СЕРИЯ ОБОРУДОВАНИЯ MLink

MLink-WNET-C33R

Руководство пользователя

МИКРОЛИНК-СВЯЗЬ

Версия:1.2

Код документа: ML-WNET-C33R 25.1.7

Дата выпуска: май 2009г.

Микролинк-Связь

111395 г. Москва
ул. Аллея Первой Маевки, д. 15, оф. 501.
Тел./факс: 941-99-19
E-mail: info@microlink.ru
Http:// www.microlink.ru

Оглавление

Аббревиатуры

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
CCK	Complementary Code Keying
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/ Collision Detection
DDNS	Dynamic Domain Name Server
DH	Diffie-Hellman Algorithm
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control
MD5	Message Digest 5
NAT	Network Address Translation
NT	Network Termination
NTP	Network Time Protocol
PPTP	Point to Point Tunneling Protocol
PSD	Power Spectral Density
RF	Radio Frequency
SHA1	Secure Hash Algorithm
SNR	Signal to Noise Ratio
SSID	Service Set Identification TCP Transmission Control Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UPNP	Universal Plug and Play
VPN	Virtual Private Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 Введение

Беспроводной широкополосный LAN маршрутизатор – это доступное по цене решение для стандарта IEEE 802.11b/g, устанавливающее стандарты высокой производительности для малых офисов и предприятий, безопасную, управляемую и надёжную беспроводную локальную сеть.

В данном документе описаны шаги по настройке WLAN маршрутизатора.

1.1 Комплектация

В комплектацию широкополосного WLAN маршрутизатора входят следующие элементы: широкополосный WLAN маршрутизатор, AC/DC адаптер питания, CD с документацией.

1.2 Техническая характеристика изделия

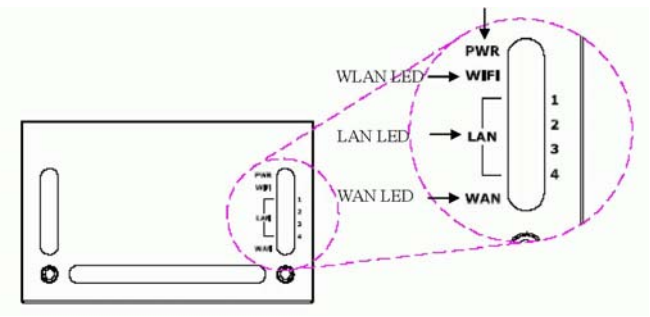
Название устройства	WLAN широкополосный маршрутизатор
Стандарты	802.11b/g(Wireless), 802.3(10BaseT), 802.3u(100BaseT)
Скорость передачи данных	54Мб/сек (Wireless), 100Мб/сек (Ethernet)
Метод модуляции	CCK(802.11b), OFDM(802.11g)
Полоса частот	2.4ГГц – 2.497ГГц ISM, DSSS
RF выходная мощность	CCK< 17 dBm, OFDM< 13.5 dBm
Чувствительность приёмника	802.11b -80 dBm, 802.11g -68 dBm
Зона покрытия	от 30 до 280 метров
Антенна	Внешняя съемная антенна
Индикаторы	Power, Active (WLAN/Ethernet)
Безопасность	64-битное/128-битное WEP-шифрование, WPA, WPA2, фильтрация на порту, фильтрация по IP, фильтрация по MAC, переадресация (перенаправление) портов и DMZ.
LAN интерфейс	1 (WAN), 4 (LAN) , 10/100BaseT, RJ45
Потребляемая мощность	7.5В DC адаптер источника питания
Рабочие температуры	0 ~ 50ºC: температура окружающей среды
Температуры хранения	-20 ~ 70ºC: температура окружающей среды
Влажность	от 5 до 90 % максимум (без конденсации)
Размеры	118x95x25мм (модель A) 120x75x26мм (модель B)

1.3 Свойства устройства

- ✓ Взаимодействие со стандартом IEEE 802.11b/g для 2.4 ГГц WLAN;
- ✓ Поддержка многооперационных режимов (bridge/gateway/WISP) между беспроводными и проводными Ethernet интерфейсами;
- ✓ 64/128-битное WEP-, WPA-, WPA2- шифрование для защиты передачи данных по радиосвязи;
- ✓ Поддержка аутентификации IEEE 802.1x;

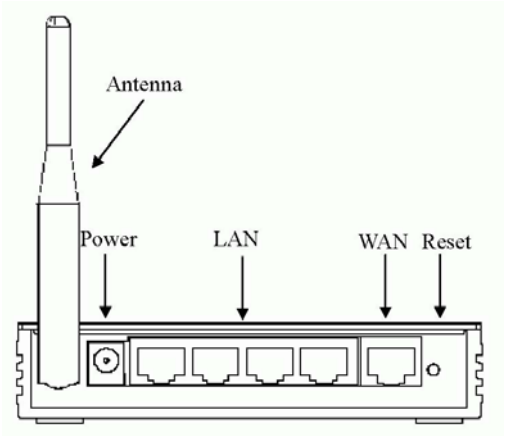
- ✓ Поддержка защищённого метода аутентификации Wi-Fi с использованием RADIUS сервера и режима Pre-Shared Key;
- ✓ Поддержка протокола IAPP (Inter-Access Point Protocol);
- ✓ Поддержка WDS (Wireless Distribution System);
- ✓ Поддержка IEEE 802.3x full duplex flow control на интерфейсе 10/100M;
- ✓ Поддержка DHCP-сервера для автоматического назначения IP адреса клиенту;
- ✓ Поддержка DHCP-клиента для автоматического назначения IP адреса от провайдера WAN-интерфейсе;
- ✓ Поддержка PPPoE на WAN-интерфейсе;
- ✓ Поддержка PPTP- клиента на WAN-интерфейсе;
- ✓ Поддержка функции клонирования MAC адресов;
- ✓ Поддержка безопасного брандмауэра с использованием: фильтрации на порту, IP фильтрации, MAC фильтрации, перенаправлением портов, trigger port, DMZ и функции фильтрации URL;
- ✓ Поддержка веб-интерфейса для настройки и конфигурации;
- ✓ Поддержка UPnP для автоматического доступа к Интернет;
- ✓ Поддержка DDNS;
- ✓ Поддержка сервисов NTP-клиента;
- ✓ Поддержка таблицы логов и службы удалённых логов;
- ✓ Поддержка установки в режиме помощника;
- ✓ Поддержка функции DoS (Denial of Service);
- ✓ Поддержка функции WMM;
- ✓ Поддержка Ping watchdog;
- ✓ Поддержка функции контроля QoS/Bandwidth;
- ✓ Поддержка соединения VPN;
- ✓ Поддержка шифрования IPSEC (3DES/AES128) и аутентификации (MD5/SHA1);

1.4 Описание модели (модель А)



Описание состояния индикаторов

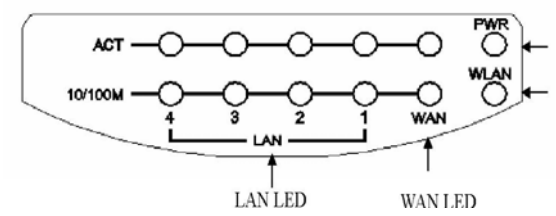
Индикаторы	Статус	Описание
Индикатор питания	Вкл.	WLAN маршрутизатор включен
	Выкл.	WLAN маршрутизатор выключен
Индикатор WLAN	Мигание	Антенна принимает или передаёт данные
	Выкл.	Антенна не принимает и не передаёт данные
Индикатор LAN	Мигание	Данные принимаются или передаются на LAN-интерфейсе
	Вкл.	Порт активен
	Выкл.	Нет активности
Индикатор WAN	Мигание	Данные принимаются или передаются на WAN-интерфейсе
	Вкл.	Порт активен
	Выкл.	Нет активности



Описание интерфейсов

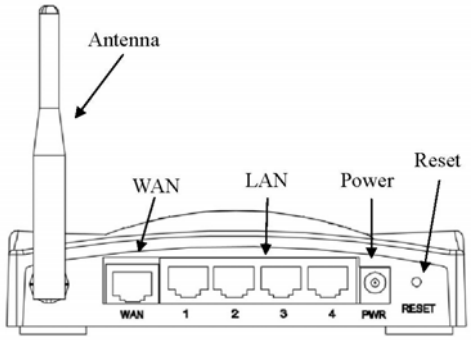
- *Antenna* - WLAN антенна (съемная/ разъем SMA);
- *Power* - Разъем питания DC +7.5;
- *LAN* - Гнёзда RJ-45 обеспечивают LAN-подключение с помощью кабелей UTP 5-й категории. Поддержка авто-определения скорости 10/100M в режиме полного дуплекса и полудуплекса; совместимость с IEEE 802.3/802.3u;
- *WAN* - Гнёзда RJ-45 обеспечивают WAN-подключение с помощью кабелей UTP 5-й категории. Поддержка авто-определения на скорости 10/100M в режиме полного дуплекса и полудуплекса; совместимость с IEEE 802.3/802.3u;

1.5 Описание панели (модель B)



Описание состояния индикаторов

Индикаторы	Статус	Описание
Индикатор питания	Вкл.	WLAN маршрутизатор включен
	Выкл.	WLAN маршрутизатор выключен
Индикатор WLAN	Мигание	Антенна принимает или передаёт данные
	Выкл.	Антенна не принимает и не передаёт данные
Индикатор LAN	Мигание	Данные принимаются или передаются на LAN-интерфейсе
	Выкл.	Нет активности
10/100 M	Вкл.	Скорость подключения на LAN-интерфейсе составляет 100 Мбит/сек
	Выкл.	Скорость подключения на LAN-интерфейсе составляет 10 Мбит/сек
Индикатор WAN	Мигание	Данные принимаются или передаются на WAN-интерфейсе
	Выкл.	Нет активности
10/100 M	Вкл.	Скорость подключения на WAN-интерфейсе составляет 100 Мбит/сек
	Выкл	Скорость подключения на WAN-интерфейсе составляет 10 Мбит/сек



Описание интерфейсов

- *Антенна* - Антенна WLAN;
- *WAN* - Гнёзда RJ-45 обеспечивают WAN-подключение с помощью кабелей UTP 5-й категории. Поддержка авто-определения на скорости 10/100M в режиме полного дуплекса и полудуплекса; совместимость с IEEE 802.3/802.3u;
- *LAN* - Гнёзда RJ-45 обеспечивают LAN-подключение с помощью кабелей UTP 5-й категории. Поддержка авто-определения на скорости 10/100M в

режиме полного дуплекса и полудуплекса; совместимость с IEEE 802.3/802.3u;

- *Power* - Разъем питания DC +7.5;

2 Установка

2.1 Установка оборудования

Шаг 1: Расположите широкополосный WLAN маршрутизатор для оптимальной передачи данных. Обычно, лучшее положение широкополосного WLAN маршрутизатора для передачи это центр вашей беспроводной сети с прямой видимостью для всех ваших мобильных станций.

Шаг 2: Подключите широкополосный WLAN маршрутизатор к вашей проводной сети. Подключите WAN-интерфейс Ethernet-кабелем 5-й категории к вашему коммутатору/хабу/xDSL-модему или кабельному модему. Требуется прямой Etrhernet-кабель.

Шаг 3: Подайте DC-питание на широкополосный WLAN-маршрутизатор. Используйте только AC/DC источник питания, поддерживаемый этим маршрутизатором; использование альтернативного источника питания может повредить устройство.

Установка оборудования закончена.

2.2 Ввод в действие системы программного обеспечения

Не требуется установка никаких драйверов, пэтчей и утилит, только установка конфигурации. Пожалуйста, обратитесь к главе 3 для получения детальной информации о настройке конфигурации.

ВНИМАНИЕ: Загрузка широкополосного WLAN маршрутизатора занимает около 55 секунд после включения устройства; индикатор питания будет включен, и затем замигает индикатор WLAN Activity, как признак того, что WLAN-интерфейс включен и работает нормально.

3 Конфигурация

Для упрощения вашей работы существуют веб-интерфейс.

Широкополосный WLAN маршрутизатор оснащён следующими заводскими параметрами на LAN-интерфейсах. IP адрес по умолчанию: ***192.168.1.254***. Маска подсети по умолчанию: ***255.255.255.0***.

Логин: <***пусто***>. Пароль: <***пусто***>.

3.1 Подготовка вашего компьютера к настройке широкополосного WLAN маршрутизатора

Для ОС Microsoft Windows 95/98/Me:

1. Нажмите кнопку ***Start (Пуск)*** и выберите ***Settings (Параметры)***, затем кликните по ***Control Panel (Панель управления)***. После этого появится окно ***Control Panel.*** **Внимание**: Пользователи Windows ME могут не обнаружить Контрольную панель. Если так и случилось, нажмите **View all Control Panel options** на левой стороне окна.
2. Кликните два раза правой кнопкой мыши по иконе ***Network.*** Появится окно ***Network***.
3. Проверьте список установленных компонентов ***Network Components***. Если не установлен TCP/IP, кликните по ***Add (Добавить)***, для установки; в противном случае перейдите к пункту 6.
4. Выберите ***Protocol*** в диалоговом окне ***Network Component Type*** и кликните по ***Add.***
5. Выберите ***TCP/IP*** в диалоговом окне ***Microsoft Select Network Protocol*** и затем кликните OK для установки протокола TCP/IP, возможно, вам понадобится установочный диск Microsoft Windows CD для завершения установки. Закройте это окно и перейдите вновь к диалоговому окну ***Network*** после установки TCP/IP.
6. Выберите ***TCP/IP*** и кликните по опции ***Properties (Свойства)*** в диалоговом окне ***Network.***
7. Выберите ***Specify an IP address (Установка IP-адреса)*** и введите данные как показано в следующем примере: IP адрес: **192.168.1.1**, Любой IP адрес из диапазона 192.168.1.1 - 192.168.1.253 подойдёт для подключения WLAN точки доступа. Маска подсети: **255.255.255.0.**
8. Нажмите OK для перезагрузки вашего компьютера после завершения установки IP параметров.

Для ОС Microsoft Windows 2000, XP:

1. Нажмите кнопку ***Start*** и выберите ***Settings***, затем кликните по ***Control Panel***. После этого появится окно ***Control Panel.***
2. Кликните два раза правой кнопкой мыши по иконе ***Network and Dial-up Connections.*** Появится окно ***Local Area Connection.*** Кликните по кнопке ***Properties*** в окне ***Local Area Connection.***

3. Проверьте список установленных компонентов ***Network Components.*** Если не установлен TCP/IP, кликните по ***Add***, для установки; в противном случае перейдите к пункту 6.
4. Выберите ***Protocol*** в диалоговом окне ***Network Component Type*** и кликните по ***Add.***
5. Выберите ***TCP/IP*** в диалоговом окне ***Microsoft Select Network Protocol*** и затем кликните OK для установки протокола TCP/IP, возможно, вам понадобится установочный диск Microsoft Windows CD для завершения установки. Закройте это окно и перейдите вновь к диалоговому окну ***Network*** после установки TCP/IP.
6. Выберите ***TCP/IP*** и кликните по опции ***Properties*** в диалоговом окне ***Network.***
7. Выберите ***Specify an IP address*** и введите данные как показано в следующем примере: IP адрес: **192.168.1.1**, Любой IP адрес из диапазона 192.168.1.1 - 192.168.1.253 подойдёт для подключения WLAN точки доступа. Маска подсети: **255.255.255.0.**
8. Нажмите OK для перезагрузки вашего компьютера после завершения установки IP параметров.

Для ОС Microsoft Windows NT:

1. Нажмите кнопку ***Start*** и выберите ***Settings***, затем кликните по ***Control Panel***. После этого появится окно ***Control Panel.***
2. Кликните два раза правой кнопкой мыши по иконе ***Network.*** Появится окно ***Network***. Кликните по ***Protocol*** в окне ***Network.***
3. Проверьте список установленных компонентов ***Network Components.*** Если не установлен TCP/IP, кликните по ***Add***, для установки; в противном случае перейдите к пункту 6.
4. Выберите ***Protocol*** в диалоговом окне ***Network Component Type*** и кликните по ***Add.***
5. Выберите ***TCP/IP*** в диалоговом окне ***Microsoft Select Network Protocol*** и затем кликните OK для установки протокола TCP/IP, возможно, вам понадобится установочный диск Microsoft Windows CD для завершения установки. Закройте это окно и перейдите вновь к диалоговому окну ***Network*** после установки TCP/IP.
6. Выберите ***TCP/IP*** и кликните по опции ***Properties*** в диалоговом окне ***Network.***

7. Выберите ***Specify an IP address*** и введите данные как показано в следующем примере: IP адрес: **192.168.1.1**, Любой IP адрес из диапазона 192.168.1.1 - 192.168.1.253 подойдёт для подключения WLAN точки доступа. Маска подсети: **255.255.255.0.**
8. Нажмите ОК для перезагрузки вашего компьютера после завершения установки IP параметров.

3.2 Подключение к широкополосному WLAN маршрутизатору

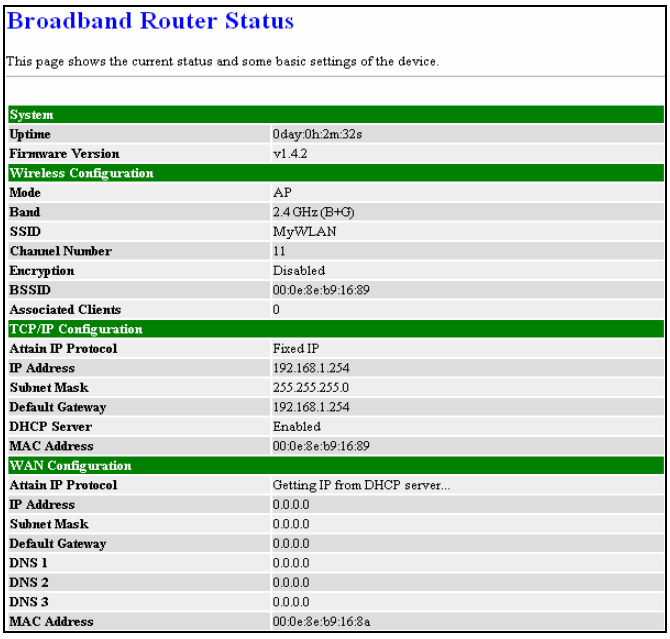
Откройте веб-браузер, например Microsoft Internet Explorer, затем введите 192.168.1.254 в поле URL для подключения к широкополосному WLAN маршрутизатору.

