает в режиме реального времени уровень энергии улавливаемый устройством AirView в зависимости от частоты.

Realtime Traces

Эти настройки применимы к диаграмме Real-time:

Current Real-time Trace: когда опция включена, будет отображаться график реального времени. Этот график представляет собой желтую линию на диаграмме, отображающую уровень мощности для каждой частоты в реальном времени. Скорость обновления зависит от параметра FPS.

Averages Trace: Это зеленая зона на третьей диаграмме, которая отображает средний уровень полученного сигнала и считает данные все время пока работает AirView. Этот график можно отключить сняв соответствующую отметку в чекбоксе “Enable”. Или можно включить только зеленую линию без затененной области, сняв пометку с чекбокса “Shaded Area”.

Maximum Power Trace: это синяя зона на третьей диаграмме, которая отображает максимальное значение мощности полученного сигнала за все время работы AirView. Этот график может быть отключен снятием пометки с чекбокса “Enable”. Или можно оставить только синюю линию без затененной области сняв пометку с чекбокса “Shaded Area”.

Frequency Range: здесь вы можете выбрать амплитуду частотного интервала для сканирования. Есть несколько предустановленных диапазонов в наиболее популярных частотах. Однако вы можете указать свой диапазон в зависимости от ваших нужд.

