54Mbps Беспроводной Широкополосный Интернет роутер

WRT-414

Инструкция по эксплуатации

Торговые марки

Copyright © PLANET Technology Corp. 2002.

Содержание подвергается пересмотру без предварительного предупреждения. PLANET зарегистрированная торговая марка PLANET Technology Corp. Все другие торговые марки принадлежат их соответствующим владельцам.

Отказ от ответственности

PLANET Technology не гарантирует, что аппаратные средства будут работать должным образом во всех средах и приложениях, и не дает гарантий и представления, подразумеваемых или выраженных, относительно качества, рабочих характеристик, или работоспособности при использовании для специфических целей. PLANET Techology приложила все усилия, чтобы сделать это Руководство пользователя наиболее точным и полным; PLANET отказывается от ответственности за любые опечатки или пропуски, которые, возможно, произошли.

Информация в любой части Руководства пользователя изменяется и дополняется PLANET без предварительного уведомления. PLANET не берет на себя никакой ответственности за любые погрешности, которые могут содержаться в этом Руководстве пользователя. PLANET не берёт на себя ответственности и не дает гарантий в выпуске обновлений или сохранения неизменной, какой либо информации в этом Руководстве пользователя, и оставляет за собой право делать изменения в этом Руководстве пользователя и/или в изделиях, описанных в Руководстве, в любое время без уведомления. Если Вы обнаружите информацию в этом руководстве, которая является неправильной, вводит в заблуждение, или неполной, мы с удовольствием ознакомимся с вашими комментариями и предложениями.

Предупреждение Федеральной Комиссии по связи

Это оборудование было протестировано и признано удовлетворяющим требованиям положения о цифровых устройствах принадлежащих к классу А, в части 15 Правил Федеральной комиссии по связи (FCC). Эти ограничения были разработаны в целях обеспечения защиты от вредных помех, которые могут возникать при использовании оборудования в коммерческих целях. Это оборудование может излучать, генерировать и использовать энергию в радиочастотном диапазоне. Если оно будет установлено, и использоваться с отклонениями от настоящего Руководства пользователя, оно может оказать вредное влияние на качество радиосвязи. Работа оборудования, установленного в жилой зоне, вероятно, может вызвать вредное воздействие, тогда владелец будет обязан исправлять последствия вредного воздействия за свой счет.

Предупреждающая маркировка CE

Это устройство может вызывать радиопомехи во внутреннем окружении. В этом случае пользователь может быть обязан принять соответствующие меры.

Поддержка

Для получения информации относительно сервиса и поддержки устройства, пожалуйста, обратитесь на сайт:
http://www.planet.com.ru

- ♦ Серийный номер и MAC адрес вашего оборудования
- ♦ Сообщения об ошибках, которые появлялись с момент возникновения проблемы
- ♦ Какое программное обеспечение работало, когда возникла проблема
- ♦ Произведённые Вами действия (по шагам), сделанные для самостоятельного разрешения проблемы

Руководство пользователя по WRT-414 (переработанное и дополненное):
Беспроводной Широкополосный Интернет Маршрутизатор
Модель: WRT-414
Ревизия: 1.0 (Август, 2005)
Перевод 1.02 (февраль 2007) Бекетов О.Э.
Part No. RM-WRT414.001
Версия программного обеспечения 1.47

Перевод на русский язык

Данный перевод сделан на основе оригинального описания. Переводчик не несёт ответственности за какие-либо разночтения, которые могли возникнуть при переводе специальных терминов и информацию, которая может быть воспринята двояко, ввести в заблуждение или быть ошибочной. Мы не исключаем наличие в нём ошибок, недоработок и опечаток. Если таковые будут обнаружены, то просьба сообщить на e-mail: support@planet.com.ru

Оглавление

РАЗДЕЛ 1 ОБЗОР 5
- 1.1 Комплект поставки 5
- 1.2 Ключевые характеристики 5
- 1.3 Спецификация 6

РАЗДЕЛ 2 ОБЩЕЕ ОПИСАНИЕ 7
- 2.1 Внешний вид и интерфейсы 7
  - *Задняя панель* 7
  - *Передняя Панель* 7
- 2.2 Подключение 8
- 2.3 Начальная настройка подключения 9

РАЗДЕЛ 3 БЫСТРАЯ НАСТРОЙКА 12
- *Временные зоны (Time Zone)* 12
- *Тип широкополосного подключения (Broadband Type)* 12
- 3.1 Кабельный Модем 13
- 3.2 Фиксированный IP Адрес (Fixed-IP xDSL) 13
- 3.3 PPPoE (xDSL) 14
- 3.4 PPTP (xDSL) 15
- 3.5 L2TP (xDSL) 16
- 3.6 Telstra Big Pond 17
- 3.7 Save Settings Successfully (Сохранение и активация настроек) 17

РАЗДЕЛ 4 ОСНОВНЫЕ НАСТРОЙКИ 18
- 4.1 Меню System 19
  - *4.1.1 Временные зоны (Time Zone)* 19
  - *4.1.2 Изменение пароля (Password Setup)* 19
  - *4.1.3 Удаленное администрирование (Remote Management)* 20
- 4.2 Подключение к Интернет (WAN) 20
  - *4.2.1 Режим DHCP клиент (Dynamic IP)* 21
  - *4.2.2 Статический IP Адрес (Static IP Address)* 21
  - *4.2.3 PPPoE (PPP over Ethernet)* 21
  - *4.2.4 PPTP* 21
  - *4.2.5 L2TP* 21
  - *4.2.6 Telstra Big Pond* 21
  - *4.2.7 DNS* 22
  - *4.2.8 DDNS* 23
- 4.3 Локальная сеть (LAN) 23
- 4.4 Беспроводной Интерфейс (Wireless) 25
  - *4.4.1 Основные настройки (Basic Settings)* 25
  - *4.4.2 Расширенные настройки (Advance Settings)* 25
  - *4.4.3 Шифрование (Security)* 26
  - *4.4.3.1 WEP* 27
  - *4.4.3.2 Идентификация по RADIUS (802.1x)* 28
  - *4.4.3.3 WPA* 29
  - *4.4.3.4 Режим WPA Pre-shared Key* 29
  - *4.4.3.5 WPA RADIUS* 30
  - *4.4.4 Контроль доступа (Access Control)* 30
- 4.5 QoS (Quality of Service - качество обслуживания) 31
  - *4.5.1 Добавление, редактирование и удаление правил QoS* 31
- 4.6 Трансляция сетевых адресов (NAT) 32
  - *4.6.1 Перенаправление Портов (Port Forwarding)* 33
  - *4.6.2 Виртуальный Сервер (Virtual Server)* 34
  - *4.6.3 Специальные Приложения (Special Applications)* 34
  - *4.6.4 Служба Уровня Приложения (ALG Settings)* 35
  - *4.6.5 Универсальный PnP (UPnP)* 36
- 4.7 Межсетевой Экран (Firewall) 36
  - *4.7.1 Контроль доступа (Access Control)* 37
  - *4.7.2 Блокировка URL (URL Blocking)* 39
  - *4.7.3 Отказ в Обслуживании (DoS)* 39
  - *4.7.4 Демилитаризованная зона (DMZ)* 40

РАЗДЕЛ 5 НАСТРОЙКА БЕСПРОВОДНОГО ИНТЕРФЕЙСА (WIRELESS CONFIGURATION) 41
- 5.1 Режим работы Точка Доступа (AP Mode) 41
- 5.2 Режим работы Station-Ad Hoc 42
- 5.3 Режим работы Station-Infrastructure 42
- 5.4 Режим работы AP Bridge: Точка - Точка 43
- 5.5 Режим работы AP Bridge: Точка - Много точек 44
- 5.6 Режим работы AP Bridge - WDS (совмещенный режим) 44
- 5.7 Настройка шифрования для режима моста 45