3.3 Управление и настройка широкополосного WLAN маршрутизатора

3.3.1 Статус

На этой странице отображен текущий статус и некоторые основные настройки устройства, включая настройки системы, радиосвязи, информацию о настройке интерфейсов Ethernet LAN и WAN.

Окно статуса маршрутизатора:



Broadband Router Status

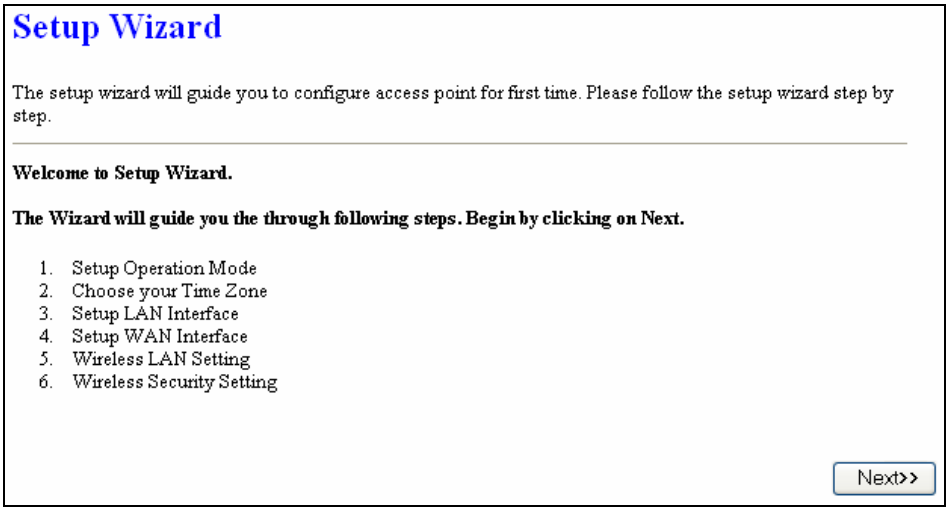
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:2m:32s
Firmware Version	v1.4.2
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	MyWLAN
Channel Number	11
Encryption	Disabled
BSSID	00:0e:8e:b9:16:89
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:0e:8e:b9:16:89
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS 1	0.0.0.0
DNS 2	0.0.0.0
DNS 3	0.0.0.0
MAC Address	00:0e:8e:b9:16:8a

Наименование	Описание
System	
Uptime	Показывает время работы широкополосного WLAN маршрутизатора
Firmware Version	Показывает версию прошивки широкополосного WLAN маршрутизатора
Wireless Configuration	
Mode	Показывает режим работы радиосвязи
Band	Показывает текущую рабочую частоту радиосвязи
SSID	Показывает SSID широкополосного WLAN маршрутизатора. SSID – это уникальное имя широкополосного WLAN маршрутизатора, транслируемое на зоне уверенного радиоприёма таким образом, что все устройства, присоединяющиеся к той же беспроводной сети, определяют его.
Channel Number	Показывает настоящий номер канала, по которому работает радиосвязь
Encryption	Показывает статус функции шифрования
BSSID	Показывает адрес BSSID широкополосного WLAN маршрутизатора. BSSID – это 6-байтовый адрес
Associated Clients	Показывает количество подключенных клиентов (или станций, компьютеров)
TCP/IP Configuration	
Attain IP address	Показывает тип подключения
IP Address	Показывает IP адрес LAN-интерфейса широкополосного WLAN маршрутизатора
Subnet Mask	Показывает маску подсети LAN-интерфейса широкополосного WLAN маршрутизатора
Default Gateway	Показывает шлюз по умолчанию для исходящих пакетов данных LAN-интерфейса
DHCP Server	Показывает, включен ли DHCP сервер
MAC Address	Показывает MAC адрес LAN-интерфейса широкополосного WLAN маршрутизатора
WAN Configuration	
Attain IP Protocol	Показывает, как широкополосный WLAN маршрутизатор получает IP адрес. IP адрес может быть установлен вручную, получен автоматически от DHCP сервера или получен по PPPoE/PPTP подключению
IP address	Показывает IP адрес WAN-интерфейса широкополосного WLAN маршрутизатора
Subnet Mask	Показывает маску подсети широкополосного WLAN маршрутизатора
DNS1/DNS2/DNS3	Показывает информацию о DNS сервере

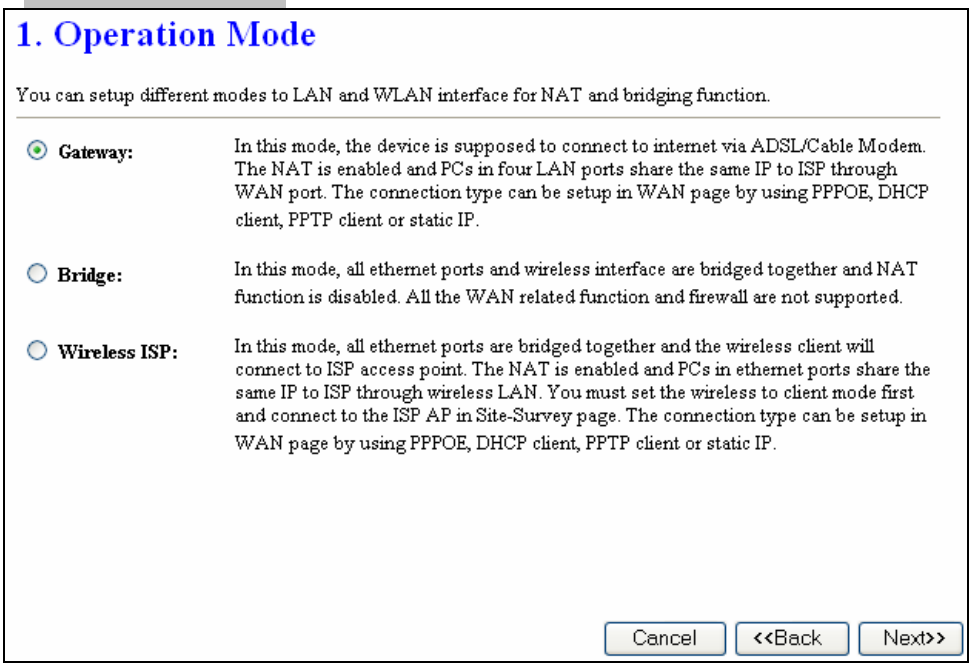
3.3.2 Помощник настройки

Эта страница поможет вам настроить широкополосный маршрутизатор при первом подключении.



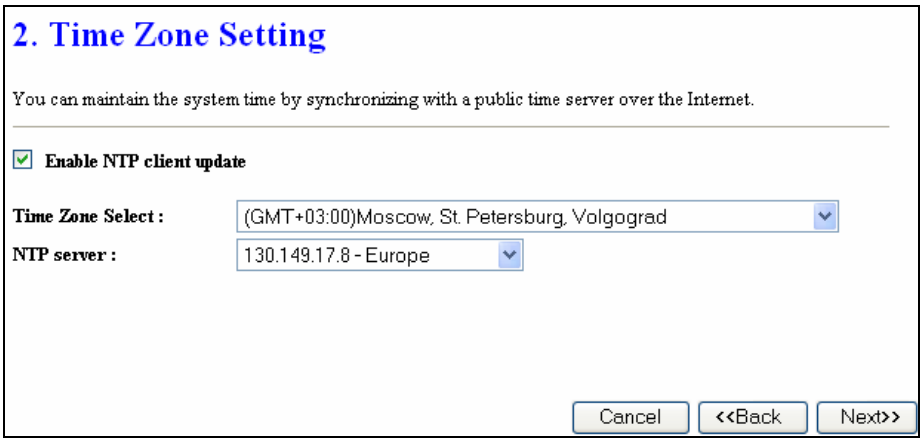
Operation Mode

Эта страница следует за страницей Setup Wizard и показывает возможность выбора режима работы:



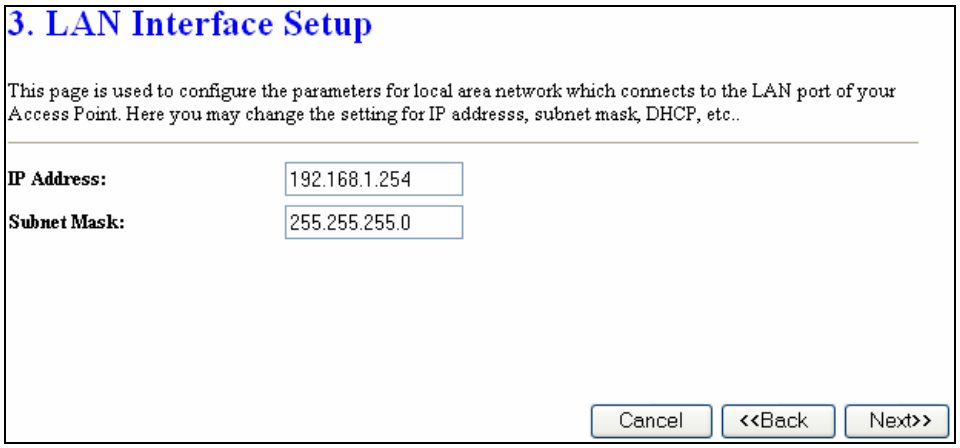
Time Zone Setting

На этой странице включается и настраивается NTP-клиент.



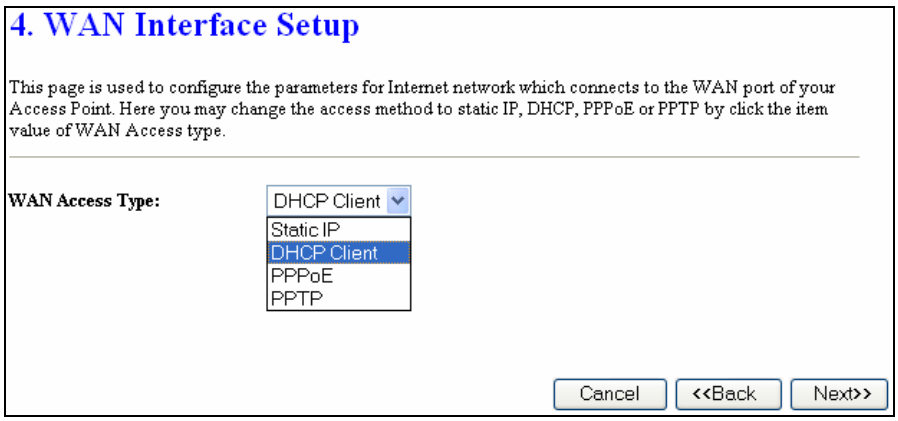
LAN Interface Setup

На этой странице настраивается IP адрес локальный сети и маска подсети:



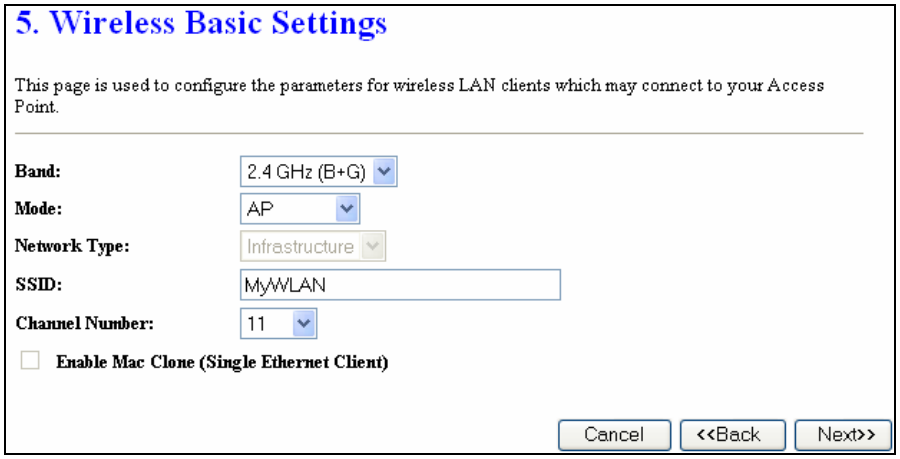
WAN Interface Setup

На этой странице тип доступа по WAN-интерфейсу:



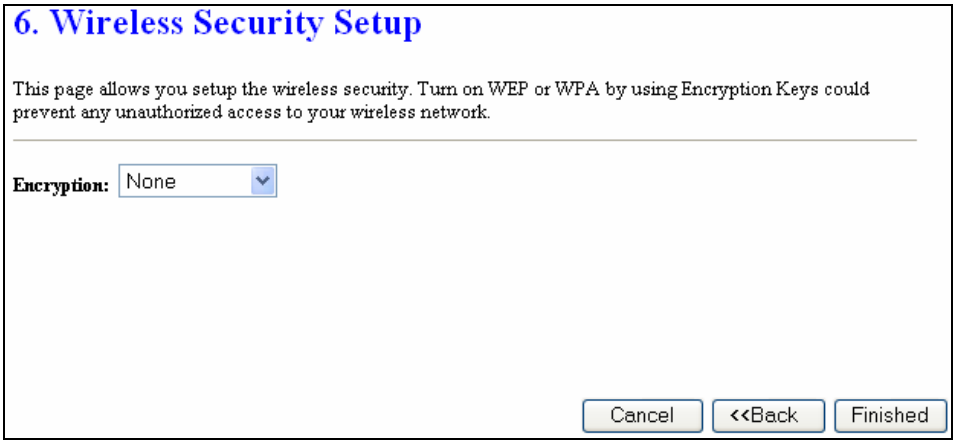
Wireless Basic Settings

На этой странице настраиваются основные параметры радиосвязи: полоса частот, режим, тип SSID, номер канала, клонирование MAC адресов (Single Ethernet Client).



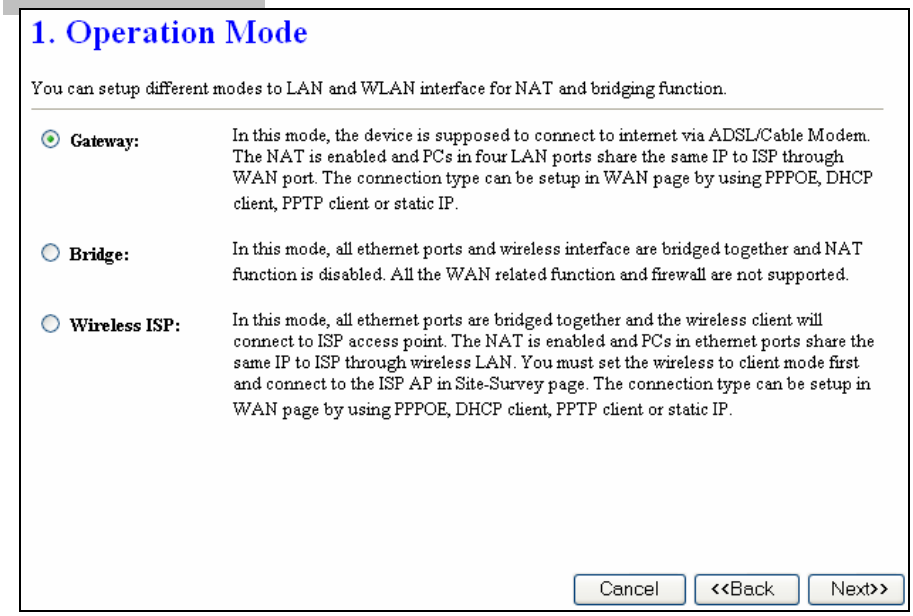
Wireless Security Setup

На этой странице настраивается безопасность радиосвязи.



3.3.3 Режим работы

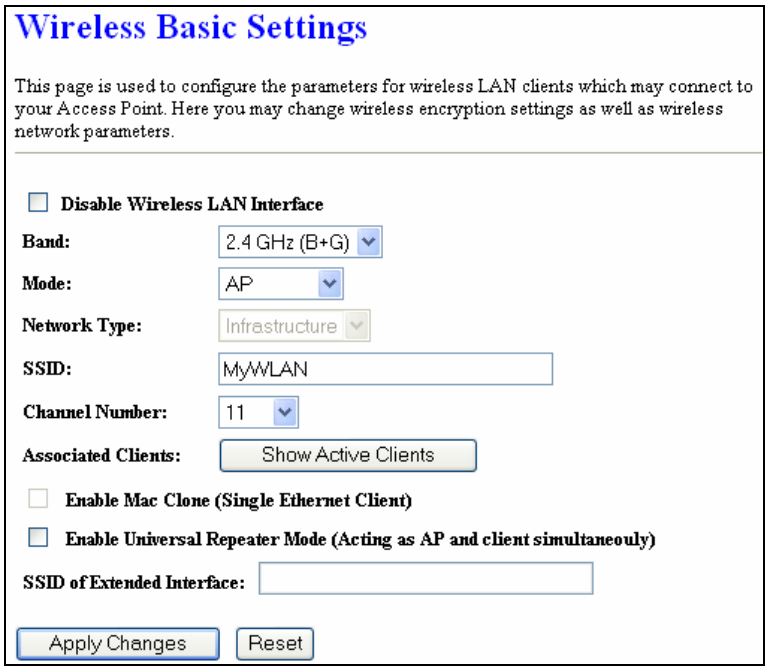
На этой странице настраивается режим работы широкополосного маршрутизатора:



Наименование	Описание
Gateway	Стандартная настройка шлюза. Она используется для подключения к Интернет через ADSL/кабельный модем, LAN-интерфейс, WAN-интерфейс, Wireless интерфейс. NAT и Firewall модули применяются в этом режиме
Bridge	Каждый интерфейс (WAN, LAN и Wireless) считается бриджом. NAT, Firewall и все функции маршрутизации не поддерживаются
Wireless ISP	Переключает wireless Интерфейс в WAN и все Ethernet порты в режим бриджа. Wireless интерфейс способен выполнять все функции маршрутизации
Apply Changes	Нажмите на эту кнопку для завершения и сохранения настроек
Reset	Нажмите на кнопку ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям.

3.3.4 Основные радио-настройки

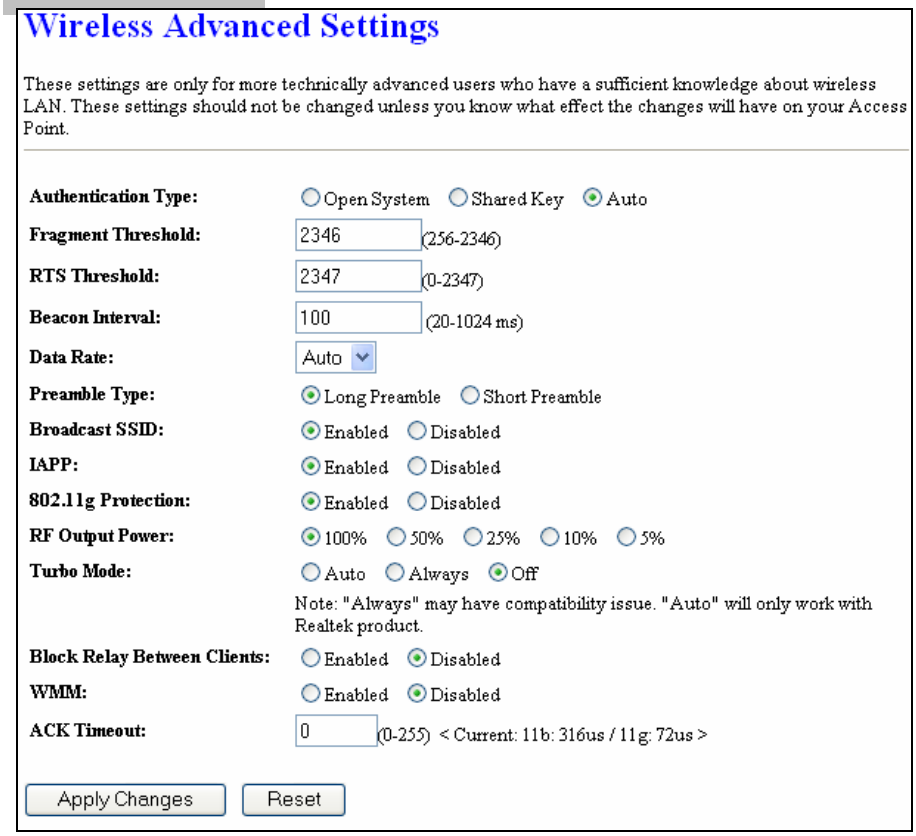
Эта страница используется для настройки параметров для клиентов беспроводной сети, которые могут подключаться к вашему широкополосному маршрутизатору. Здесь вы можете изменить настройки безопасности так же легко, как и остальные параметры радиосвязи.



Наименование	Описание
Disable Wireless LAN Interface	Кликните по полю рядом с этой опцией для отключения передачи данных по LAN
Band	Кликните для выбора 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(B+G)
Mode	Кликните для выбора беспроводного режима WLAN AP / Client / WDS / AP+WDS
SSID	Это имя беспроводной сети. SSID может быть длинной 32 байт
Channel Number	Выбор номера канала
Associated Clients	Кликните по кнопке ***Show Active Clients*** для того, чтобы открыть таблицу активных беспроводных клиентов, которая показывает MAC адрес, передаваемые пакеты, получаемые пакеты и скорость передачи данных для каждого связанного беспроводного клиента
Enable Mac Clone	Назначает MAC адрес сетевой карточки ноутбука MAC адресом беспроводного клиента (только в клиентском режиме)
Enable Universal Repeater Mode	Кликните для включения этой функции Universal Repeater Mode
SSID of Extended Interface	Назначает SSID, если включена функция Universal Repeater Mode
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.5 Особые настройки радиосвязи

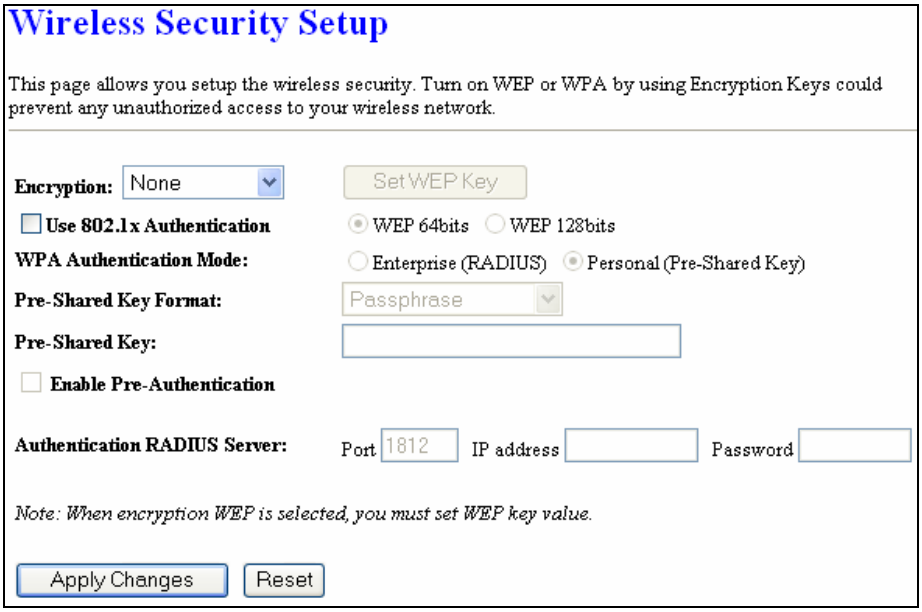
Эти настройки – только для пользователей, которые обладают достаточными знаниями о беспроводных сетях. Не следует менять эти настройки до тех пор, пока вы не убедитесь в том, каковы будет последствия их изменения для широкополосного WLAN маршрутизатора.



Наименование	Описание
Authentication Type	Кликните для выбора типа аутентификации: ***Open System***, ***Shared Key*** или ***Auto***
Fragment Threshold	Установка порога для фрагментации пакета данных, значения могут варьироваться от 256 до 2346 байт (см. параграф 4.10 - Что такое Fragment Threshold?)
RTS Threshold	Установка порога RTS, значение может варьироваться от 0 до 2347 байт
Beacon Interval	Установка интервала времени для радио маяка, значение может варьироваться от 20 до 1024 мс
Data Rate	Выберите скорость передачи данных из нисходящего меню. Скорость передачи может быть выбрана автоматически, 11M, 5,5M, 2M или 1 Мбит/сек
Preamble Type	Кликните для выбора поддержки ***Long Preamble*** или ***Short Preamble*** для беспроводной передачи пакетов данных. (см.параграф 4.13 - Что такое Preambule Type?)
Broadcast SSID	Кликните для включения или выключения функции широковещательной передачи SSID. (см. параграф 4.14 - Что такое SSID Broadcast?)
IAPP	Включите или выключите функцию IAPP. (см. параграф 4.20 - Что такое протокол IAPP?)
802.11g Protection	Защита пользователя 802.11b
RF Output Power	Регулировка мощности передатчика
Turbo Mode	Кликните для включения/выключения турбо режима
Block Relay Between Clients	Кликните Enable/Disable для решения о ретрансляции пакетов между клиентами
WMM	Кликните Enable/Disable для инициации свойства WMM.
ACK Timeout	Установите значения таймаута для ACK. Оно показывает текущее время
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям.

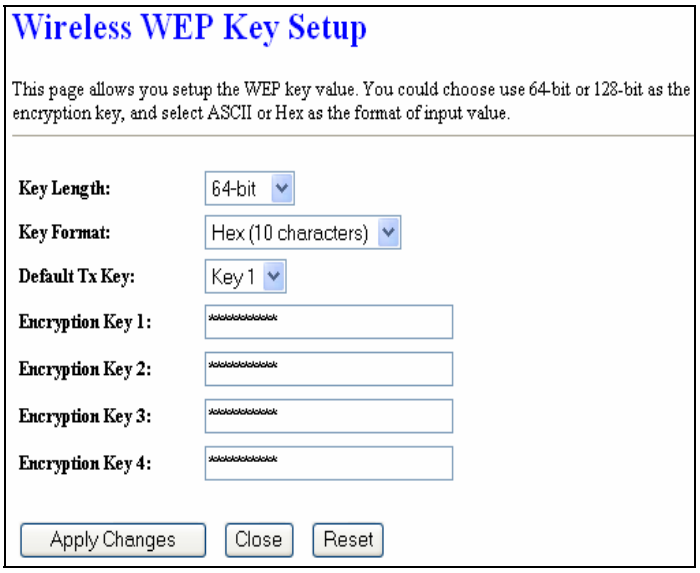
3.3.6 Настройки безопасности

На этой странице вы можете настроить различные режимы безопасности. Включив WEP, WPA, WPA2 и используя ключи шифрования, вы сможете предотвратить несанкционированный доступ к вашей беспроводной сети.



Наименование	Описание
Encryption	Выберите метод шифрования, используемый для доступа к беспроводной сети. Методы шифрования могут быть следующими: None, WEP, WPA(TKIP), WPA2 или WPA2 Mixed. См. параграфы: 4.9 Что такое WEP? 4.15 Что такое WPA? 4.16 Что такое WPA2 (AES)? 4.17 Что такое 802.1X Authentication? 4.18 Что такое Temporal Key Integrity Protocol (TKIP)? 4.19 Что такое Advanced Encryption Standard (AES)?
Use 802.1x Authentication	Используется вместе с WEP-шифрованием. Кликните по полю, чтобы включить функцию аутентификации IEEE 802.1x. (см. параграф 4.17 - Что такое 802.1X Authentication?)
WPA Authentication Mode	Используется вместе с WPA-шифрованием. Кликните для выбора режима аутентификации WPA с Enterprise (RADIUS) или Personal (Pre-Shared Key). (см. параграф 4.15 - Что такое WPA?)
Pre-Shared Key Format	Используется вместе с WPA-шифрованием. Выберите формат pre-shared key из нисходящего меню. Формат может быть Passphrase или Hex (64 символа). **[WPA, Personal(Pre-Shared Key) только]**
Pre-Shared Key	Введите ключ. **[WPA, Personal(Pre-Shared Key) только]**
Enable Pre-Authentication	Кликните для включения Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise только]
Authentication RADIUS Server	Задайте IP адрес, информацию о порте и пароле для аутентификации на RADIUS сервере
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

Установка WEP-ключа

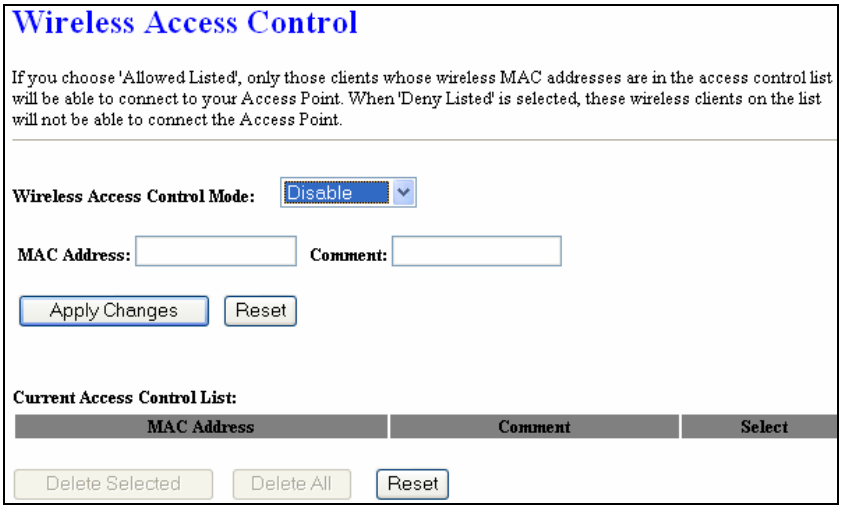


Наименование	Описание
Key Length	Выбор длинны секретного ключа. Длина может выбираться между 64 и 128 (шифрование, известное, как WEP-2) битами ключа. WEP-ключ составлен из вектора инициализации и секретного ключа (40-битного или 104-битного)
Key Format	Выберите формат WEP-ключа из нисходящего меню. Формат может быть выбран из ASCII и HEX кодами.
Default Tx Key	Установка секретного ключа по умолчанию для функции WEP-шифрования
Encryption Key 1	Секретный ключ 1 функции WEP-шифрования
Encryption Key 2	Секретный ключ 2 функции WEP-шифрования
Encryption Key 3	Секретный ключ 3 функции WEP-шифрования
Encryption Key 4	Секретный ключ 4 функции WEP-шифрования
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Close	Кликните для того, чтобы закрыть окно настройки WEP-ключа
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям.

3.3.7 Контроль доступа к радиосвязи

Если вы включили контроль доступа к радиосвязи, то доступ к вашей точке доступа будут иметь только те клиенты, чьи MAC адреса находятся в списке контроля доступа.

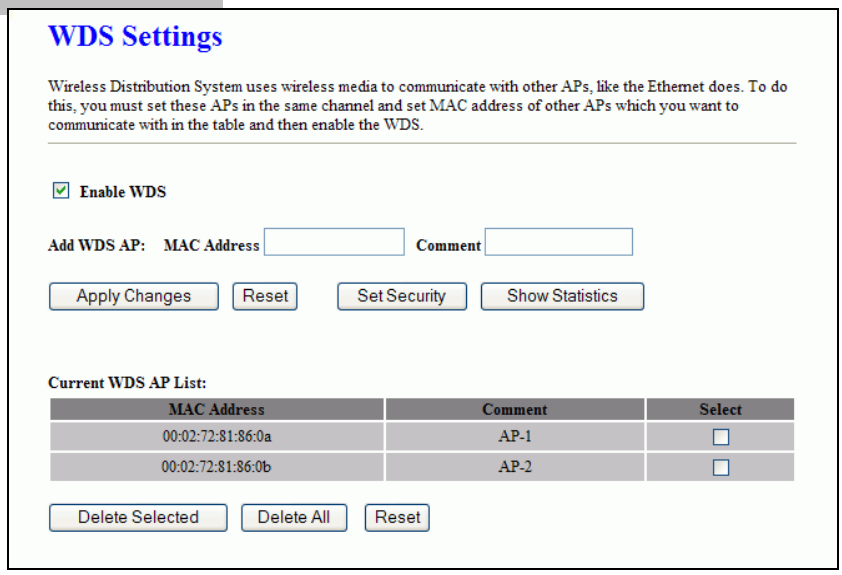
Когда эта функция включена, ни один из клиентов не будет иметь право доступа, если список контроля доступа пуст.



Наименование	Описание
Wireless Access Control Mode	Выберите ***Disabled***, ***Allow Listed*** или ***Deny Listed*** для определения режима контроля доступа к радиосвязи. Это функция контроля доступа; только зарегистрированные клиенты из списка контроля доступа будут иметь доступ к широкополосному WLAN маршрутизатору
MAC Address	Введите MAC адрес клиента для регистрации возможности доступа к широкополосному WLAN маршрутизатору
Comment	Введите комментарий для зарегистрированного клиента
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям.
Current Access Control List	Показывает зарегистрированных клиентов, которым разрешен доступ к широкополосному WLAN маршрутизатору
Delete Selected	Кликните для удаления выбранных клиентов, которым будет перекрыт доступ к широкополосному WLAN маршрутизатору
Delete All	Кликните для удаления всех зарегистрированных клиентов из разрешенного списка доступа
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям.

3.3.8 Настройки WDS

Wireless Distribution System использует радиосвязь для коммуникации с другими точками доступа, как это делает, например, Ethernet. Для того, чтобы это сделать, вы должны поместить эти точки доступа в один канал и установить MAC адрес другой точки доступа, к которой вы хотите подключиться, в таблице и затем включить WDS.



Наименование	Описание
Enable WDS	Отметьте поле для включения WDS. (см. параграф 4.21 - Что такое WDS?)
MAC Address	Введите MAC адрес точки доступа для регистрации возможности доступа WDS
Comment	Введите комментарий для зарегистрированного клиента
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям.
Set Security	Кликните по этой кнопке для настройки безопасности радиосвязи: ***WEP(64bits), WEP(128bits), WPA(TKIP), WPA2(AES)*** или ***None***
Delete Selected	Кликните для удаления выбранных клиентов, которым будет перекрыт доступ к широкополосному WLAN маршрутизатору
Delete All	Кликните для удаления всех зарегистрированных клиентов из разрешенного списка доступа
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

Настройка безопасности WDS

Шаги по настройки: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS.

Страница используется для настройки безопасности радиосвязи между точками доступа. Обратитесь к параграфу 3.3.6 Настройка безопасности.