ЧАСТЬ 6 СОСТОЯНИЕ УСТРОЙСТВА (STATUS) 47
6.1 Состояние (Status) 47
6.2 Подключение к Интернет (Internet Connection) 47
6.3 Состояние интерфейсов устройства (Device Status) 47
6.4 Системный журнал System Log 48
6.5 Журнал Защиты (Security Log) 48
6.6 Таблица активных DHCP клиентов (Active DHCP Client) 48
6.7 Статистика (Statistics) 48

ЧАСТЬ 7 РАСШИРЕННОЕ АДМИНИСТРИРОВАНИЕ (TOOLS) 49
7.1 Инструмент Конфигурация (Configuration Tools) 49
7.2 Обновление прошивки (Firmware Upgrade) 50
7.3 Решение проблем с нестабильной работой 50
7.4 Сброс (Reset) 51

ПРИЛОЖЕНИЕ A CMD (КОНСОЛЬ) 52

ПРИЛОЖЕНИЕ B ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ (FAQ) 53

СПИСОК ТЕРМИНОВ 54

Раздел 1 Обзор

PLANET WRT-414 - 802.11g Беспроводный Широкополосный Маршрутизатор, который предназначен для организации совместной работы пользователей проводной (LAN) и беспроводной (Wi-Fi) локальной сети с возможностью одновременного доступа к сети Интернет, через одно (общее) подключение. Беспроводной роутер поддерживает 64/128 -битное WEP, WPA-PSK, WPA, WPA2 шифрование и фильтрацию MAC/IP адресов для надежной защиты беспроводных подключений. Помимо обычного режима работы «Точка доступа» поддерживаются AP клиент, Bridge и WDS, что обеспечивает пользователям больше возможностей при выборе режима работы.

WRT-414 позволит Вам настроить состояние портов для использования специальных приложений. Кроме того, Межсетевой Экран SPI надёжно защитит ваши персональные компьютеры в локальной сети от несанкционированного доступа и многих видов DOS атак из сети Интернет. WRT-414 может высылать предупреждения на электронную почту при возникновении нештатных ситуаций. Функции Virtual Server и DMZ помогут Вам организовать доступ к ресурсам и определённым сервисам локальной сети из Интернета. Поддержка QoS предназначена для обеспечения гарантированной пропускной способности для критичных к задержкам сервисов (Медиа коннект, IP телефония и т.п.). Администраторы могут назначить правила QoS в соответствии с типом трафика, IP источника/адресата, номера коммуникационного порта, чтобы наиболее полно и рационально использовать пропускную способность сети.

WRT-414 представляет собой полностью законченное решение для небольших организаций и индивидуальных пользователей, сочетающее в себе Беспроводную точку доступа, Маршрутизатор с расширенными возможностями Межсетевого экрана и 4-х портовый коммутатор.

1.1 Комплект поставки

- WRT-414
- Один экземпляр инструкции по быстрой установке и настройке (англ.)
- Компакт диск с Инструкцией по эксплуатации
- Адаптер питания
- Одна внешняя Дипольная Антенна

✍**Внимание!** ***Если любая из этих частей отсутствует или повреждена, пожалуйста, немедленно свяжитесь с вашим дилером.***

1.2 Ключевые характеристики

- Частотный диапазон 2.4 ГГц.
- Поддержка беспроводного оборудования стандартов 802.11g и 802.11b
- Встроенный DHCP сервер
- Удобный пользовательский WEB интерфейс. Настройка с помощью браузера.
- Поддержка фильтрации MAC/IP адресов, блокирование URL
- Встроенный 4-х портовый коммутатор
- Встроенный Мастер Настройки, облегчающий первичную настройку оборудования.
- Подключение к Интернет через сетевой кабель или xDSL модем
- Поддерживаемые типы подключения: **Статический IP адрес, DHCP клиент, PPPoE, PPTP, L2TP**
- Позволяет настроить доступ к различным ресурсам в локальной сети из Интернет
- Режимы работы **AP / AP Client / WDS / Bridge**
- Поддержка 64/128-битное **WEP, WPA-PSK, WPA, WPA2** Шифрование для защиты беспроводной сети
- 4 порта LAN (10/100M) и один порт WAN (10/100M), с поддержкой Auto-MDI/MDI-X
- Поддержка QoS
- Контроль состояния: Активные Клиенты DHCP, лог Защиты и Состояние подключений и устройства
- Удаленное управление позволяет изменять конфигурацию удаленно (через Интернет)
- Межсетевой экран SPI и защита от DoS атак
- Поддержка функции UPnP

1.3 Спецификация

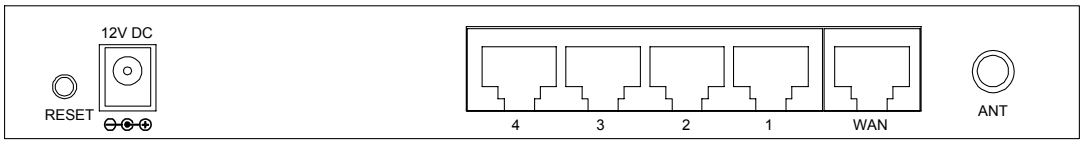
Модель	WRT-414
Стандарт	IEEE 802.11g/802.11b (Wireless), IEEE 802.3 (Wired)
Частотный диапазон	2.400~2.4835GHz
Скорость канала	802.11g: 54/48/36/24/18/12/9/6Mbps 802.11b: 11/5.5/2/1Mbps
Модуляция	OFDM@54Mbps, CCK@11/5.5Mbps, DQPSK@2Mbps and DBPSK@1Mbps
Тип сигнала	Direct Sequence Spread Spectrum (DSSS)
Антенна	Одна Съемная Дипольная Антенна
Режимы работы	Access Point Station - Ad-Hoc Station - Infrastructure Bridge - Point to Point Bridge - Point to MultiPoint Bridge - WDS
Каналы	FCC: 11 Channels (US, Canada) ETSI: 13 Channels (Europe) ELEC: 14 Channels (Japan)
Выходная мощность	18dBm (типовая)
WAN разъём	1-порт RJ-45, Auto-MDI/MDI-X
LAN Интерфейс	4-порта RJ-45, Auto-MDI/MDI-X
Сетевой кабель	Категории 5/5e или выше, 4-х парный
Индикация	PWR (Питание) WLAN (Беспроводная сеть) WAN: 10/100M, LNK/ACT LAN: 4 x 10/100M, 4 x LNK/ACT
Адаптер питания	12 Вольт постоянного тока, 1A
Температура	0 ~ 55 градусов C (Рабочая)
Влажность	10 ~ 90%, без образования конденсата (Рабочая)
Габариты	193 x 93 x 28 (мм)
Вес	285г
Электромагнитная совместимость	FCC class B, CE-mark

Раздел 2 Общее описание

2.1 Внешний вид и интерфейсы

Задняя панель

На рисунке показана задняя панель WRT-414. На ней расположены порты **LAN (1,2,3,4)**, порт **WAN**, разъём питания, разъём подключения антенны и кнопка сброса **(Reset)**.



1) Локальная Сеть (LAN)
Вы можете подключить к портам встроенного 4-х портового коммутатора LAN ваши компьютеры, серверы печати и данных, другие коммутаторы в локальной сети, Интернет камеры, IP телефоны и другое активное сетевое оборудование.

2) Глобальная сеть (WAN)
WAN порт предназначен для подключения к сети Интернет или другой внешней сети через кабель или xDSL модем для обеспечения совместного использования ресурсов глобальной сети всеми пользователями LAN.

3) Reset
Это кнопка выполняет две функции одновременно.