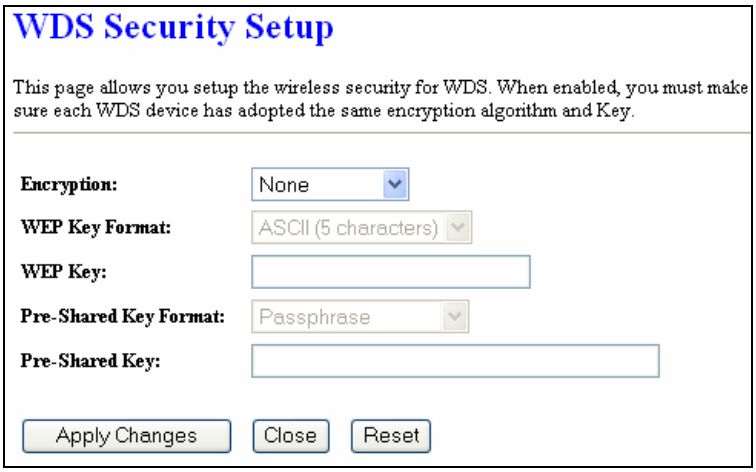
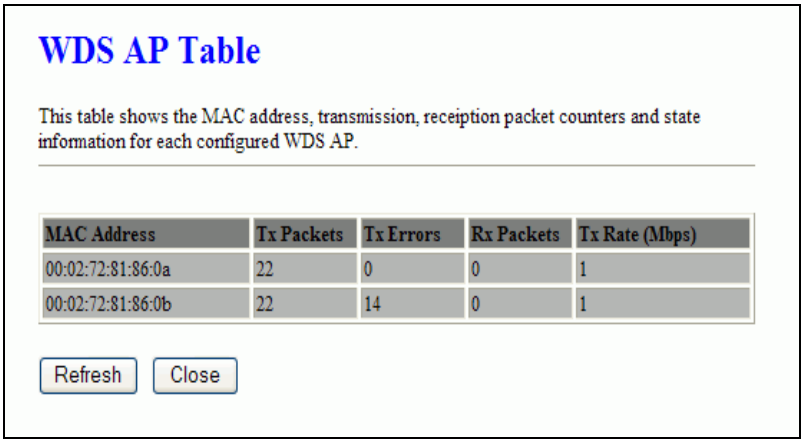


Таблица точек доступа WDS

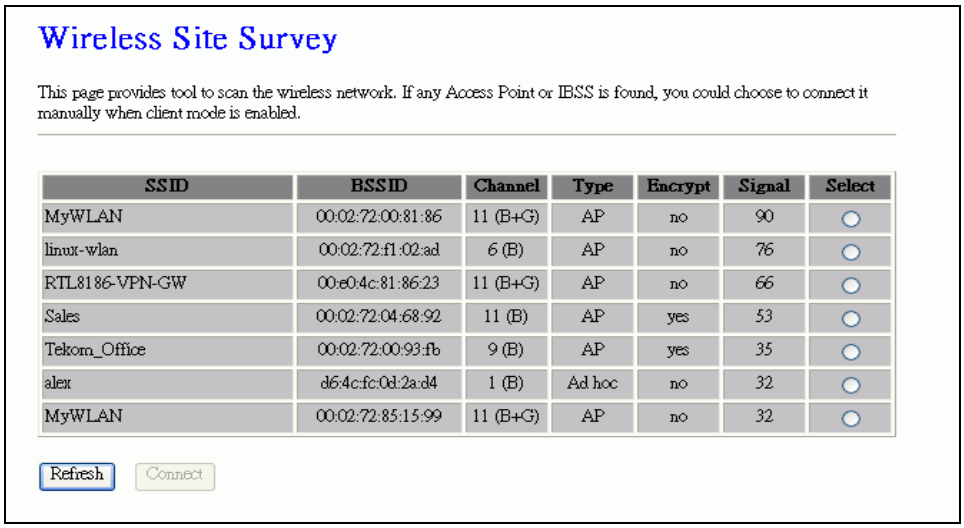
Эта страница используется для обзора статистики WDS:



Наименование	Описание
MAC Address	Показывает MAC адрес внутри WDS
Tx Packets	Показывает статистику отправленных пакетов на беспроводном LAN-интерфейсе
Tx Errors	Показывает статистику ошибок для отправленных пакетов на беспроводном LAN-интерфейсе
Rx Packets	Показывает статистику полученных пакетов на беспроводном LAN-интерфейсе
Tx Rare (Mbps)	Показывает скорость подключения по радиосвязи для WDS
Refresh	Кликните для обновления статистических показателей на экране
Close	Кликните для того, чтобы закрыть окно

3.3.9 Обзор доступных сетей (Site survey)

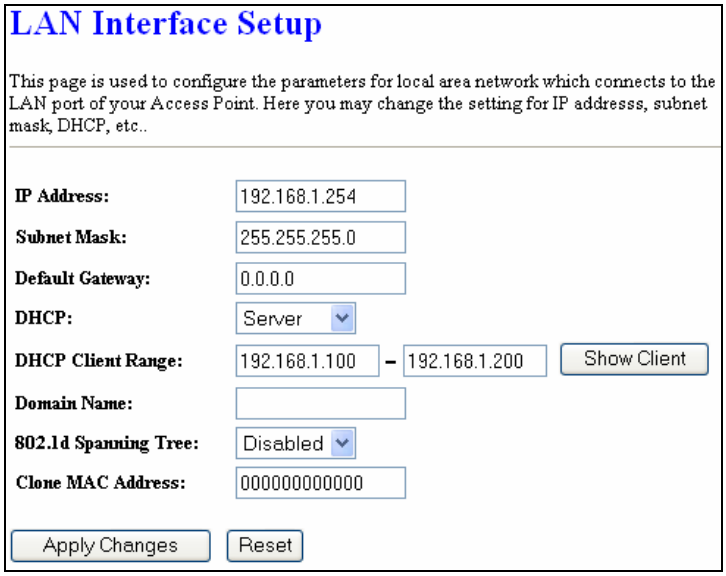
Страница используется для обзора других точек доступа, находящихся в зоне действия вашей беспроводной сети:



Наименование	Описание
SSID	Показывает SSID точки доступа
BSSID	Показывает BSSID точки доступа
Channel	Показывает канал, который использует точка доступа
Type	Показывает, в каком режиме работает точка доступа
Encrypt	Показывает статус шифрования
Signal	Показывает уровень сигнала при приеме
Select	Кликните для выбора точки доступа или клиента, к которому вы хотите подключиться
Refresh	Кликните ***Refresh*** для повторного обновления информации об узле на экране
Connect	Кликните ***Connect*** для установки соединения

3.3.10 Настройка LAN-интерфейса

Эта страница используется для настройки параметров локальной сети. Здесь вы можете изменить настройки IP адреса, маски подсети, DHCP и т.д.

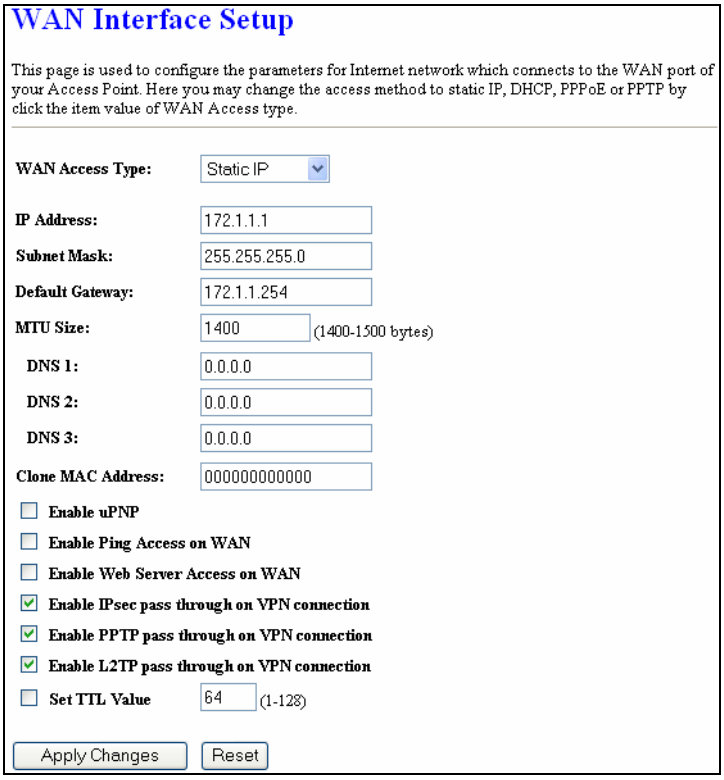


Наименование	Описание
IP address	Введите IP адрес LAN-интерфейсов
Subnet Mask	Введите маску подсети LAN-интерфейсов
Default Gateway	Введите шлюз по умолчанию для исходящих пакетов данных с LAN-интерфейсов
DHCP	Кликните для выбора ***Disabled***, ***Client*** или ***Server***
DHCP Client Range	Введите начальный и конечный IP адрес для обозначения диапазона IP адресов; клиенту, у которого включена функция DHCP, будет назначен IP адрес из этого диапазона
Show Client	Кликните, для того, чтобы открыть окно ***Active DHCP Client Table***, которое показывает активных клиентов с назначенными IP адресами, MAC адресами и информацией о времене работы (только для режима сервера)
DNS Server	Ручная настройка адреса DNS сервера
Domain Name	Назначение доменного имени DHCP клиентам. Эта функция - по выбору
802.1d Spanning Tree	Выберите для включения или выключения функции IEEE 802.1d Spanning Tree
Clone MAC Address	Введите MAC адрес, который должен быть клонирован. (см. параграф 4.24 - Что такое клонирование MAC адресов?)
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.11 Настройка WAN-интерфейса

На этой странице настраиваются параметры внешней сети, которая подключается к WAN-порту вашего широкополосного WLAN маршрутизатора. Здесь вы можете выбрать метод доступа: ***Static IP***, ***DHCP***, ***PPPoE*** или ***PPTP*** кликнув по полю напротив **WAN Access Type**.

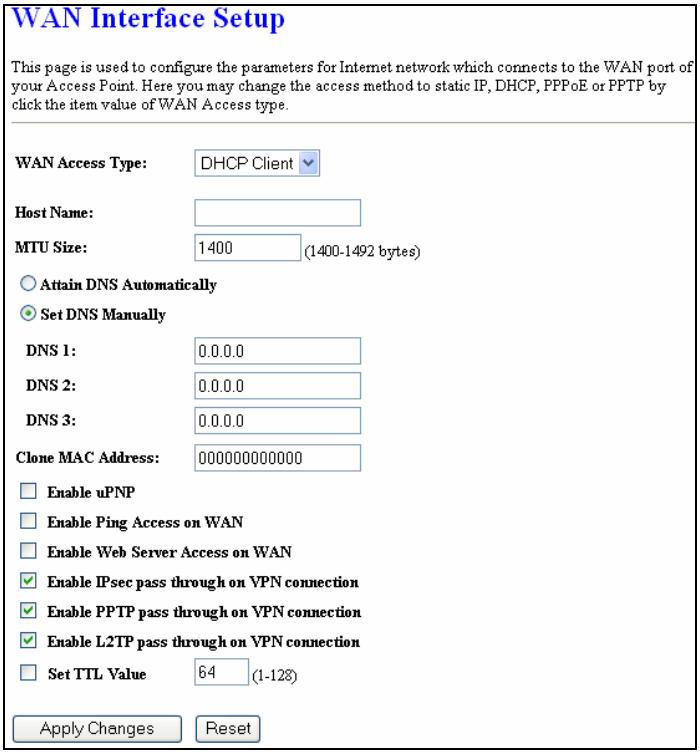
Статический IP адрес



Наименование	Описание
Static IP	Кликните для выбора поддержки Static IP на WAN-интерфейсе. Вы должны выбрать настройки IP адреса, маски подсети и шлюза по умолчанию
IP Address	Если вы выбираете поддержку статического IP адреса на WAN-интерфейсе, введите IP адрес для него
Subnet Mask	Если вы выбираете поддержку статического IP адреса на WAN-интерфейсе, введите маску подсети для него
Default Gateway	Если вы выбираете поддержку статического IP адреса на WAN-интерфейсе, введите шлюз по умолчанию для отправки исходящих пакетов
MTU Size	Введите размер MTU. Величина по умолчанию равна 1400
DNS 1	Введите IP адрес DNS сервера 1
DNS 2	Введите IP адрес DNS сервера 2
DNS 3	Введите IP адрес DNS сервера 3
Clone MAC Address	Введите MAC адрес, который должен быть клонирован
Enable uPNP	Кликните по полю для включения функции uPNP
Enable Web Server Access on WAN	Кликните по полю для включения веб-конфигурирования через WAN-интерфейс
Enable WAN Echo Reply	Кликните по полю для включения ответа WAN ICMP
Enable IPsec pass through on VPN connection	Кликните по полю для включения IPSec
Enable PPTP pass through on VPN connection	Кликните по полю для включения PPTP

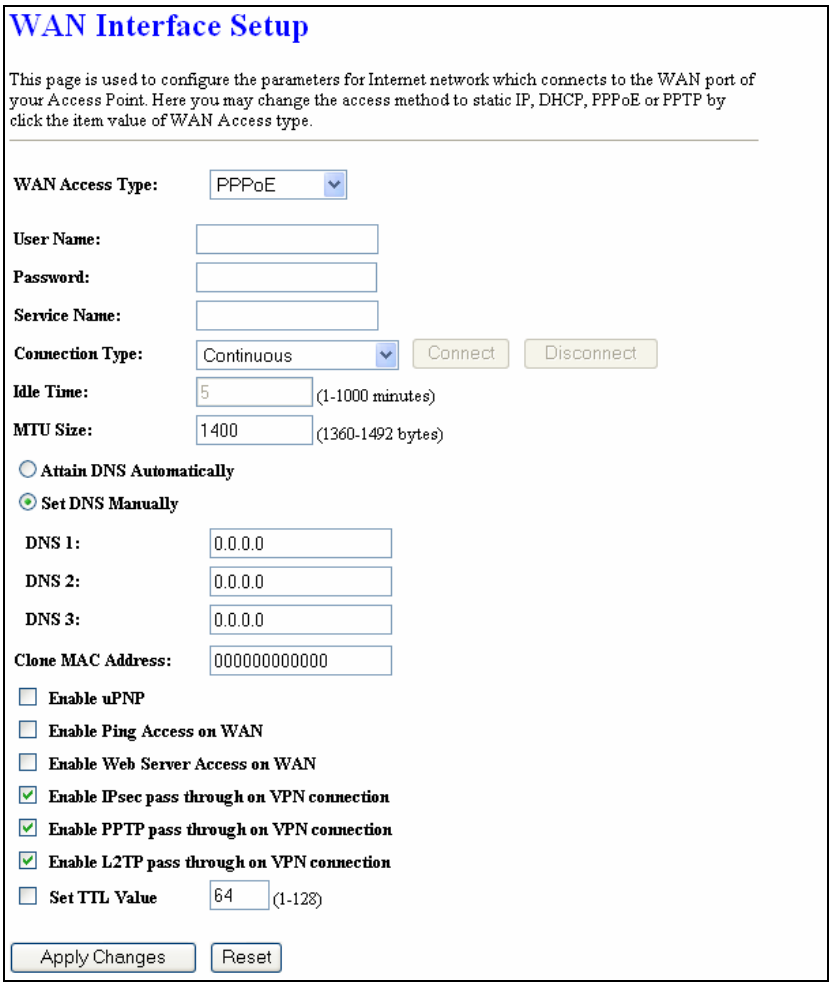
Enable L2TP pass through on VPN connection	Кликните по полю для включения L2TP
Set TTL value	Кликните для включения и введите значение Time to Live
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям.

DHCP клиент



Наименование	Описание
DHCP клиент	Кликните для выбора поддержки DHCP на WAN-интерфейсе, для того чтобы IP адреса назначались автоматически DHCP сервером
Host Name	Введите имя хоста. По умолчанию эта строка пуста
MTU Size	Введите размер MTU. Величина по умолчанию равна 1400
Attain DNS Automatically	Кликните для выбора получения DNS адреса по DHCP
Set DNS Manually	Кликните для выбора ручной настройки DNS, если включена поддержка DHCP
DNS 1	Введите IP адрес DNS сервера 1
DNS 2	Введите IP адрес DNS сервера 2
DNS 3	Введите IP адрес DNS сервера 3
Clone MAC Address	Введите MAC адрес, который должен быть клонирован
Enable uPNP	Кликните по полю для включения функции uPNP
Enable Web Server Access on WAN	Кликните по полю для включения веб-конфигурирования через WAN-интерфейс
Enable WAN Echo Reply	Кликните по полю для включения ответа WAN ICMP
Set TTL value	Кликните для включения и введите значение Time to Live
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

PPPoE



Наименование	Описание
PPPoE	Кликните для выбора PPPoE на WAN-интерфейсе. Здесь вы должны настроить имя пользователя, пароль, тип подключения и время ожидания
User Name	Если вы выбираете поддержку PPPoE на WAN-интерфейсе, введите имя пользователя для того, чтобы зайти на PPPoE сервер
Password	Если вы выбираете поддержку PPPoE на WAN-интерфейсе, введите пароль для того, чтобы зайти на PPPoE сервер
Service Name	Введите Service Name
Connection Type	Выберите тип подключения из нисходящего меню. Здесь вы можете выбрать ***Continuous***, ***Connect on Demand*** и ***Manual. Continuous*** означает, что настройка подключения осуществляется с помощью протокола PPPoE, когда бы ни был включен широкополосный WLAN маршрутизатор. ***Connect on Demand*** означает, что настройка подключения осуществляется с помощью протокола PPPoE, когда бы ни посылали пакеты данных через WAN-интерфейс; существует сторожевое устройство для закрытия PPPoE подключения в то время, когда пакеты не посылаются дольше, чем составляет настроенное время бездействия системы ***Manual*** означает, что настройка подключения осуществляется с помощью протокола PPPoE с помощью двойного клика по ***Connect*** и клика по ***Disconnect***
Idle Time	Если вы выбираете PPPoE и Connect on Demand тип подключения, введите время бездействия для автоматического отключения функции. Эта величина может варьироваться от 1 до 1000 минут
MTU Size	Введите размер MTU. Величина по умолчанию равна 1400. (см. параграф 4.23 - Что такое размер MTU?)
Attain DNS Automatically	Кликните для выбора получения DNS адреса по ***PPPoE***. Выберите ***Set DNS Manually*** если включена поддержка ***PPPoE***

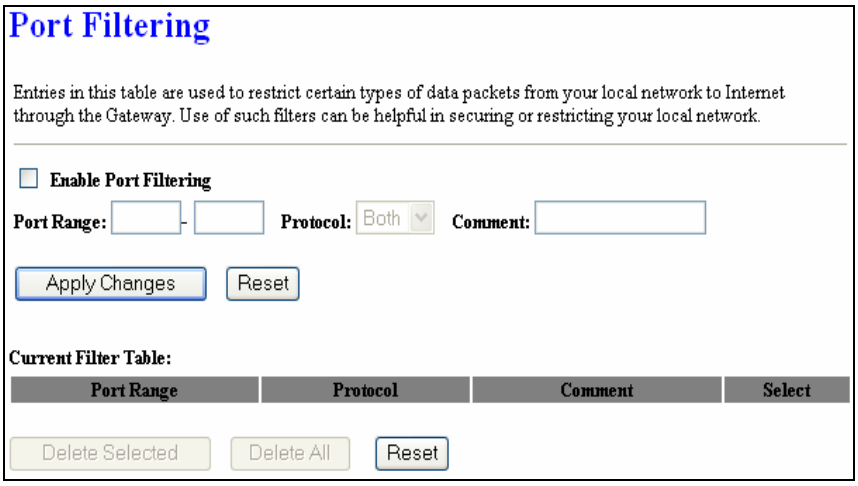
Set DNS Manually	Кликните для выбора ручной настройки DNS, если включена поддержка статического IP адреса
DNS 1	Введите IP адрес DNS сервера 1
DNS 2	Введите IP адрес DNS сервера 2
DNS 3	Введите IP адрес DNS сервера 3
Clone MAC Address	Введите MAC адрес, который должен быть клонирован
Enable uPNP	Кликните по полю для включения функции uPNP
Enable Web Server Access on WAN	Кликните по полю для включения веб-конфигурирования через WAN-интерфейс
Enable WAN Echo Reply	Кликните по полю для включения ответа WAN ICMP
Set TTL value	Кликните для включения и введите значение Time to Live
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