Перезагрузка – если роутер завис в результате скачка напряжения, или по какой либо другой причине (к нему невозможно подключиться через WEB интерфейс или он не отвечает на ping), то нажмите на кнопку reset на время меньше 5-ти секунд. Отпустите кнопку и дождитесь перезагрузки роутера. После завершения перезагрузки должна восстановиться нормальная работа роутера.

Полный сброс настроек – если вы забыли настройки (Имя пользователя и пароль) или имеются проблемы с работой оборудования, и вы не можете найти причину, то нажмите и удерживайте кнопку **reset** больше 5-ти секунд. Отпустите кнопку и дождитесь перезагрузки роутера. Все настройки будут сброшены (включая IP адрес, Имя пользователя и пароль) на значения по умолчанию.

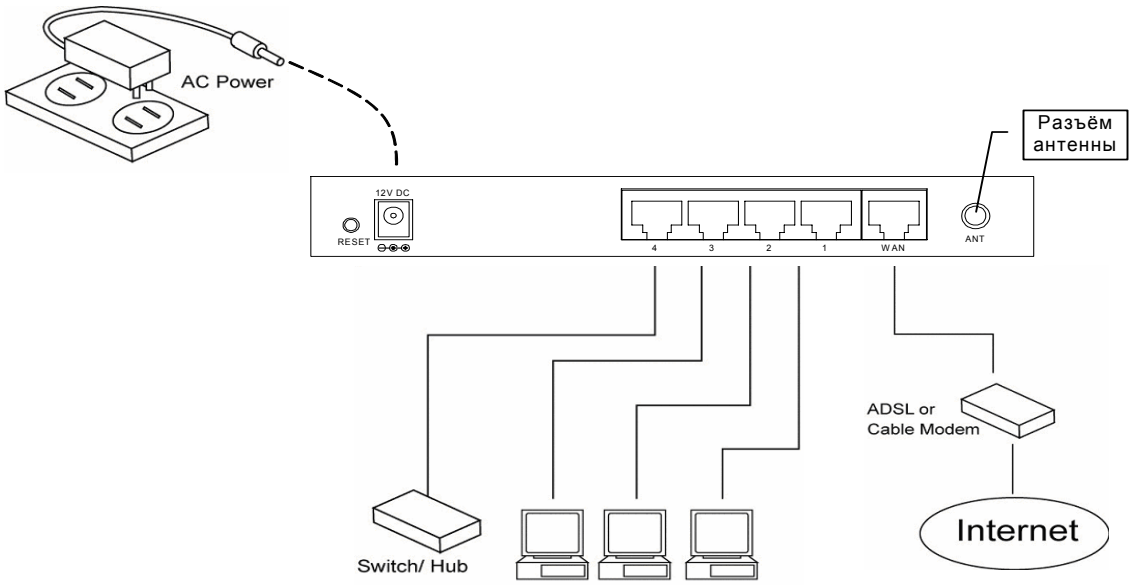
Передняя Панель

На передней панели расположены индикаторы, отображающие состояние интерфейсов роутера.

Индикация		Цвет	Состояние	Описание
PWR		Зелёный	Горит	Питание включено
			Не горит	Питание выключено
			Моргает	Процесс загрузки оборудования
WLAN		Оранжевый	Моргает	Передача или прием пакетов через беспроводной интерфейс
			Не горит	Беспроводной интерфейс не активен
WAN	**10/100M**	Зелёный	Горит	WAN порт подключен на скорости 100Mbps
			Не горит	WAN порт подключен на скорости 10Mbps
	LNK/ACT	Зелёный	Горит	Подключение установлено
			Моргает	Передача или прием пакетов
LAN	**10/100M**	Зелёный	Горит	LAN порт подключен на скорости 100Mbps
			Не горит	LAN порт подключен на скорости 10Mbps
	LNK/ACT	Зелёный	Горит	Подключение установлено
			Моргает	Передача или прием пакетов
			Не горит	нет подключения LAN

2.2 Подключение

На рисунке показано общее схемотехническое подключения устройств к интерфейсам маршрутизатора.



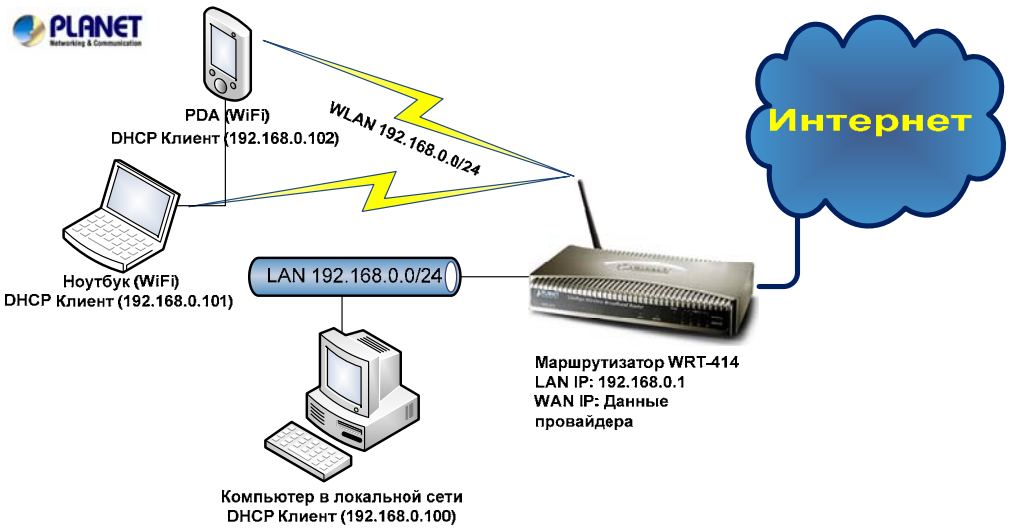
Перед настройкой оборудования необходимо выполнить следующие действия:

1. **Определить оптимальное место для размещения WRT-414.** Обычно беспроводной оборудование принято размещать в центре, относительно беспроводных клиентов, которые будут к нему подключаться.
2. **Прикрутите внешнюю антенну и выберите её оптимальное положение.**
3. **Подключить кабели RJ-45 к LAN портам WRT-414.** Соедините LAN порты WRT-414 с коммутаторами, компьютерами или другим активным сетевым оборудованием в вашей локальной сети кабелем RJ-45.

ВАЖНО! Перед подключением необходимо убедиться, что LAN IP адрес WRT-414 не конфликтует ни с одним из адресов в Вашей локальной сети и настройки сетевого окружения подходят для вашей локальной сети. Также необходимо убедиться, что в Вашей локальной сети больше нет активного DHCP сервера. Если одно из этих условий не соблюдается, то перед подключением всей локальной сети необходимо выполнить соответствующие настройки, описанные ниже. В этом случае подключите к любому порту LAN только один компьютер и с него произведите начальную настройку.

4. **Подключить кабель RJ-45 к WAN порту WRT-414.** Детальная настройка будет описана ниже.
5. **Подключите адаптер питания**. После включения адаптера в розетку и загрузки маршрутизатора он будет готов для дальнейшей настройки.

Внимание! Для питания устройства необходимо использовать только оригинальный сетевой адаптер из комплекта поставки! В случае выхода адаптера из строя обратитесь к поставщику оборудования.