PPTP

Наименование	Описание
PPTP	Разрешение пользователям создать туннель с удалённым узлом напрямую для обеспечения безопасности при передаче данных между подключенными устройствами. Пользователь может использовать встроенного PPTP клиента, поддерживаемого маршрутизатором для создания VPN туннеля
IP Address	Если вы выбираете поддержку PPTP на WAN-интерфейсе, введите IP адрес для него
Subnet Mask	Если вы выбираете поддержку PPTP на WAN-интерфейсе, введите маску подсети для него
Server IP Address	Введите IP адрес PPTP сервера
User Name	Если вы выбираете поддержку PPTP на WAN-интерфейсе, введите имя пользователя для того, чтобы зайти на PPTP сервер
Password	Если вы выбираете поддержку PPTP на WAN-интерфейсе, введите пароль для того, чтобы зайти на PPTP сервер
MTU Size	Введите размер MTU. Величина по умолчанию равна 1400. (см. параграф 4.23 - Что такое размер MTU?)
Request MPPE Encryption	Кликните по полю для включения запроса MPPE-шифрования
Attain DNS Automatically	Кликните для выбора получения DNS адреса по ***PPTP***. Пожалуйста, выберите ***Set DNS Manually*** если включена поддержка ***PPTP***
Set DNS Manually	Кликните для выбора ручной настройки DNS, если включена поддержка статического IP адреса
DNS 1	Введите IP адрес DNS сервера 1
DNS 2	Введите IP адрес DNS сервера 2
DNS 3	Введите IP адрес DNS сервера 3
Clone MAC Address	Введите MAC адрес, который должен быть клонирован
Enable uPNP	Кликните по полю для включения функции uPNP
Enable Web Server Access on WAN	Кликните по полю для включения веб-конфигурирования через WAN-интерфейс
Enable WAN Echo Reply	Кликните по полю для включения ответа WAN ICMP
Set TTL value	Кликните для включения и введите значение Time to Live
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.12 Firewall – фильтрация на порту

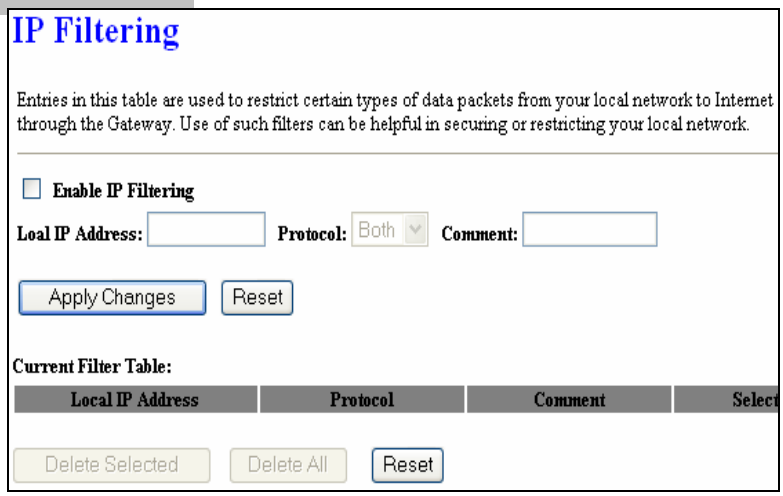
Записи в этой таблице используются для ограничения определенных типов пакетов данных в вашей локальной сети, которые могут попасть в Интернет через шлюз. Использование таких фильтров может быть полезным в обеспечении безопасности и ограничении вашей локальной сети.



Наименование	Описание
Enable Port Filtering	Включение функции фильтрации на порту для обеспечения безопасности
Port Range Protocol Comments	Для ограничения передачи данных из локальной сети на определенные порты, введите номер начального и конечного порта, протокола, а также введите комментарий
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для того, чтобы удалить выбранный диапазон портов из списка фильтрации
Delete All	Кликните для удаления всех зарегистрированных записей из списка фильтрации
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.13 Firewall – IP фильтрация

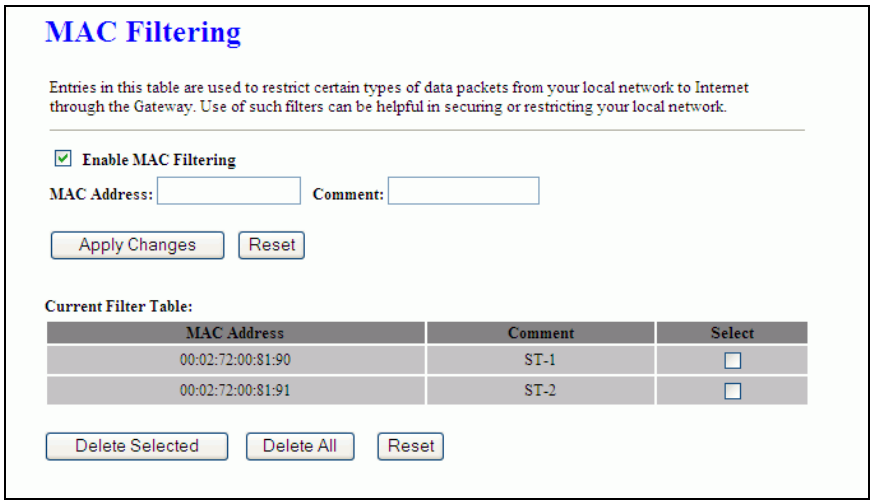
Записи в этой таблице используются для ограничения определенных типов пакетов данных в вашей локальной сети, которые могут попасть в Интернет через шлюз. Использование таких фильтров может быть полезным в обеспечении безопасности вашей локальной сети.



Наименование	Описание
Enable IP Filtering	Включение функции IP фильтрации для обеспечения безопасности
Local IP Address Protocol Comments	Для ограничения передачи данных из локальной сети на определенные IP адреса, введите IP адрес и протокол, а также введите комментарий. ***Protocol*** может быть TCP, UDP или оба. ***Comment*** даст вам знать причины ограничения передачи данных по IP адресу
Apply Changes	Кликните по этой кнопке для завершения и сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для того, чтобы удалить выбранный IP адрес из списка фильтрации
Delete All	Кликните для удаления всех зарегистрированных записей из списка фильтрации
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.14 Firewall – MAC фильтрация

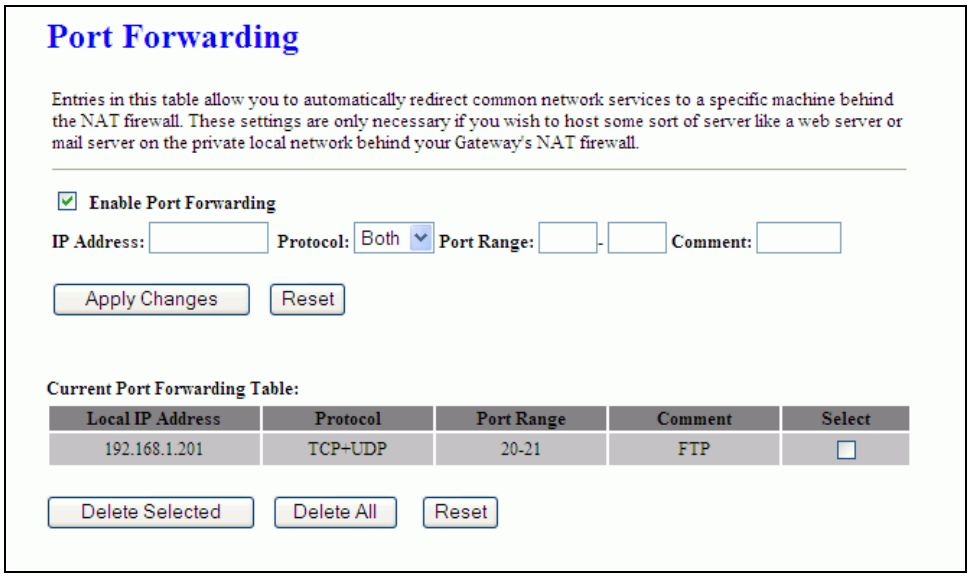
Записи в этой таблице используются для ограничения определенных типов пакетов данных в вашей локальной сети, которые могут попасть в Интернет через шлюз. Использование таких фильтров может быть полезным в обеспечении безопасности вашей локальной сети.



Наименование	Описание
Enable MAC Filtering	Включение функции MAC фильтрации для обеспечения безопасности
MAC Address Comments	Для ограничения передачи данных из локальной сети на определенные MAC адреса, введите MAC адрес, а также введите комментарий. ***Comment*** даст вам знать причины ограничения передачи данных по IP адресу
Apply Changes	Кликните по этой кнопке для регистрации MAC адреса в таблице фильтрации MAC адресов
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для того, чтобы удалить выбранный MAC адрес из списка фильтрации
Delete All	Кликните для удаления всех зарегистрированных записей из списка фильтрации
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.15 Firewall - переадресация портов

Записи в этой таблице позволяют вам автоматически переадресовывать общие сетевые сервисы на указанное устройство за NAT. Эти настройки необходимы, только если вы желаете разместить какие-то серверы, как например web-сервер или mail-сервер в частной локальной сети за NAT шлюза.

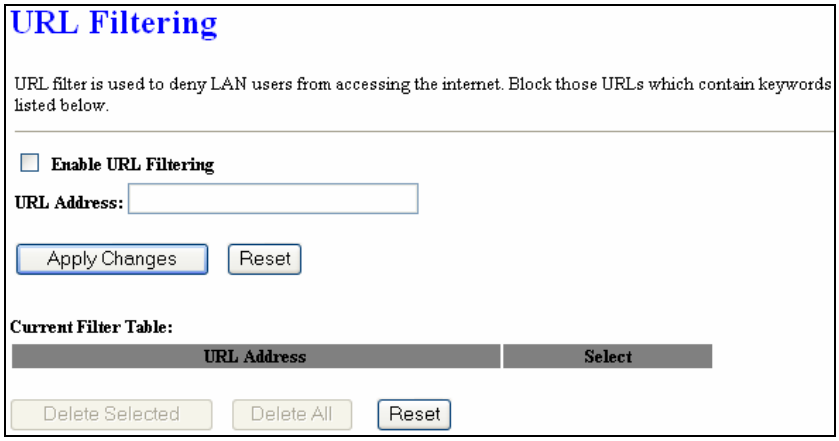


Наименование	Описание
Enable Port Forwarding	Включение функции безопасности Port Forwarding
IP Address Protocol Port Range Comment	Для переадресации пакетов, приходящих от WAN на указанный IP адрес, который расположен в локальной сети за NAT, введите IP адрес, протокол, диапазон портов и ваши комментарии. ***Protocol*** может быть TCP, UDP или оба. ***Port Range*** – диапазон портов для передачи данных. ***Comments*** дадут вам знать причины разрешения переадресации пакетов на указанный IP адрес и порт
Apply Changes	Кликните по этой кнопке для регистрации IP адреса в списке переадресации IP адресов
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для того, чтобы удалить выбранный IP адрес и порт из списка фильтрации
Delete All	Кликните для удаления всех зарегистрированных записей из списка

	переадресации портов
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.16 Firewall – URL фильтрация

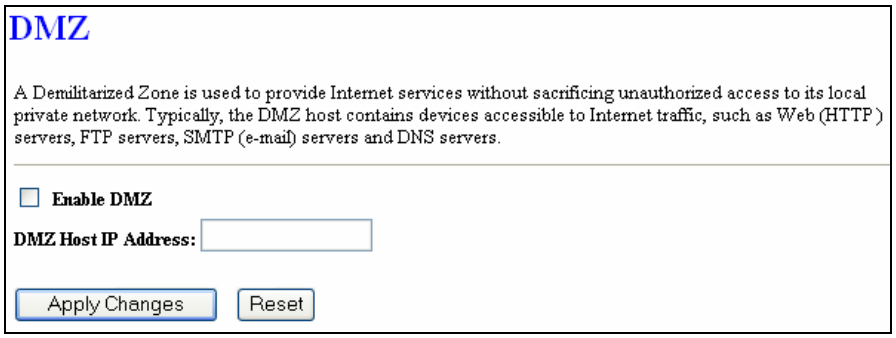
URL фильтрация используется для ограничения доступа пользователям к особым веб сайтам в Интернете.



Наименование	Описание
Enable URL Filtering	Включение функции фильтрации URL
URL Address	Добавьте один URL адрес
Apply Changes	Кликните по этой кнопке для сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для того, чтобы удалить выбранный URL адрес из списка фильтрации
Delete All	Кликните для удаления всех зарегистрированных записей из списка фильтрации
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.17 Firewall - DMZ

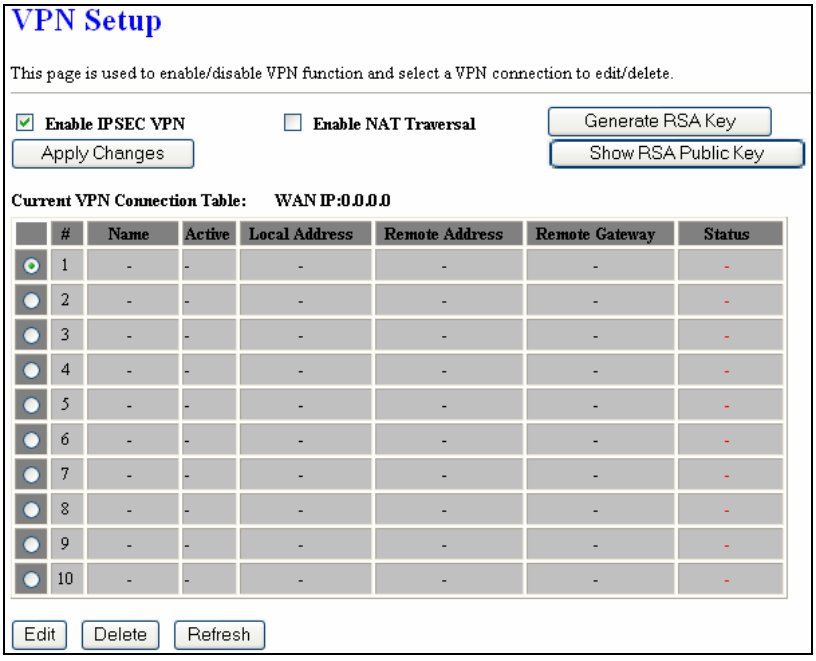
Демилитаризованная зона используется для обеспечения сервисов Интернет без риска доступа к частной локальной сети неавторизованных пользователей. Это часть компьютерной сети, находящаяся между локальной сетью и Интернетом. Обеспечивает выход в Интернет и внешнее присутствие в нём, скрывая при этом внутреннюю сеть организации и предотвращая прямое обращение к ней. Обычно, в DMZ находятся устройства, которые имеют доступ к трафику Интернет, в частности к Web (HTTP) серверам, FTP серверам, SMTP (e-mail) серверам и DNS серверам.



Наименование	Описание
Enable DMZ	Включение функции DMZ
DMZ Host IP Address	Для поддержки DMZ в вашей схеме брандмауэра, введите IP адрес хоста DMZ, на который можно зайти через WAN-интерфейс
Apply Changes	Кликните по этой кнопке для регистрации IP адреса хоста DMZ
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.18 Настройки VPN

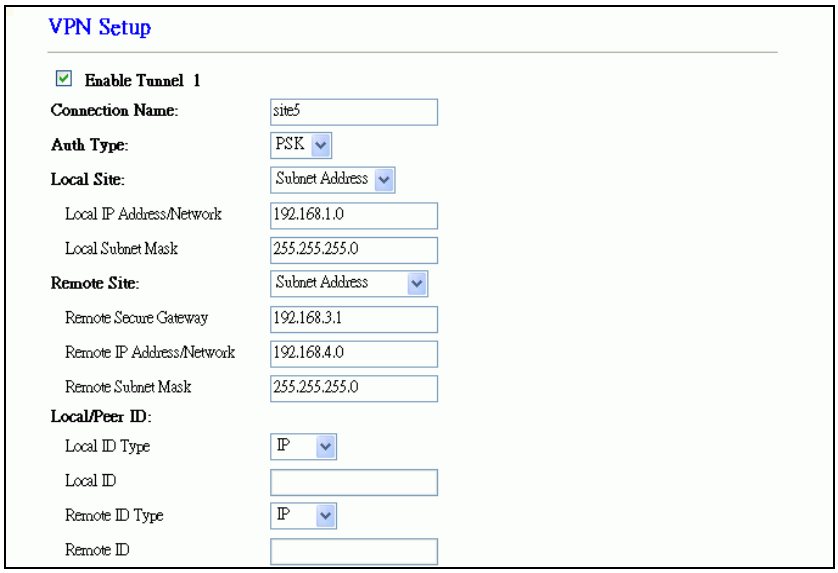
Эта страница используется для того, чтобы показать таблицу подключений VPN, настроить IPsec VPN, NAT Traversal, Generate RSA Key, Show RSA Public Key.



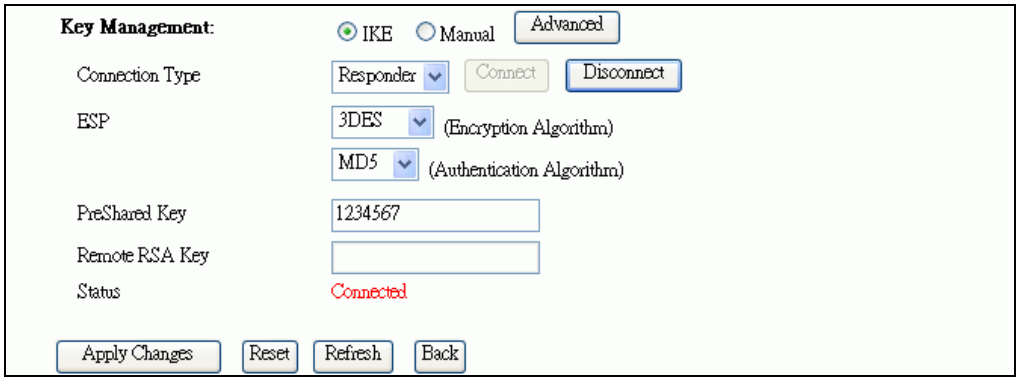
Наименование	Описание
Enable IPSEC VPN	Включение функции IPSEC VPN. (см.параграф 4.27 Что такое VPN? и 4.28 Что такое IPSEC?)
Enable NAT Traversal	Кликните для включения функции NAT Traversal
Generate RSA Key	Кликните для генерации RSA ключа
Show RSA Public Key	Кликните для просмотра публичного RSA ключа, который сгенерировали
Apply Changes	Кликните по этой кнопке для включения IPSEC VPN, NAT Traversal
Current VPN Connection Table	Показывает информацию о конкретном WAN-интерфейсе и таблице подключений по VPN
Edit	Кликните для того, чтобы зайти на страницу конфигурирования VPN туннеля

Delete	Кликните для удаления настоящего VPN туннеля
Refresh	Кликните для обновления таблицы VPN

Настройки VPN – изменение туннеля

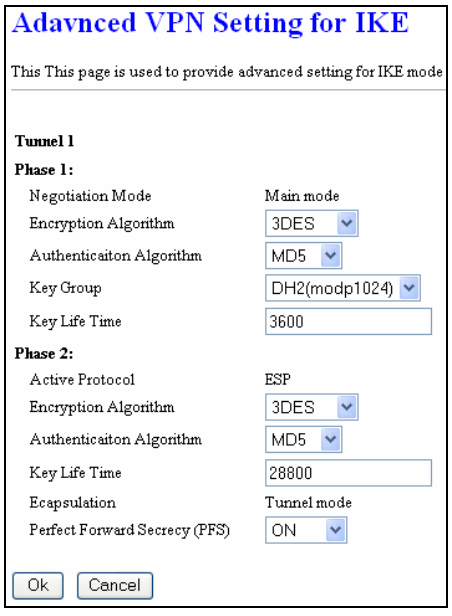


Наименование	Описание
Enable Tunnel #	Кликните для включения туннеля IPSEC VPN
Connection Name	Назначьте имя для подключения
Auth Type	Кликните для выбора ***PSK*** или ***RSA***
Local Site ***Local IP Address/Network*** ***Local Subnet Mask***	Кликните для выбора ***Single Address*** или ***Subnet Address*** VPN подключения. Введите IP адрес или маску подсети в зависимости от того, какую опцию локального сайта вы выбираете
Remote Site ***Remote Secure Gateway*** ***Remote IP Address/Network*** ***Remote Subnet Mask***	Кликните для выбора ***Single Address, Subnet Address***, ***Any Address*** или ***NAT-T Any Address*** удалённого VPN подключения. Введите IP адрес удаленного шлюза. Введите IP адрес или маску подсети в зависимости от того, какую опцию локального сайта вы выбираете. Введите удаленную маску подсети
Local/Peer ID ***Local ID Type*** ***Local ID***	Определите IKE тип обмена информации. Кликните для выбора ***IP***, ***DNS*** или ***E-mail*** как типа локального коммутатора (обмена). Введите локальные IP за исключением выбранных IP
Remote ID Type	Кликните для выбора ***P***, ***DNS*** или ***E-mail*** как типа локального коммутатора (обмена)
Remote ID	Введите удалённые ID за исключением выбранных IP



Наименование	Описание
Key Management	Кликните для выбора ***IKE*** или режима ***Manual***
Advanced	Кликните по кнопке ***Advanced*** для настройки дополнительных возможностей IKE
Connection Type	Кликните для выбора режима ***Initiator*** или ***Responder***
Connect	Кликните для ручного подключения (только для режима ***Responder***)
Disconnect	Кликните для ручного отключения (только для режима ***Responder***)
ESP	Кликните для настройки шифрования ***3DES***, ***AES128*** или ***NULL.*** Кликните для настройки аутентификации ***MD5*** или ***SHA1***
PreShared Key	Введите ключ (только для режима IKE)
Remote RSA Key	Введите RSA ключ удаленного шлюза (только для режима IKE)
Status	Показывает статус подключения (только для режима IKE)
SPI	Введите значение параметра Security Parameter Index (Только для режима Manual)
Encryption Key	Введите ключ шифрования (только для режима Manual)
Authentication Key	Введите ключ аутентификации (только для режима Manual)
Apply Change	Кликните по этой кнопке для сохранения настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям
Refresh	Показывает настоящий статус подключения (только для режима Manual)
Back	Возврат к странице настроек VPN

Настройка специального протокола IKE

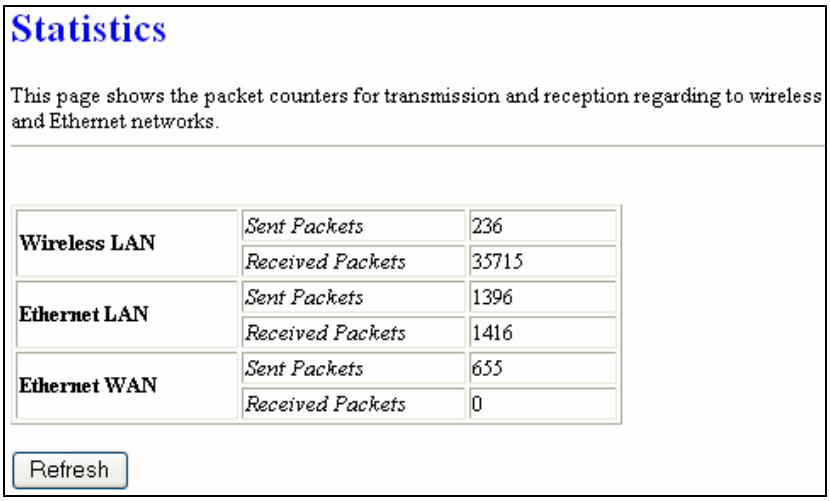


Наименование	Описание
Phase 1	
Negotiation Mode	Основной режим
Encryption Algorithm	Кликните для выбора шифрования ***3DES*** или ***AES128***
Authentication Algorithm	Кликните для выбора аутентификации ***MD5*** или ***SHA1***
Key Group	Кликните для выбора группы ключей ***DH1(modp768)***, ***DH2(modp1024)*** или ***DH5(modp1536)***
Key Life Time	Введите значение времени действия ключа в секундах
Phase 2	
Active Protocol	ESP
Encryption Algorithm	Кликните для выбора типа шифрования ***3DES***, ***AES128*** или ***NULL***
Authentication Algorithm	Кликните для выбора аутентификации ***MD5*** или ***SHA1***
Key Life Time	Введите значение времени действия ключа в секундах

Encapsulation	Режим туннеля
Perfect Forward Secrecy (PFS)	Кликните для выбора ***ON*** или ***NONE***
Ok	Кликните по кнопке ***Ok*** для сохранения текущих настроек туннеля
Cancel	Кликните ***Cancel*** для того, чтобы закрыть окно без сохранения изменений настроек

3.3.19 Управления - статистика

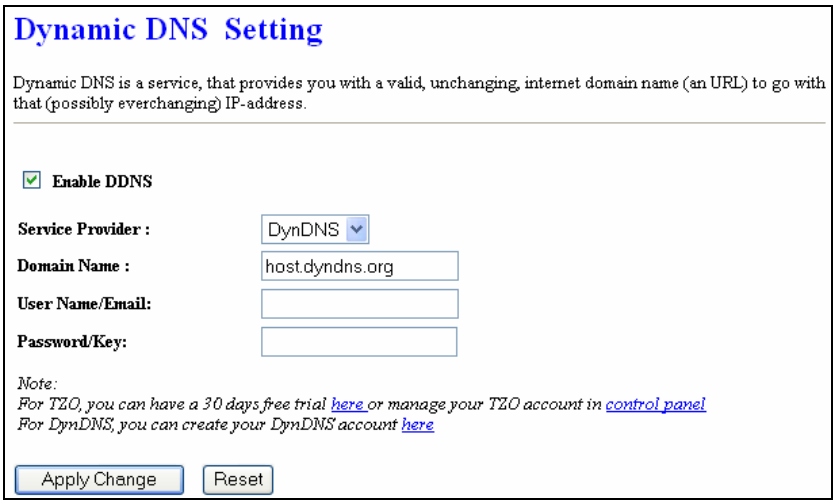
На этой странице показаны счётчики пакетов при передаче и приёме для беспроводной сети, сетей Ethernet LAN и Ethernet WAN.



Наименование	Описание
Wireless LAN ***Sent Packets***	Показывает статистику по отправленным пакетам на беспроводном LAN-интерфейсе
Wireless LAN ***Received Packets***	Показывает статистику по полученным пакетам на беспроводном LAN-интерфейсе
Ethernet LAN ***Sent Packets***	Показывает статистику по отправленным пакетам на Ethernet LAN-интерфейсе
Ethernet LAN ***Received Packets***	Показывает статистику по полученным пакетам на Ethernet LAN-интерфейсе
Ethernet WAN ***Sent Packets***	Показывает статистику по отправленным пакетам на Ethernet WAN-интерфейсе
Ethernet WAN ***Received Packets***	Показывает статистику по полученным пакетам на Ethernet WAN-интерфейсе
Refresh	Кликните ***Refresh*** для обновления статистических счётчиков на экране

3.3.20 Управление - DDNS

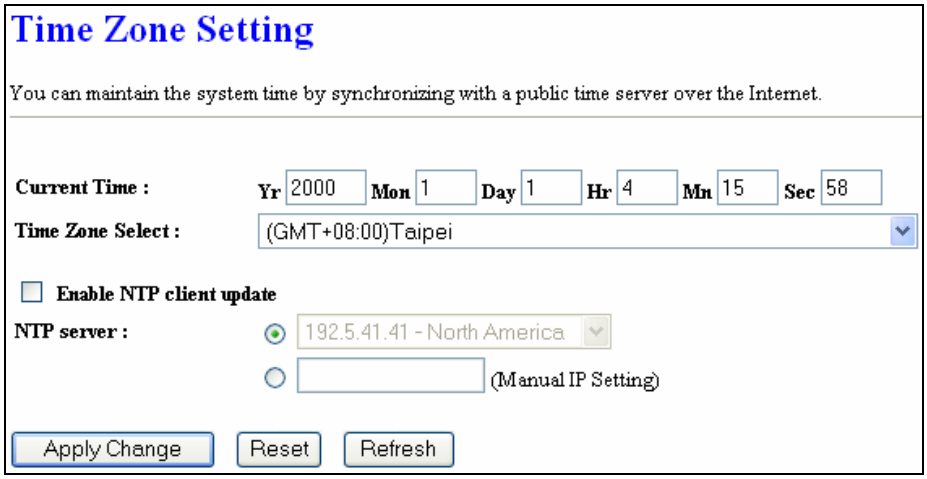
Эта страница используется для настройки динамического DNS сервиса таким образом, чтобы получить DNS с динамическим IP адресом.



Наименование	Описание
Enable DDNS	Включение DDNS сервиса. (см. параграф 4.25 - Что такое DDNS?)
Domain Name	Настройка доменного имени
User Name/Email	Настройка имени пользователя, e-mail
Password/Key	Настройка пароля/ключа
Apply Change	Кликните ***Apply Change*** для сохранения включения DDNS сервиса
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.21 Управление – настройка часового пояса

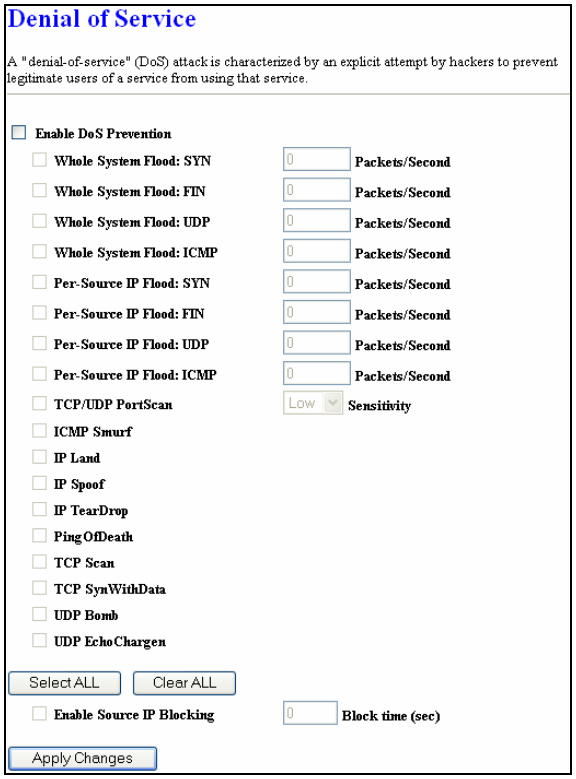
Эта страница используется для настройки NTP клиента для получения настоящего времени.



Наименование	Описание
Current Time	Показывает текущее время
Time Zone Select	Кликните для выбора часового пояса вашей страны
Enable NTP client update	Кликните по полю для включения обновления NTP клиента. Обратитесь к параграфу 4.26 Что такое NTP клиент?
NTP Server	Кликните для выбора адреса NTP сервера – по умолчанию или того IP адреса, который вы введёте
Apply Change	Кликните ***Apply Change*** для сохранения включения сервиса NTP клиента
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям
Refresh	Кликните для обновления текущего времени, обновляемого на экране

3.3.22 Управление – отказ от обслуживания

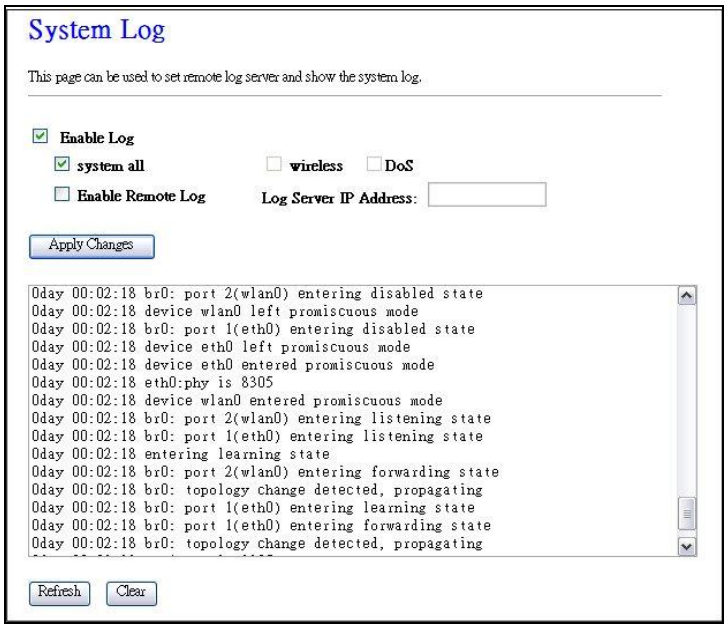
Эта страница используется для включения и настройки защиты от возможных хакерских атак. Обеспечивает большую безопасность для пользователей.



Наименование	Описание
Enable DoS Prevention	Кликните по полю для включения защиты DoS
Whole System Flood / Per-Source IP Flood…	Включите и настройте защиту детализировано
Select ALL	Кликните по полю для включения всех функций защиты
Clear ALL	Кликните по полю для выключения всех функций защиты
Apply Changes	Кликните ***Apply Changes*** для сохранения настроек

3.3.23 Управление – журнал регистрации

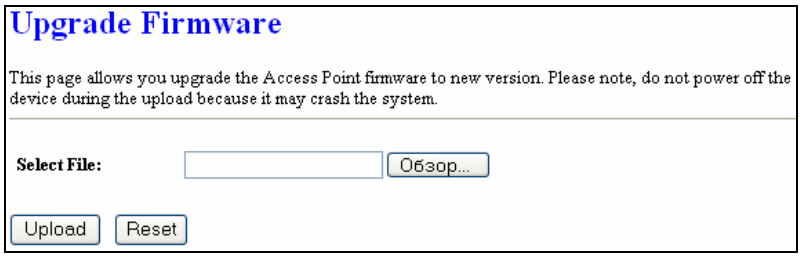
Эта страница используется для настройки удаленного сервера журнала регистрации и просмотра текущих записей в журнале.



Наименование	Описание
Enable Log ***System all*** ***Wirelessy*** ***DoS***	Кликните по полю для включения журнала регистрации. Просмотр всех записей беспроводного широкополосного маршрутизатора. Просмотр записей только о радиосвязи. Просмотр записей только о Denial-of-Service
Enable Remote Log ***Log Server IP Address***	Кликните по полю для включения сервиса удалённого журнала регистрации. Введите IP адрес удалённого журнала регистрации
Apply Changes	Кликните ***Apply Changes*** для сохранения настроек
Refresh	Кликните ***Refresh*** для обновления журнала регистрации на экране
Clear	Очистка журнала регистрации на экране

3.3.24 Управление – обновление прошивки

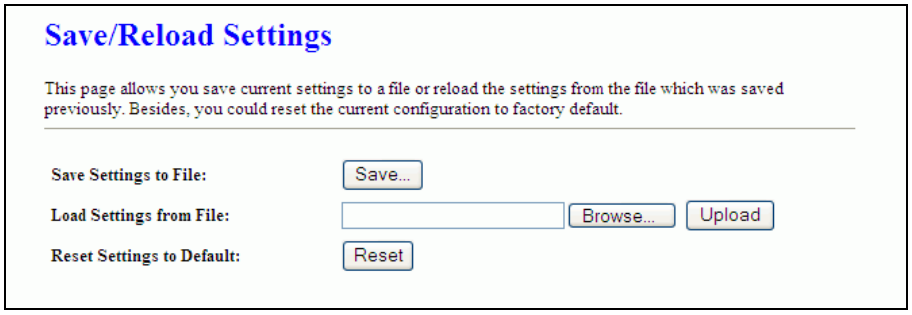
Эта страница позволяет вам обновлять прошивку точки доступа до последней версии. Пожалуйста, обратите внимание на то, что не следует отключать питание устройства во время загрузки обновления, поскольку это может повредить систему.



Наименование	Описание
Select File	Кликните по кнопке ***Browse*** для выбора файла новой версии прошивки
Upload	Кликните по кнопке ***Upload*** для того, чтобы залить выбранный файл на маршрутизатор
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.25 Управление – сохранение/перезагрузка настроек

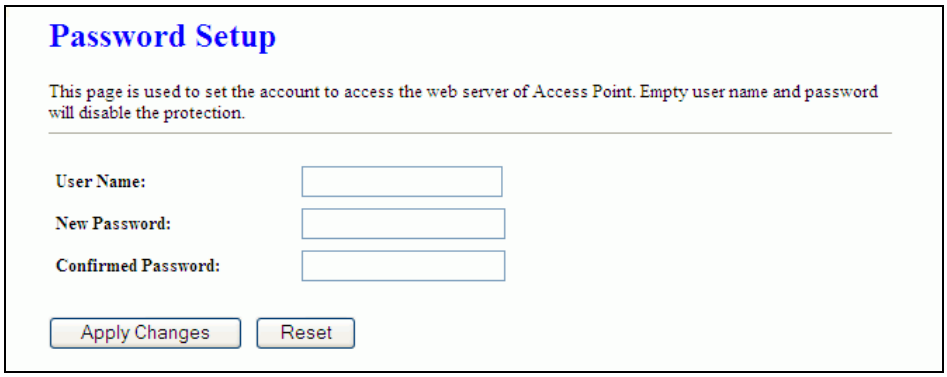
На этой странице вы можете сохранить текущие настройки в виде файла или загрузить файл, который вы сохранили прежде. Кроме того, вы можете вернуть заводские настройки системы.