Настройки маршрутизатора по умолчанию:

LAN IP: 192.168.0.1
Имя пользователя: admin
Пароль: admin

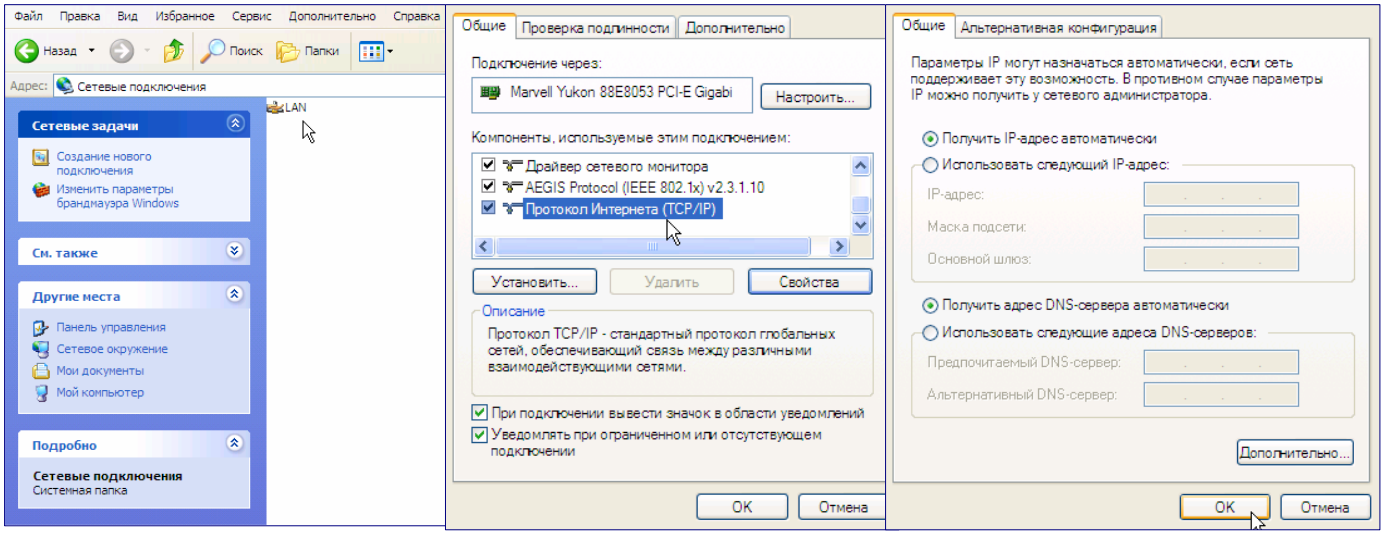
2.3 Начальная настройка подключения

Выполните пошаговую первоначальную настройку роутера в соответствии с приведённым ниже описанием.

Шаг I. Включите маршрутизатор, подключив адаптер питания к разъёму 12V DC и вставив его в розетку 220 Вольт.

Шаг II. Дождитесь загрузки роутера (примерно 2-3 минуты)

Шаг III. Подключите к одному из портов LAN персональный компьютер. В свойствах сетевого окружения персонального компьютера для подключения по локальной сети (для сетевой карточки Вашего компьютера) предварительно установите получить IP адрес автоматически и получить адрес DNS сервера автоматически (см. Скриншоты)



Шаг IV. Все остальные хосты (персональные компьютеры или другие активные сетевые устройства) должны также подключаться с аналогичными настройками (автоматическое получение параметров сетевого окружения) или их параметры следует настроить вручную на соответствующую подсеть.

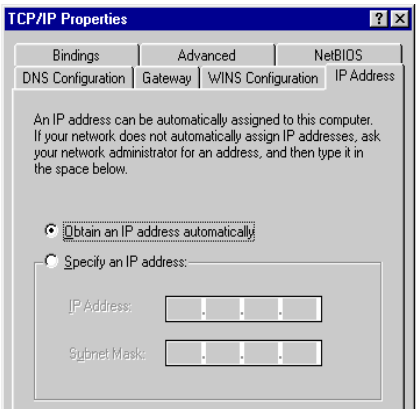
✍Внимание! ***По умолчанию маршрутизатор использует для Локальной сети IP адреса из подсети класса С (192.168.0.0/24). Если Вам необходимо использовать другой диапазон адресов, то впоследствии, при настройке маршрутизатора вы можете изменить этот параметр.***

Правильно настроенные компьютеры должны получить IP адрес автоматически

По умолчанию у роутера включен DHCP сервер и он выдает параметры сетевого окружения автоматически всем активным сетевым устройствам, подключенным в режиме DHCP клиент. В данном описании приведены примеры настройки для операционных систем семейства Windows 95/98/Me, 2000, NT, XP и Vista. Для других операционных систем (Macintosh, Sun, Linux и т.п.) следует обратиться к руководству настройки сетевого подключения этой операционной системы. Ниже показана пошаговая настройки для следующих ОС: 2a) **Windows 95/98/Me**, 2b) **Windows XP**, 2c) **Windows 2000** и 2d) **Windows NT**.

2a) Windows 95/98/Me

1. Нажмите кнопку ***Start (ПУСК)*** и выберите ***Settings (Настройки)***, откройте ***Control Panel (Панель Управления)***.
2. Дважды нажмите левой кнопкой мышки на иконку ***Network (Сеть)***. Откроется окно *Network*.
3. Проверьте список Сетевых Компонентов. Если протокол TCP/IP не установлен, нажмите кнопку *Add* (добавить), чтобы установить. Если протокол TCP/IP установлен, то переходите к **Шагу 6**.
4. В диалоговом окне ***Network Component Type (Тип сетевых компонентов)***, выберите ***Protocol (Протокол)***, и нажмите кнопку ***Add (Добавить)***.
5. В диалоговом окне ***Select Network Protocol (Выбор сетевых протоколов)***, выберите ***Microsoft*** и ***TCP/IP*** и затем нажмите *кнопку* ***OK***, чтобы начать установку протокола TCP/IP. Для завершения настройки скорее всего потребуется компакт-диск с Вашей версией Windows.
6. После установки TCP/IP, возвратитесь к диалоговому окну ***Network***. Выберите ***TCP/IP*** из списка ***Network Component (Сетевых Компонентов)***, и нажмите кнопку ***Properties (Свойства)***.
7. Проверьте параметры настройки для всех вкладок открывшегося окна:



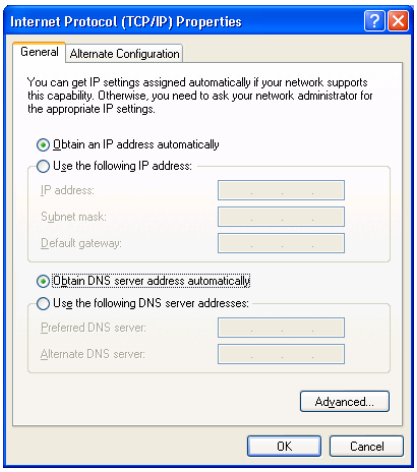
- **Bindings**: Проверить наличие *Client for Microsoft Networks* и *File and printer sharing for Microsoft Networks*.
- **Gateway**: все поля пустые.
- **DNS Configuration**: выбрать *Disable DNS (отключить DNS).*
- **WINS Configuration**: выбрать *Disable WINS Resolution.*
- **IP Address**: выбрать *Obtain IP address automatically (получить IP адрес Автоматически)*.

8. Перезагрузите компьютер. После завершения загрузки компьютер получит IP адрес от DHCP сервера роутера.

✍Внимание! **Обязательно убедитесь, что DHCP сервер маршрутизатора является единственным DHCP сервером в вашей локальной сети! Если в локальной сети используется ещё один DHCP сервер, то его следует временно отключить и в дальнейшем решить, какой из DHCP серверов Вы будете использовать (встроенный в маршрутизатор или другой).**

Как только Вы завершили настройку сетевого интерфейса Вашего компьютера на автоматическое получение IP адреса Вы можете перейти к **Шагу III**.

2b) Windows XP



1. Нажмите кнопку ***Start (ПУСК)*** и выберите ***Settings (Настройки)***, откройте ***Network Connections (Сетевые подключения)***.
2. Дважды нажмите левой кнопкой мышки на иконку ***Local Area Connection (Подключение по локальной сети)***. Откроется окно ***Local Area Connection (Подключение по локальной сети)***.
3. В диалоговом окне ***Подключение по локальной сети*** на вкладке общие, выберите ***Properties (Свойства)***и в списке компонентов используемых этим подключением нужно выбрать **протокол Интернета TCP IP** и нажать ***Properties (Свойства)***.
4. Откроется окно свойств Протокола TCP IP.
5. Необходимо выбрать ***Obtain an IP address automatically (Получить IP адрес автоматически)*** и ***Obtain DNS server address automatically (Получить адрес DNS-Сервера автоматически)***.
6. Нажмите несколько раз кнопку OK на соответствующих открытых вкладках, чтобы сохранить изменения.
7. После сохранения изменений компьютер сможет автоматически получить IP адрес от DHCP сервера роутера.

✍Внимание! **Обязательно убедитесь, что DHCP сервер маршрутизатора является единственным DHCP сервером в вашей локальной сети! Если в локальной сети используется ещё один DHCP сервер, то его следует временно отключить и в дальнейшем решить, какой из DHCP серверов Вы будете использовать (встроенный в маршрутизатор или другой).**

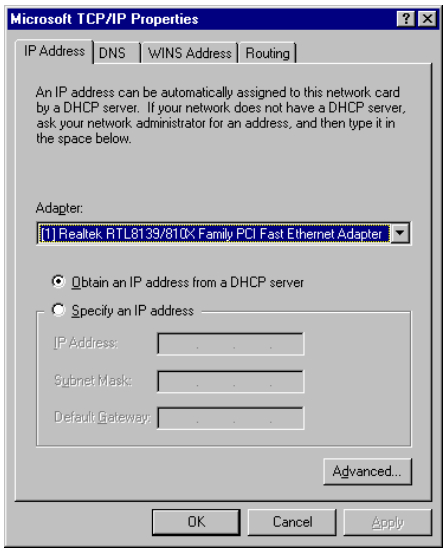
Как только Вы завершили настройку сетевого интерфейса Вашего компьютера на автоматическое получение IP адреса Вы можете перейти к **Шагу III**.

2c) Windows 2000

1. Нажмите кнопку ***Start (ПУСК)*** и выберите ***Settings (Настройки)***, откройте ***Network and Dial-up Connections***.
2. Дважды нажмите левой кнопкой мышки на иконку ***Network and Dial-up Connections***. В открывшемся окне ***Network and Dial-up Connections*** нажмите на иконку ***Local Area Connection (Подключение по локальной сети)***.
3. В диалоговом окне ***Подключение по локальной сети*** выберите ***Properties (Свойства)*** и в списке компонентов используемых этим подключением нужно выбрать **протокол Интернета TCP IP** и нажать ***Properties (Свойства)***.
4. Откроется окно свойств Протокола TCP IP.
5. Необходимо выбрать ***Obtain an IP address automatically (Получить IP адрес автоматически)*** и ***Obtain DNS server address automatically (Получить адрес DNS-Сервера автоматически)***.
6. Нажмите несколько раз кнопку OK на соответствующих открытых вкладках, чтобы сохранить изменения.
7. После сохранения изменений компьютер сможет автоматически получить IP адрес от DHCP сервера роутера.

Как только Вы завершили настройку сетевого интерфейса Вашего компьютера на автоматическое получение IP адреса Вы можете перейти к **Шагу III**.

2d) Windows NT



1. Нажмите кнопку ***Start*** и выберите ***Settings,*** откройте ***Control Panel***.
2. Дважды нажмите левой кнопкой мышки на иконку ***Network***. Выберите ***Protocol*** в открывшемся окне *Network*.
3. В списке Сетевых Протоколов нужно выбрать TCP/IP Protocol. Если протокол TCP/IP не установлен, нажмите кнопку *Add* (добавить), чтобы установить. Если протокол TCP/IP установлен, то переходите к **Шагу 5**.
4. В диалоговом окне ***Network Component Type (Тип сетевых компонентов)***, выберите ***Protocol (Протокол)***, и нажмите кнопку ***Add (Добавить)***.
5. В диалоговом окне ***Select Network Protocol (Выбор сетевых протоколов)***, выберите ***TCP/IP Protocol*** и затем нажмите *кнопку* ***OK***, чтобы начать установку протокола TCP/IP. Для завершения настройки, скорее всего, потребуется компакт-диск с Вашей версией Windows.
6. После установки TCP/IP, возвратитесь к диалоговому окну ***Network***. Выберите ***TCP/IP*** из списка ***Network Protocols***, и нажмите кнопку ***Properties***.
7. Проверьте параметры настройки для всех вкладок открывшегося окна:
- **DNS Configuration**: выбрать *Disable DNS (отключить DNS).*
- **WINS Configuration**: выбрать *Disable WINS Resolution.*
- **IP Address**: выбрать *Obtain IP address automatically (получить IP адрес Автоматически)*.
8. Перезагрузите компьютер. После завершения загрузки компьютер получит IP адрес от DHCP сервера роутера.

✍Внимание! **Обязательно убедитесь, что DHCP сервер роутера является единственным DHCP сервером в вашей локальной сети! Если в локальной сети используется ещё один DHCP сервер, то его следует временно отключить и в дальнейшем решить, какой из DHCP серверов Вы будете использовать (встроенный в роутер или другой).**

Как только Вы завершили настройку сетевого интерфейса Вашего компьютера на автоматическое получение IP адреса Вы можете перейти к **Шагу III**.

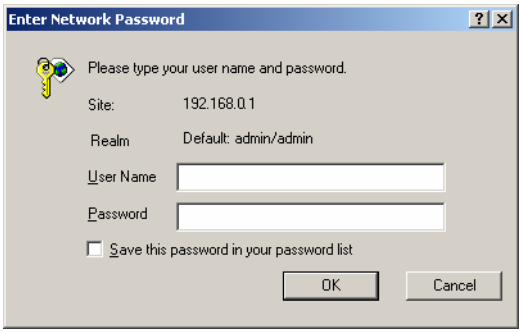
Шаг V. Как только Вы настроили ваши персональные компьютеры для автоматического получения IP адреса, DHCP сервер маршрутизатора автоматически назначит вашим клиентам LAN IP адреса. По умолчанию DHCP сервер включен, для того чтобы Вы могли получить адрес IP автоматически.

☝ Пример просмотра параметров сетевого окружения с помощью командной строки показан в Приложении А.

✍Внимание! **Чтобы отключить встроенный DHCP сервер роутера Вам необходимо обратиться к Разделу 3.3 Локальная сеть LAN**

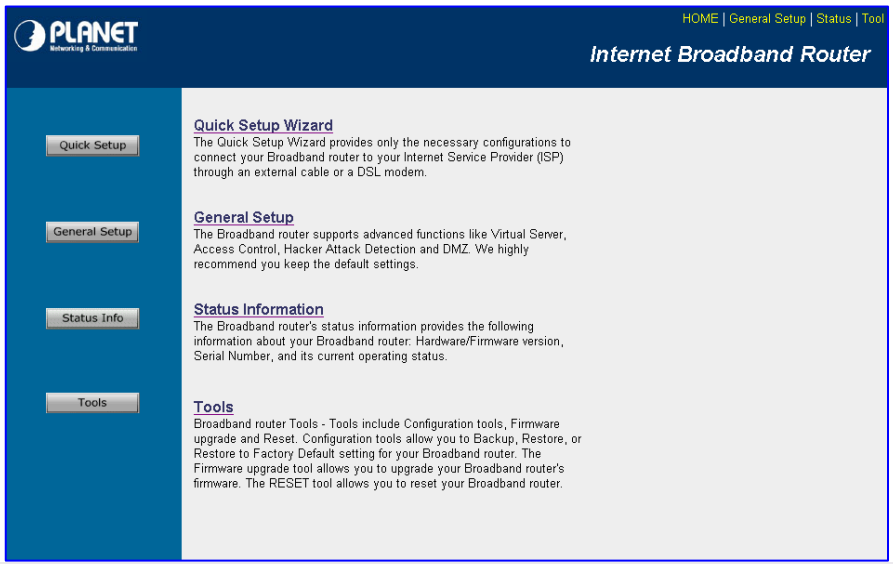
Шаг VI. Как только ваш персональный компьютер получил адрес IP от вашего маршрутизатора, введите в адресной строке браузера **IP адрес http://192.168.0.1** (IP адрес широкополосного маршрутизатора) и нажмите **Enter**.