Наименование	Описание
Save Settings to File	Кликните по кнопке ***Save,*** чтобы сохранить параметры конфигурации на ваш компьютер
Load Settings from File	Кликните по кнопке ***Browse*** для того, чтобы выбрать файл конфигурации, а затем кликните по кнопке ***Upload***, чтобы загрузитьить выбранный файл на широкополосный WLAN маршрутизатор
Reset Settings to Default	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к заводским настройкам

3.3.26 Управление – настройка пароля

Эта страница используется для настройки учётной записи для доступа к веб-серверу точки доступа. Пустые поля для имени пользователя и пароля отключают защиту.

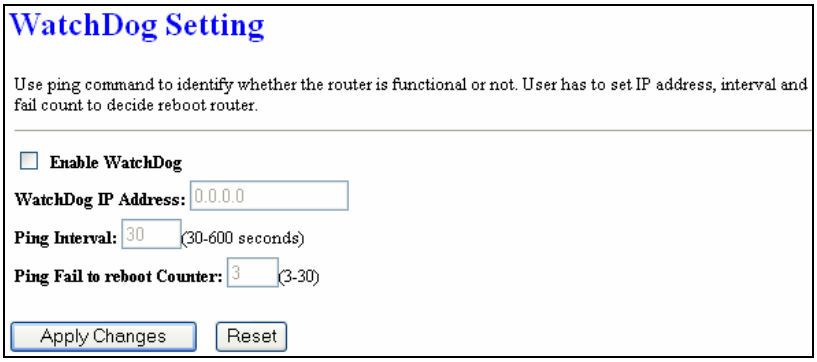


Моментальный снимок экрана – управление – настройка пароля.

Наименование	Описание
User Name	Введите имя пользователя для контроля логина с помощью веб управления
New Password	Введите пароль для контроля логина с помощью веб управления
Confirmed Password	Т.к. пароль, который вы вводите, невидим, введите его повторно для подтверждения
Apply Changes	Если поля для имени пользователя и пароля останутся пустыми, это будет означать, что контроль логина с помощью веб-управления отключен
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.27 Управление – WatchDog (сторожевое устройство)

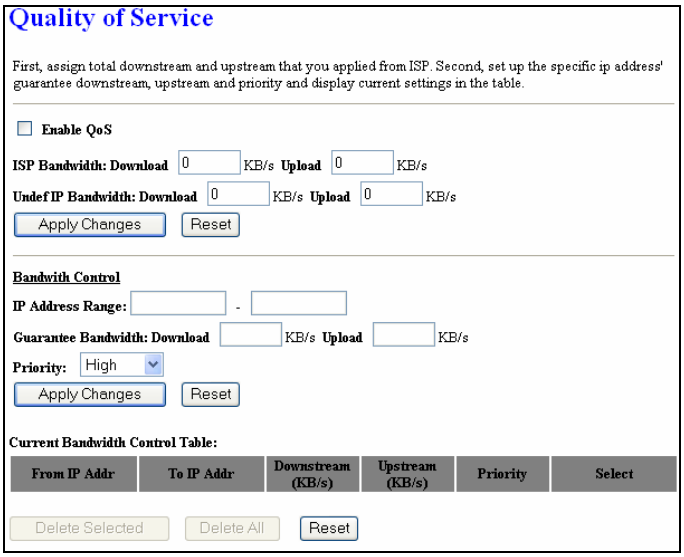
Эта страница используется для выполнения функции watchdog с помощью команды ping. Пользователь устанавливает IP адрес, интервал и другие условия для команды Ping, чтобы понять перезагружается маршрутизатор или нет.



Наименование	Описание
Enable WatchDog	Кликните для включения функции watchdog
WatchDog IP Address	IP адрес, к которому обращается устройство
Ping Interval	Введите значение в секундах
Ping Fail to reboot Count	Введите пороговое значение для перезагрузки маршрутизатора, когда пропадают пинги
Apply Changes	Кликните по кнопке ***Apply Changes*** для завершения новых настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

3.3.28 Управление – Quality of Service (качество сервиса)

Эта страница используется для управления шириной полосы по IP адресу. Пользователь устанавливает общую и неопределенную полосу в первую очередь. Затем регулирует полосу заданием диапазона IP адресов.



Наименование	Описание
Enable QoS	Кликните для включения QoS
ISP Bandwidth	
Download	Введите значения для скорости скачивания в КБ/сек
Upload	Введите значения для скорости закачивания в КБ/сек
Undef IP Bandwidth	

Download	Определите полосу для скачивания, которая ещё не определена
Upload	Определите полосу для закачивания, которая ещё не определена
Apply Changes	Кликните по кнопке ***Apply Changes*** для завершения новых настроек
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

Наименование	Описание
Bandwidth Control	
IP Address Range	Введите начальный и конечный IP адрес
Guarantee Bandwidth	
Download	Введите значения для скорости скачивания в КБ/сек
Upload	Введите значения для скорости закачивания в КБ/сек
Piority	Выберите приоритет: **High (**высокий**)**, **Medium(**средний**)** или **Low (**низкий**)**
Apply Changes	Кликните по кнопке ***Apply Changes*** для завершения новых настроек. Они добавлены в **Current Bandwidth Control Table**
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям
Delete Selected	Кликните для удаления выбранных IP адресов из **Current Bandwidth Control Table**
Delete All	Кликните для удаления всех зарегистрированных записей из **Current Bandwidth Control Table**
Reset	Кликните по кнопке ***Reset*** для прекращения изменений и возврата к предыдущим конфигурациям

4 Часто задаваемые вопросы (FAQ)

4.1 Где и как найти IP и MAC адрес моего компьютера?

IP адрес - это идентификатор компьютера или устройства в сети TCP/IP. Сети, использующие протокол TCP/IP, маршрутизируют сообщения, руководствуясь IP адресом назначения. Формат IP адреса представляет собой 32-битный числовой адрес, записанный в виде 4 чисел, разделенных точками. Каждое число может быть от 0 до 255. Например, 191.168.1.254 может быть IP адресом.

MAC адрес (Media Access Control) это уникальный аппаратный номер вашего компьютера. (В сети Ethernet LAN это тот же самый адрес, что и ваш Ethernet адрес). Когда ваш компьютер (или хост, как его определяет Интернет-протокол) подключен к Интернету, ваш физический MAC и IP адреса LAN-интерфейса сравниваются в таблице соответствий.

Для того чтобы найти ваш IP и MAC адрес:

- ✓ Откройте программу Command в Microsoft Windows.
- ✓ Впечатайте ***ipconfig/all*** и нажмите Enter
- ✓ IP адрес вашего компьютера так и будет назван, а MAC адрес определяется как физический адрес

4.2 Что такое Wireless LAN?

Wireless LAN (WLAN) – это сеть, которая обеспечивает доступ в Интернет без проводных соединений к пользовательским машинам.

4.3 Что такое ISM полосы?

(Industrial, Scientific and Medical band) - диапазон ISM

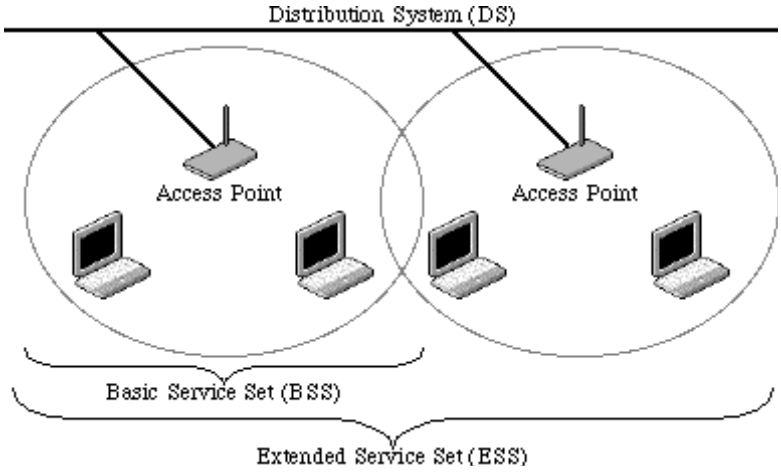
Различные диапазоны радиочастотного спектра, выделяемые на основе международных соглашений для некоммерческого использования в перечисленных выше областях, например 902 - 928 МГц. В 2001 г. частоты с 2,4 по 2,4835 ГГц (UHF) были выделены для беспроводных сетей (WLAN) и других беспроводных технологий.

4.4 Как работает беспроводная сеть?

Стандарт 802.11 определяет два режима: режим инфраструктуры и специальный режим. В первом режиме беспроводная сеть состоит, по крайней мере, из одной точки доступа, подключенной к инфраструктуре проводной сети и комплекта беспроводных станций.

Эта конфигурация называется Basic Service Set (BSS).

Extended Service Set (ESS) – это комплект из двух или больше BSS, формирующих одну подсеть. С тех пор как корпоративные сети WLAN предоставляют доступ к проводным сервисам LAN (файловые сервисы, принтеры, Интернет ссылки), они работают в режиме инфраструктуры.



Пример 1. Режим беспроводной инфраструктуры

4.5 Что такое BSSID?

6-байтовый адрес, который разделяет определенную точку доступа от других. Также известен как просто SSID. Выступает в роли идентификаторы сети или имени.

4.6 Что такое ESSID?

Extended Service Set ID (ESSID) – это имя сети, к которой вы хотите получить доступ. Оно используется для идентификации разных беспроводных сетей.

4.7 Каковы причины возникновения помех?

Факторы, вызывающие помехи:

- Преграды: стены, потолки, мебель и т.д.
- Строительные материалы: металлические двери, алюминиевые брусья.
- Электрические устройства: микроволновые печи, мониторы и электрические моторы.

Решения, позволяющие преодолеть помехи:

- Минимизация количества стен и потолков.
- Расположение WLAN антенны для лучшего приёма.
- Держите устройства WLAN вдали от других электрических приборов. В том числе от: микроволновых печей, мониторов, электрических моторов и т.д.
- Добавьте дополнительные WLAN точки доступа, если требуется.

4.8 Что такое Open System и аутентификации Shared Key?

Стандарт IEEE 802.11 поддерживает два подтипа сервисов аутентификации в сетях: open system и shared key. При работе аутентификации open system любая беспроводная станция запрашивает аутентификацию. Станция, которая запрашивает аутентификацию от другой беспроводной станции, посылает аутентификационный управляемый фрейм, который содержит идентификатор станции. Принимающая станция затем возвращает фрейм, который сигнализирует о том, распознаёт ли он посылающую станцию. При использовании shared key аутентификации предполагается, что каждая беспроводная станция получила секретный ключ shared key по безопасному каналу, который независим от канала связи беспроводной сети стандарта 802.11.

4.9 Что такое WEP?

Опциональная функция IEEE 802.11 предлагает приватность при передаче фреймов аналогичную той, которая существует в проводных сетях. Wired Equivalent Privacy (WEP) формирует секретные ключи (shared keys) шифрования таким образом, что обе станции – источника и назначения – могут использовать для сигнализации фреймы с битами для того, чтобы избежать распознавания устройствами слежения.

WEP полагается на секретный ключ, который рассекречен для мобильной станции (например, лэптопа с беспроводной Ethernet картой) и точки доступа

(например, базовой станции). Секретный ключ используется для шифрования пакетов перед их передачей, и проверка однозначности (интерпретации данных) используется для того, чтобы убедиться в неизменности пакетов при передаче.

4.10 Что такое Fragment Threshold?

Предложенный протокол использует механизм фрагментации фреймов, определенный стандартом IEEE 802.11 для достижения параллельных передач. Большой фрейм данных фрагментируется на несколько блоков, каждый из которых по размеру равен порогу фрагмента (Fragment Threshold). Настраивая значение порога фрагмента, мы можем использовать переменные размеры фрагментов. Определение эффективного порога фрагмента важная задача в этой процедуре. Если порог фрагмента мал, перекрывающая часть основной и параллельной передачи велика. Это означает, что доля пространственного использования параллельной передачи велика. И, наоборот, при большом пороге фрагмента, перекрывающая часть мала и доля пространственного использования мала. Большой порог фрагмента приводит к малым потерям фрагмента.

Порог фрагмента – это максимальный размер пакета, используемый для фрагментации. Пакеты больше запрограммированного размера в соответствующем поле будут фрагментированы.

Если вы обнаружили поврежденные пакеты или ассиметричный приём пакетов, вы можете уменьшить порог фрагмента. Это разобьёт пакеты на более мелкие фрагменты. Эти маленькие фрагменты, если они повреждены, могут быть посланы повторно быстрее, чем большие. Фрагментация увеличивает накладные расходы на передачу, поэтому, выгодно задавать соответствующее значение как можно более близким к максимально возможному.

4.11 Что такое порог RTS (Request To Send)?

Порог RTS – это размер пакета, который допустим для передачи при операции связи RTS/CTS. Стандарт IEEE 802.11-1997 позволяет коротким пакетам передаваться без операции связи RTS/CTS. Каждая станция может иметь разный порог RTS. RTS/CTS используется, когда размер пакетов данных превышает определенный порог RTS. Используя механизм передачи CSMA/CA, передающая станция посылает RTS пакет принимающей станции и ждёт, когда принимающая станция пришлёт обратно пакет CTS (Clear to Send) перед посылкой актуальных пакетов данных.

Эти настройки полезны для сетей с большим количеством клиентов.

С большим количеством клиентов и высокой загрузкой сети будет гораздо больше коллизий. Уменьшая порог RTS, можно уменьшить количество коллизий, и производительность должна возрасти. Пакеты RTS используют полноценную полосу, таким образом, уменьшение полосы может привести к ухудшению производительности.

4.12 Что такое Beacon Interval?

Пакет, переданный точкой доступа для синхронизации в сети.

4.13 Что такое тип преамбулы?

Существует два типа преамбул, определенных в спецификации стандарта IEEE 802.11. Длинная преамбула обычно даёт декодеру больше времени на её обработку. Все устройства 802.11 поддерживают длинную преамбулу. Короткая преамбула разработана для повышения эффективности (например, систем VoIP). Различие между этими двумя типами преамбул находится в поле синхронизации. Длинная преамбула состоит из 128 битов, а короткая - из 56 битов.

4.14 Что такое широковещательная передача SSID?

Широковещательная передача SSID организована в точках доступа с применением радиомаяков. Это позволяет анонсировать вашу точку доступа (включая различные биты информации о ней) для беспроводных устройств в сети. При отключении этой опции, SSID, настроенный у клиента должен согласовываться с SSID точки доступа.

Некоторые беспроводные устройства не могут нормально работать, если SSID не передаётся по широковещательной передаче (например, адаптер D-link DWL-120 USB 802.11b). Как правило, если аппаратура вашего клиента поддерживает работу с отключенным SSID, то это может быть полезно с точки зрения повышения безопасности сети. Однако это не заменит WEP, MAC фильтрацию и другие средства защиты.

4.15 Что такое Wi-Fi Protected Access (WPA)?

Оригинальный механизм безопасности Wi-Fi, Wired Equivalent Privacy (WEP), считается недостаточным для осуществления безопасных бизнес коммуникаций. **Wi-Fi Protected Access** (**WPA** и **WPA2**) — протокол безопасности, применяемый для обеспечения безопасности в беспроводных Wi-Fi сетях.

Он был создан в качестве замены для **Wired Equivalent Privacy** (WEP), который более уязвим. WPA реализует большую часть стандарта IEEE 802.11i и предназначен для замены WEP пока 802.11i не будет готов.

Для обновления WLAN сети таким образом, чтобы она поддерживала WPA, точка доступа затребует программное обеспечение WPA. Клиенты затребуют

обновления программного обеспечения для сетевых карт, и, возможно, обновления операционной системы. Для сетей больших компаний сервер аутентификации (обычно тот, который поддерживает RADIUS и выбранный протокол аутентификации EAP) будет добавлен в сеть.

4.16 Что такое WPA2?

Это второе поколение WPA. WPA2 базируется на поправке IEEE 802.11i к стандарту 802.11. WPA2 реализует полный стандарт, но он не будет работать на некоторых старых сетевых картах.

4.17 Что такое аутентификация 802.1x?

802.1x – это основа для контроля доступа, аутентификации, по MAC адресу, которая определяет Extensible Authentication Protocol (EAP) по сетям LAN (WAPOL). Стандарт инкапсулирует и использует многое из протокола EAP, который был определен для dial-up аутентификации с протоколом точка-точка (Point-to-Point) в RFC 2284. Кроме инкапсуляции пакетов EAP стандарт 802.1x также определяет сообщения EAPOL, которые передают информацию о ключах шифрования (shared key), необходимую для безопасности беспроводной сети.

4.18 Что такое Temporal Key Integrity Protocol (TKIP)?

Temporal Key Integrity Protocol (TKIP) - это часть стандарта шифрования IEEE 802.11i для беспроводных LAN. TKIP – это протокол следующего поколения WEP-шифрования (Wired Equivalency Protocol), который используется для безопасности беспроводных LAN стандарта 802.11. TKIP предоставляет ключи, строящиеся на смешении пакетов, целостности сообщений и механизме смены одного или более шифровальных ключей (re-keying), устраняя, таким образом, недостатки WEP.

4.19 Что такое Advanced Encryption Standard (AES)?

Средства безопасности являются приоритетными для беспроводных LAN. В правительстве США криптографический алгоритм следующего поколения AES заменяет DES и 3DES.

4.20 Что такое Inter-Access Point Protocol (IAPP)?

Протокол стандарта IEEE 802.11f Inter-Access Point Protocol (IAPP) обеспечивает совместимость с производителем точек доступа (Access Point Vendor), включая роуминг станций 802.11 внутри IP-подсети.

IAPP определяет сообщения и данные, которыми обмениваются точки доступа, объекты IAPP и объекты более высоких уровней, для поддержки роуминга. Протокол IAPP использует TCP для связи с Inter-access точками

доступа и UDP для обмена запросами/ответами RADIUS. Он также использует фреймы второго уровня для обновления таблицы адресации устройств второго уровня.

4.21 Что такое Wireless Distribution System (WDS)?

Wireless Distribution System (WDS) - это опция, позволяющая WLAN точкам доступа связываться напрямую с другими точками доступа по беспроводному каналу (например, беспроводные мосты, сервисы повторителей).

4.22 Что такое Universal Plug and Play (uPNP)?

UPnP – это открытая сетевая архитектура, которая состоит из сервисов, устройств и точек контроля. Её конечная цель заключается в разрешении передачи данных между всеми uPnP устройствами в независимости от того, осуществляется ли эта передача в аудиовизуальной среде, среде операционных систем, языков программирования, проводной/беспроводной среде.

4.23 Что такое размер Maximum Transmission Unit (MTU)?

Maximum Transmission Unit (MTU) - максимальный размер передаваемого блока данных сигнализирует о том, что сетевой стек каких-либо пакетов больше величины, которая будет фрагментирована перед передачей. Во время PPP соединения узел PPP подключения отобразит MRU (список последних по времени использования файлов) и будет принят. Настоящий MTU PPP подключения будет назначен самому малому MTU и MRU узла. Значение по умолчанию – 1400.

4.24 Что такое клонирование MAC адреса?

Клонирование MAC адреса предназначено для ваших специальных приложений, которые требуют регистрации клиентов на сервере с одним идентифицированным MAC адресом.

С тех пор как все клиенты выходят во внешние сети через широкополосный WLAN маршрутизатор, функция клонирования MAC адресов, установленная на маршрутизаторе, обеспечивает правильную работу устройств.

4.25 Что такое DDNS?

Аббревиатура DDNS расшифровывается как Dynamic Domain Name Server (сервер динамических доменных имен). DDNS разработан для того, чтобы пользователи получали DNS сервер с динамическим WAN IP адресом.

4.26 Что такое NTP-клиент?

NTP-клиент разработан для получения временной метки из Интернета с помощью протокола Network Time Protocol. Пользователь может указать часовой пояс, IP адрес NTP-сервера.

4.27 Что такое VPN?

Аббревиатура VPN расшифровывается как Virtual Private Network (частная виртуальная сеть). Она разработана для создания частного канала точка-точка в сети общего пользования или публичной сети.

4.28 Что такое IPSEC?

Аббревиатура IPSEC расшифровывается как IP Security (безопасность IP). Используется для безопасной передачи данных по VPN.

4.29 Что такое WLAN реле блокировки между клиентами?

Infrastructure Basic Service Set – это BSS (оборудование базовой станции) с компонентом, называемым Access Point (точка доступа). Точка доступа выполняет функцию локального реле для BSS. Все станции в BSS связываются с точками доступа и более не связываются напрямую. Станции обмениваются фреймами с помощью точек доступа. Эта функция локального реле эффективно дублирует диапазон IBSS.

4.30 Что такое WMM?

WMM основан на подсети стандарта IEEE 802.11e WLAN QoS. WMM добавляет приоритетные возможности Wi-Fi сетям и оптимизирует их производительность, когда одновременно запущенные различные приложения, с разными требованиями по пропускной способности и задержке, конкурируют за доступ к сетевым ресурсам. Используя WMM, требования конечных пользователей удовлетворяются и поддерживаются на более высоком уровне при работе в различных условиях трафика и окружения. WMM делает возможным для домашних пользователей и менеджеров сетей крупных компаний решить, какие информационные потоки наиболее важны, и назначить им соответствующий приоритет по трафику.

4.31 Что такое WLAN ACK TIMOUT?

Фрейм ACK должен получить истечение времени ожидания события (timeout ACK frame). Если удалённо не получилось его получить в указанный период времени, то timeout фрейм будет послан ещё раз.

5 Примеры настроек

5.1 Пример первый – PPPoE на WAN

Настройки WAN:

PPPoE

User Name (имя пользователя)	**H890123456**
Password (пароль)	**PW192867543210**

Настройки LAN:

IP Address (IP адрес)	**192.168.1.254**
Subnet Mask (маска подсети)	**255.255.255.0**
Default Gateway (шлюз по умолчанию)	**0.0.0.0**
DHCP Client Range (диапазон адресов)	**192.168.1.100 – 192.168.1.200**

Настройки WLAN:

SSID	**MyWLAN**
Channel Number (номер канала)	**11**

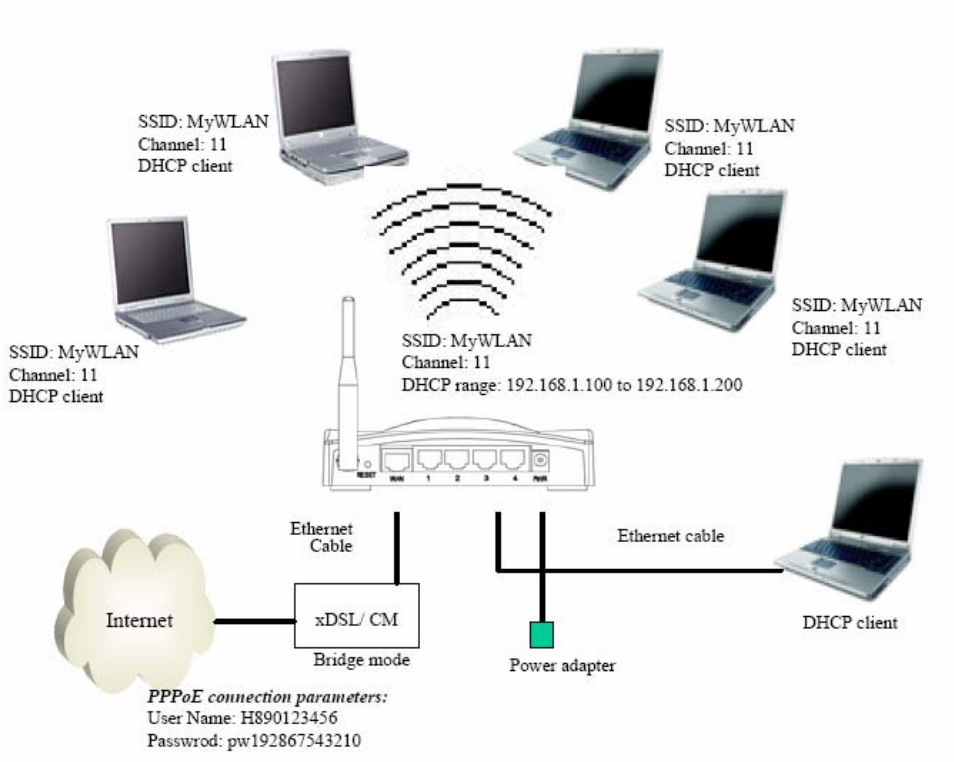


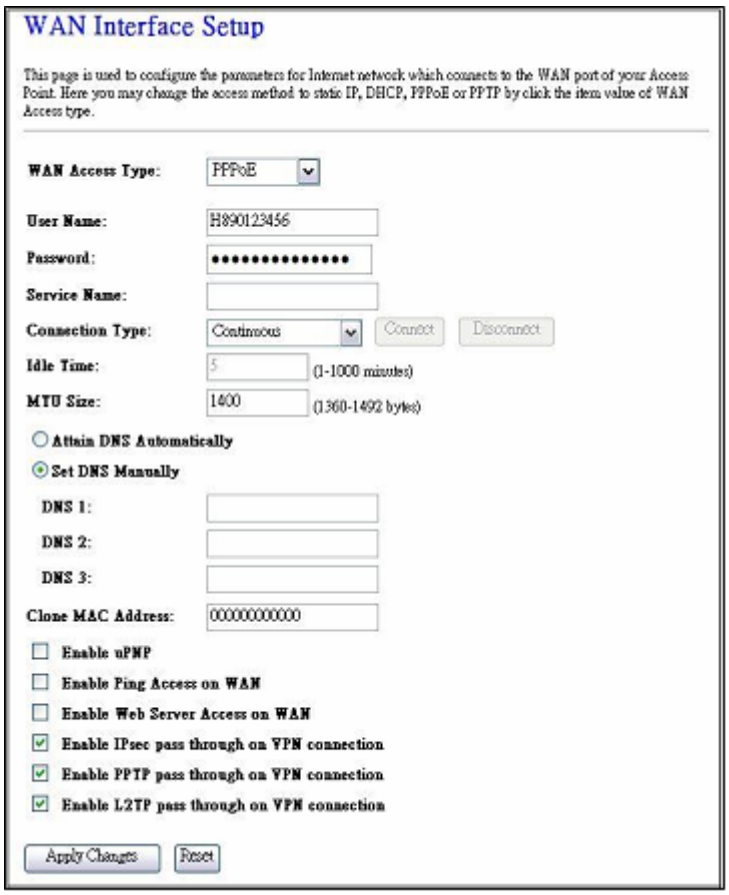
Рисунок 5.1 Первый пример конфигурации – PPPoE на WAN

Настройка на WAN-интерфейсе

Откройте страницу настроек WAN-интерфейса, затем выберите PPPoE и введите имя пользователят PPPoE:

“**H890123456”** и пароль;

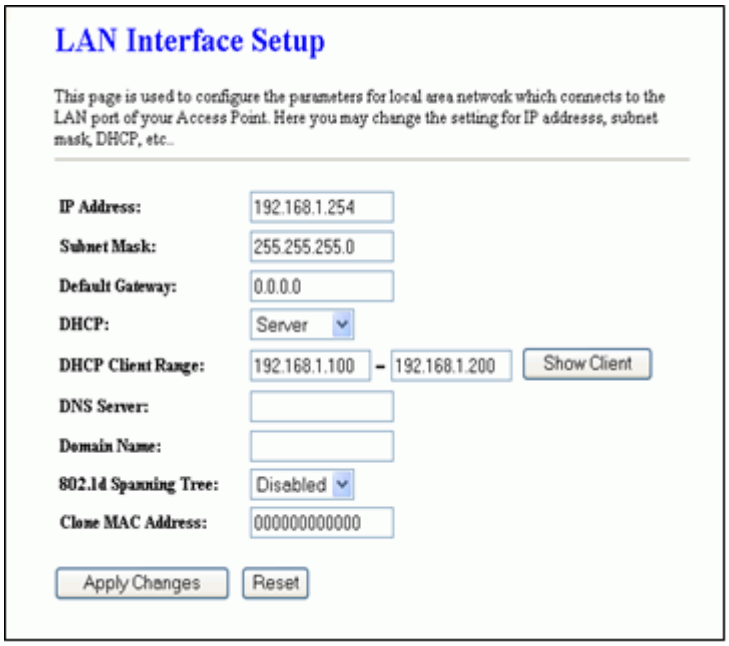
“**PW192867543210**”, пароль на экране зашифрован.



Нажмите кнопку **Apply Changes** для подтверждения настроек.

Настройка на LAN-интерфейсе:

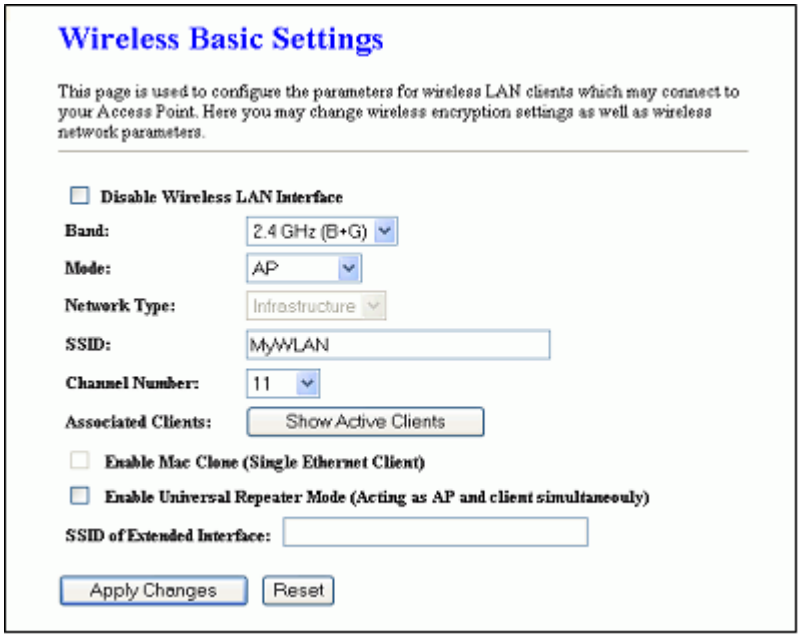
Откройте страницу настроек LAN-интерфейса, введите IP адрес “**192.168.1.254**”, маску подсети “**255.255.255.0**”, шлюз по умолчанию “**0.0.0.0**”, включите DHCP сервер, DHCP клиентский диапазон адресов от “**192.168.1.100**” до “**192.168.1.200**”.



Нажмите кнопку **Apply Changes** для подтверждения настроек.

Настройка на WLAN-интерфейсе

Откройте страницу настроек WLAN-интерфейса, введите SSID “**MyWLAN**”, номер канала“**11**”.



Нажмите кнопку **Apply Changes** для подтверждения настроек.

5.2 Пример второй – фиксированный IP адрес на WAN

Настройки WAN:

IP Address (IP адрес)	**192.168.2.254**
Subnet Mask (маска подсети)	**255.255.255.0**
Default Gateway(шлюз по умолчанию)	**192.168.2.10**
DNS Address(адрес DNS)	**168.95.1.1**

Настройки LAN:

IP Address (IP адрес)	**192.168.1.254**
Subnet Mask (маска подсети)	**255.255.255.0**
Default Gateway (шлюз по умолчанию)	**0.0.0.0**
DHCP Client Range (диапазон адресов)	**192.168.1.100 – 192.168.1.200**

Настройки WLAN:

SSID	**MyWLAN**
Channel Number (номер канала)	**11**

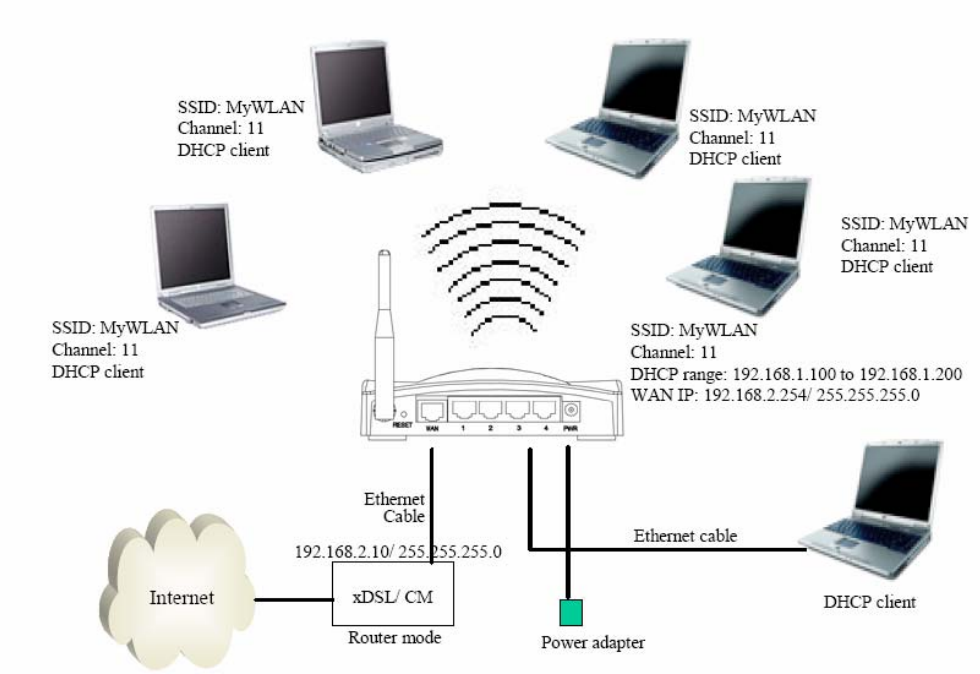
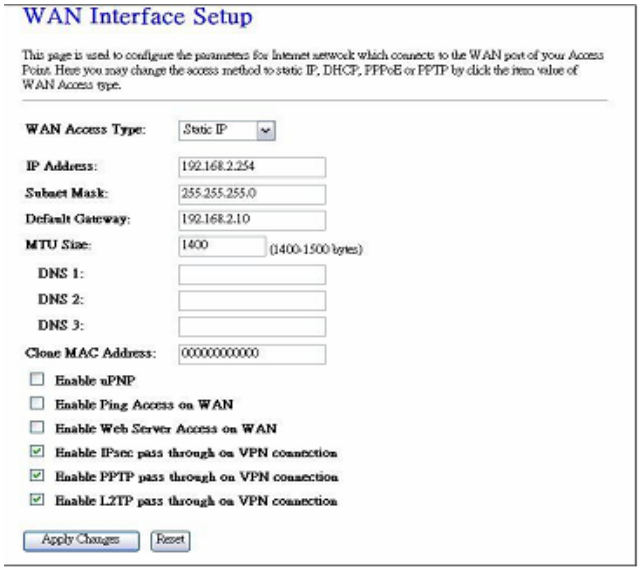


Рисунок 5.2 Второй пример конфигурации – фиксированный IP адрес на WAN

Настройка на WAN-интерфейсе:

Откройте страницу настроек WAN-интерфейса, затем выберите Fixed IP и введите IP адрес “**192.168.2.254”,** маску подсети “**255.255.255.0**”, шлюз по умолчанию “**192.168.2.10**”.

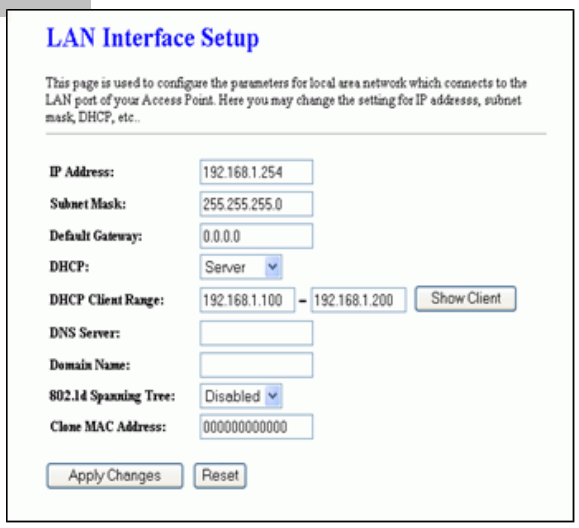


Нажмите кнопку **Apply Changes** для подтверждения настроек.

Настройка на LAN-интерфейсе:

Откройте страницу настроек LAN-интерфейса, введите IP адрес “**192.168.2.254”,** маску подсети “**255.255.255.0**”, включите DHCP сервер, введите клиентский диапазон IP адресов “**192.168.1.100**” - “**192.168.1.200**”.

Нажмите кнопку **Apply Changes** для подтверждения настроек.



Настройка на WLAN-интерфейсе:

Откройте страницу настроек WLAN-интерфейса, введите SSID “**MyWLAN**”, номер канала“**11**”.