Шаг VII. Откроется окно с запросом имени пользователя и пароля. Введите Имя пользователя (User Name) и Пароль (Password) и нажмите кнопку **OK**.



✍Внимание! **По умолчанию имя пользователя "*admin*", а пароль "*admin*". После завершения настройки рекомендуется изменить эти значения (Смотрите 3.1.2 Изменение Пароля)**

Шаг VIII. Откроется "Домашняя" страница WEB интерфейса маршрутизатора. Эта страница содержит несколько разделов: **Quick Setup Wizard**, **General Setup**, **Status Information** и **Tools.**



Меню	Описание
Quick Setup Wizard – Быстрая Настройка *(Раздел 3)*	**Этот раздел меню поможет выполнить начальную настройку роутера**
General Setup – *Основные Настройки (Раздел 4)*	**В этом разделе можно изменить как основные настройки для портов LAN и WAN, так и дополнительные (NAT, Межсетевой экран, DMZ, Контроль доступа и т.п.).**
Status Information – *Информация о состоянии устройства (Раздел 6)*	**В этом разделе можно посмотреть информацию о статистике и состоянии подключений.**
Tools – *Расширенное Администрирование (Раздел 7)*	**Этот раздел предназначен для сохранения или восстановления конфигурации роутера, а также для обновления прошивки оборудования.**

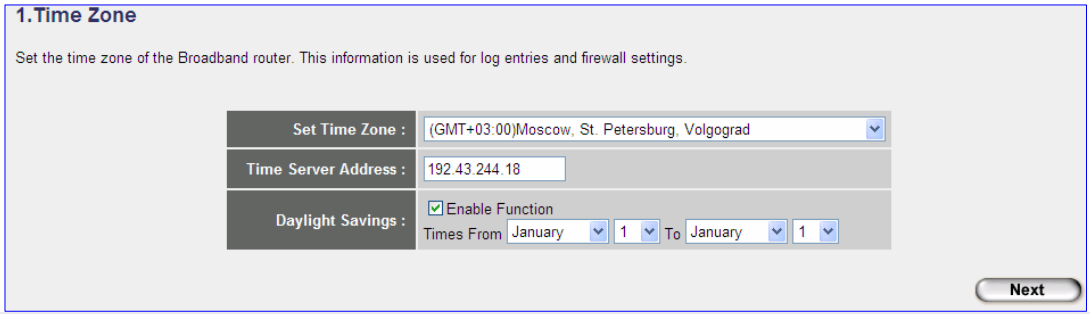
Шаг IX. Нажмите **Quick Setup Wizard** (см. Раздел 3) для выполнения основных настроек по подключению вашего роутера к сети Интернет Провайдера. После завершения Быстрой настройки обратитесь к меню General Setup для выполнения дополнительных настроек.

Раздел 3 Быстрая настройка

Этот раздел меню поможет выполнить начальную настройку маршрутизатора для подключения его к Интернет. После нажатия кнопки **Quick Setup** откроется меню настройки Временной зоны.

Временные зоны (Time Zone)

В этом меню необходимо выбрать и настроить временную зону в соответствии с вашим часовым поясом. Например, для Москвы это +3.

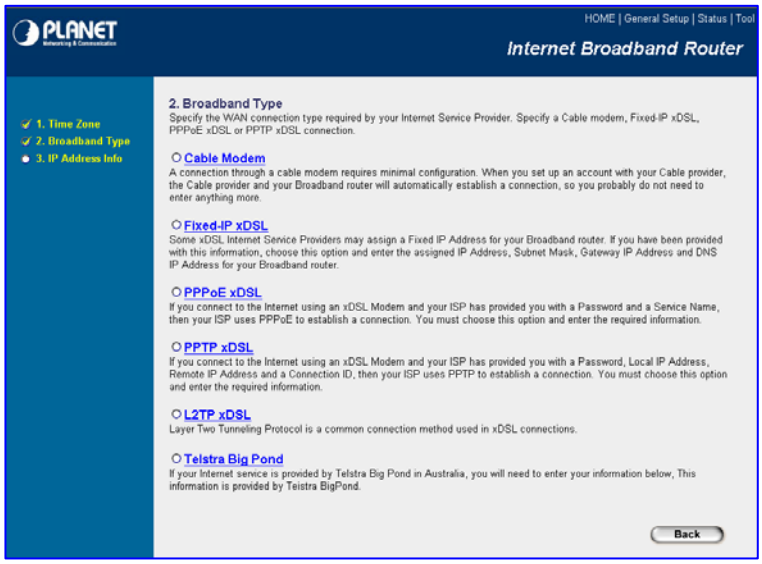


Параметр	Описание
Set Time Zone	Выбор часового пояса.
Time Server Address	IP адрес сервера времени. Измените этот IP адрес, если указанный по умолчанию не работает.
Enable Daylight Savings	Маршрутизатор умеет учитывать переход на летнее время и обратно. Если Вы хотите использовать эту функцию, то поставьте галочку и настройте даты перехода на летнее время и обратно в двух следующих строках меню.
Start Daylight Savings Time	Начало периода "Летнее Время"
End Daylight Savings Time	Конец периода "Летнее Время"

Нажмите **NEXT** для сохранения параметров и перехода к следующему пункту меню раздела Быстрой настройки.

Тип широкополосного подключения (Broadband Type)

В этом разделе меню вы можете настроить параметры сетевого окружения WAN интерфейса для подключения к Интернет. Для этого необходимо обратиться к настройкам, выданным Вам Интернет провайдером. Также здесь настраиваются дополнительные DNS сервера и сервер Динамических Доменных Имен (DDNS).



Внимание!: **Интернет провайдеры предоставляют доступ в Интернет используя различные типы подключения. Пожалуйста, перед настройкой оборудования уточните эти данные.**

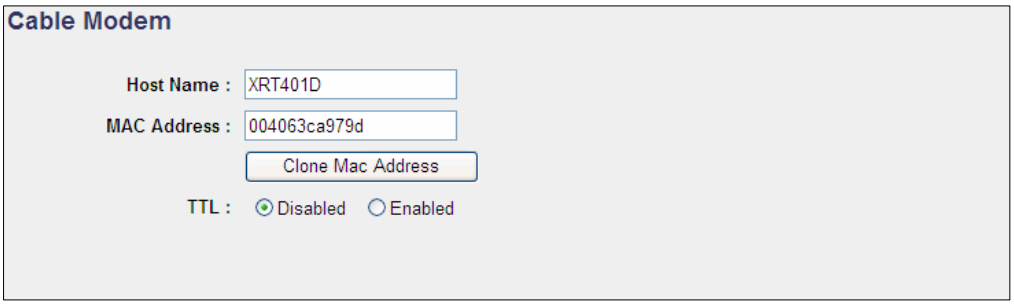
Раздел меню	Описание
3.1 Cable Modem	Интернет провайдер автоматически назначает IP адрес (режим DHCP клиент)
3.2 Fixed-IP xDSL	Интернет провайдер выдал Вам статический IP адрес
3.3 PPPoE	Интернет провайдер осуществляет подключение по протоколу Point-to-Point Protocol over Ethernet (PPPoE).
3.4 PPTP	Интернет провайдер осуществляет подключение по протоколу Point-to-Point Tunneling Protocol (PPTP).

Также маршрутизатор может выполнять подключение по протоколам L2TP и Telstra Big Point, но они не будут рассматриваться в этом мануале, так как Российские провайдеры обычно не используют эти типы подключения.

Выберите нужный тип подключения (2.1, 2.2, 2.3 или 2.4). Если Вы ошиблись, то нажмите Back для возврата к предыдущему меню.

3.1 Кабельный Модем

В режиме **Cable Modem** маршрутизатор получает IP адрес и все необходимые дополнительные параметры сетевого окружения от DHCP сервера Интернет провайдера.



Параметр	Описание
Имя ХОСТА (HOST Name)	Если Интернет провайдер требует ввода определённого Имени хоста, то его следует ввести в поле **Host Name**.
Подмена MAC адреса (MAC Address)	Если Интернет провайдер ранее привязал подключение по MAC адресу Вашего компьютера, то можно заменить MAC адрес роутера для порта WAN, чтобы не обращаться в службу технической поддержки провайдера. Для этого подключите к порту LAN компьютер, который ранее был напрямую подключен к сети Интернет (используйте ту сетевую карту компьютера, в которую ранее был подключен сетевой кабель от провайдера). Выполните необходимые начальные настройки сетевого окружения для этой сетевой карты компьютера. Запустите Браузер и войдя в этот раздел меню нажмите кнопку **Clone MAC Address**. Для дополнительной информации смотрите приложение А.
TTL	Функция определения времени жизни пакетов. Включение функции добавляет 1 к времени жизни пакета при прохождении его из локальной сети через роутер (можно посмотреть командой Ping). По умолчанию – **Выключено**.

Внимание!:

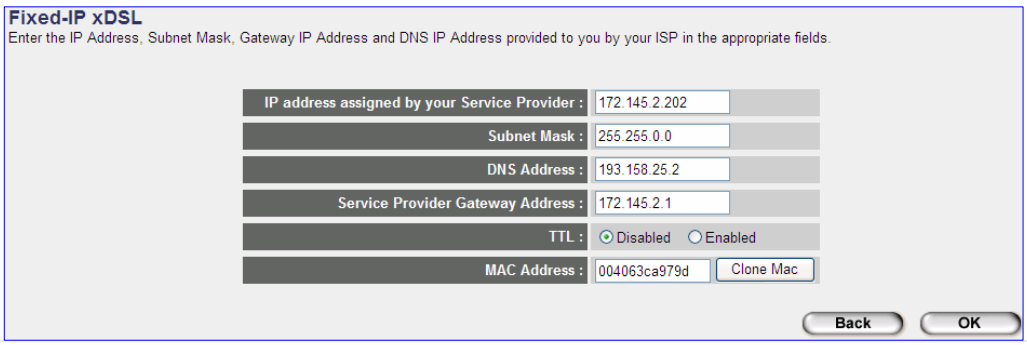
- Разделы **Host Name** и **MAC** address являются дополнительными и могут не потребоваться при настройке подключения к Интернет.
- Для правильной работы Интернет Браузера и других приложений на компьютерах и других хостах в локальной сети, использующих Доменные Имена, не забудьте указать в меню **DNS (раздел 4.2.7)** IP адреса первичного и вторичного **DNS** сервера.

*Нажмите кнопку **OK**, после завершения настройки. Роутер сохранит изменения и откроет окно: **Save Setting Successfully**. Нажмите кнопку **Continue** для выполнения других настроек или **Apply** для перезагрузки роутера и активации сделанных изменений. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет. Для тонкой настройки роутера обратитесь к разделам 4–7.*

3.2 Фиксированный IP Адрес (Fixed-IP xDSL)

Если для подключения к Интернет провайдер выдал Вам статический IP адрес, то необходимо выбрать тип подключения Fixed-IP xDSL. Введите параметры сетевых настроек в соответствующие строки и нажмите OK.

Подмена MAC адреса – Если Интернет провайдер ранее привязал подключение по MAC адресу Вашего компьютера, то можно заменить MAC адрес роутера для порта WAN, чтобы не обращаться в службу технической поддержки провайдера. Для этого подключите к порту LAN компьютер, который ранее был напрямую подключен к сети Интернет (используйте ту сетевую карту компьютера, в которую ранее был подключен сетевой кабель от провайдера). Выполните необходимые начальные настройки сетевого окружения для этой сетевой карты компьютера. Запустите Браузер и войдя в этот раздел меню нажмите кнопку **Clone MAC Address** в меню Кабельный модем. После этого сделайте настройку в этом меню, выбрав тип подключения Fixed-IP. Для дополнительной информации смотрите приложение А.



Параметр	Описание
IP Address	Статический IP адрес, выданный Вам Интернет провайдером.

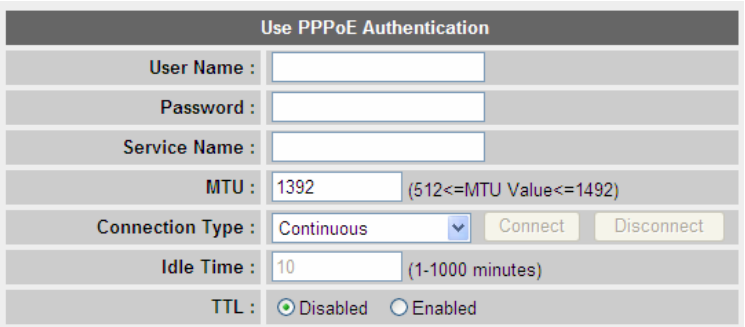
Параметр	Описание
SP Gateway address	Шлюз по умолчанию (Интернет провайдера)
DNS aAdress	IP адрес DNS сервера провайдера
Subnet Mask	Маска подсети, используемая Интернет провайдером (например, 255.255.0.0)
TTL	Функция определения времени жизни пакетов. Включение функции добавляет 1 к времени жизни пакета при прохождении его из локальной сети через роутер (можно посмотреть командой Ping). По умолчанию – **Выключено**.

*Нажмите кнопку **OK**, после завершения настройки. Роутер сохранит изменения и откроет окно: **Save Setting Successfully**. Нажмите кнопку **Apply** для перезагрузки роутера и активации сделанных изменений. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет. Для тонкой настройки роутера обратитесь к разделам 4–7.*

Внимание!: Для правильной работы Интернет Браузера и других приложений на компьютерах и других хостах в локальной сети, использующих Доменные Имена, не забудьте указать в меню **DNS (раздел 4.2.7)** IP адреса первичного и вторичного **DNS** сервера.

3.3 PPPoE (xDSL)

Обычно этот режим используется при широкополосном подключении через ADSL модем. Также его используют некоторые провайдеры кабельных сетей. Этот режим позволяет автоматически получить все необходимые настройки подключения от PPPoE сервера, используя выданные провайдером имя пользователя и пароль. Для настройки этого типа подключения нужно включить этот режим и ввести в соответствующие строки Имя пользователя и пароль, выданные Вам Интернет провайдером. При вводе имени пользователя и пароля следует обязательно соблюдать регистр букв (он учитывается при проверке вашей учетной записи).



Параметр	Описание
User Name	Введите имя пользователя предоставленное Вам провайдером
Password	Введите пароль предоставленный Вам провайдером
Service Name	Поле **Service Name** является опциональным. Необходимость его заполнения уточните у провайдера. Если Вам ничего не известно о необходимости заполнения этого поля, то просто оставьте его пустым.
MTU (Размер Пакета)	Поле **MTU** является опциональным. Оно определяет максимальный размер пакета который может быть отправлен в сеть Интернет. Если Вы не знаете этих настроек, то установленное значение изменять не надо. Смотрите описание в Глоссарии
Connection Type (Тип подключения)	Если выбрать **Continuous**: Ваш роутер будет постоянно подключен к сети Интернет. При разрыве подключения он автоматически переподключится к PPPoE Серверу провайдера.
	Если выбрать **Connect On Demand**: Ваш роутер будет автоматически подключаться к PPPoE серверу провайдера при детектировании сетевой активности пользователей в сегменте LAN (обращении к внешним ресурсам). Подключение будет разорвано, если пауза в сетевой активности превысит значение, введенное в поле **Idle Time**. При возобновлении сетевой активности роутер опять автоматически переподключится к PPPoE Серверу провайдера.
	Если выбрать **Manual**: роутер подключится к PPPoE серверу провайдера только после нажатия кнопки **Connect**. Подключение будет разорвано, если пауза в сетевой активности превысит значение, введенное в поле **Idle Time**. При возобновлении сетевой активности роутер не подключится к PPPoE Серверу провайдера, а будет ожидать нажатия кнопки **Connect**.
Idle Time* (в минутах)	определяет максимальное время задержки на отключения от сети Интернет при отсутствии активности подключения. По истечении этого времени произойдет автоматическое отключение от PPPoE сервера.
TTL	Функция определения времени жизни пакетов. Включение функции добавляет 1 к времени жизни пакета при прохождении его из локальной сети через роутер (можно посмотреть командой Ping). По умолчанию – **Выключено**.

*** Внимание!: С некоторыми Интернет провайдерами, программами и активным сетевым оборудованием функция Idle Time может работать некорректно. Например: даже когда вы не используете Интернет, некоторые программы могут самостоятельно посылать пакеты, что приведёт к постоянному обнулению счетчика и отключение никогда не произойдет.**

*Нажмите кнопку **OK**, после завершения настройки. Роутер сохранит изменения и откроет окно: **Save Setting Successfully**. Нажмите кнопку **Apply** для перезагрузки роутера и активации сделанных изменений. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет. Для тонкой настройки роутера обратитесь к разделам 4–7.*

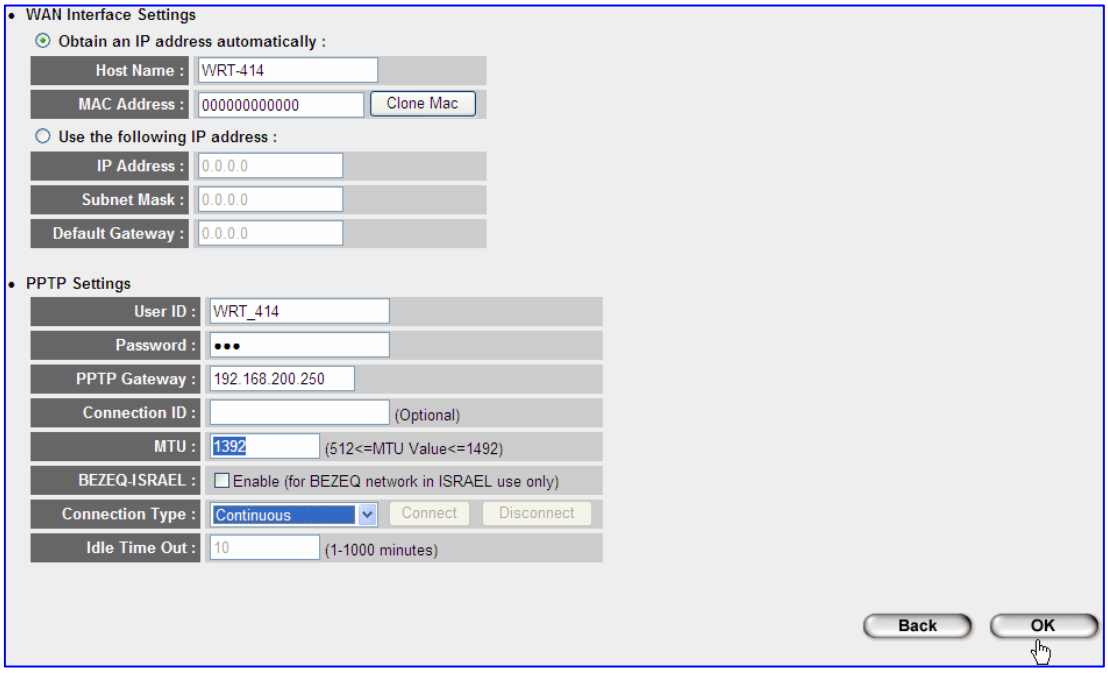
Внимание!: Для правильной работы Интернет Браузера и других приложений на компьютерах и других хостах в локальной сети, использующих Доменные Имена, не забудьте указать в меню **DNS (раздел 4.2.7)** IP адреса первичного и вторичного **DNS** сервера.

3.4 PPTP (xDSL)

Протокол PPTP - позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например Интернет. Для подключения PPTP необходимо знать IP-адрес сервера для соединения, имя пользователя и пароль. Протокол PPTP маршрутизатор использует для подключения к PPTP Серверу Провайдера, через который пользователю предоставляется доступ к ресурсам сети Интернет. Подробности по настройке подключения уточните у своего Интернет провайдера.

Типовые вопросы и проблемы при использовании PPTP подключения:

Недоступны локальные ресурсы Провайдера при использовании PPTP. Если Вы используете тип подключения PPTP, то ресурсы локальной сети провайдера будут Вам недоступны, так как этот тип подключения строится на основе туннеля и все пакеты из Вашей локальной сети (LAN порты маршрутизатора) будут направлены непосредственно на PPTP сервер. В отличие от ОС Windows, которая позволяет настроить обычное подключение для сетевой карты (статический или динамический IP адрес), и как отдельное подключение создать PPTP туннель этот маршрутизатор не умеет создавать двух независимых подключений через одни WAN порт (для прошивок версий до 3.22).
В качестве альтернативного варианта можно настроить WAN порт роутера на режим статического или динамического IP адреса, а PPTP сессию настроить на компьютере. Ограничения для подобного варианта: нельзя поднять несколько PPTP сессий с разных компьютеров подключенных к портам LAN роутера и как следствие, только один хост (компьютер или другое активное сетевое устройство) могут быть подключены к сети Интернет.
Вариант два: настройте и сохраните две конфигурации (для Static или Dynamic IP и для PPTP). При необходимости загрузите в маршрутизатор нужную конфигурацию. Этот способ позволит использовать подключение PPTP для всех хостов подключенных к портам LAN маршрутизатора и одновременно (загрузив другую конфигурацию) получать доступ к ресурсам локальной сети провайдера.
При настроенном на роутере подключении PPTP невозможно с локального компьютера настроить подключение к другому удаленному серверу PPTP. К сожалению, это ограничение на роутере обойти нельзя.



Параметр	Описание
Obtain an IP address	Провайдер выдает Вам IP адрес и другие параметры сетевого окружения автоматически, для соединения с PPTP сервером.
Use the following IP address	Вы должны ввести IP адрес и другие параметры сетевого окружения самостоятельно, для соединения с PPTP сервером.
IP Address	Статический IP адрес, выделенный Вам Интернет провайдером, для подключения к PPTP серверу.
Subnet Mask	Маска подсети, используемая Интернет провайдером (например, 255.255.0.0)
Gateway	Шлюз по умолчанию (Интернет провайдера)
User ID	Введите имя пользователя предоставленное Вам провайдером
Password	Введите пароль предоставленный Вам провайдером
PPTP Gateway	Если в вашей локальной сети есть PPTP шлюз, то здесь необходимо ввести его IP адрес. Во всех остальных случаях тут необходимо указать IP адрес PPTP шлюза Вашего Интернет Провайдера.

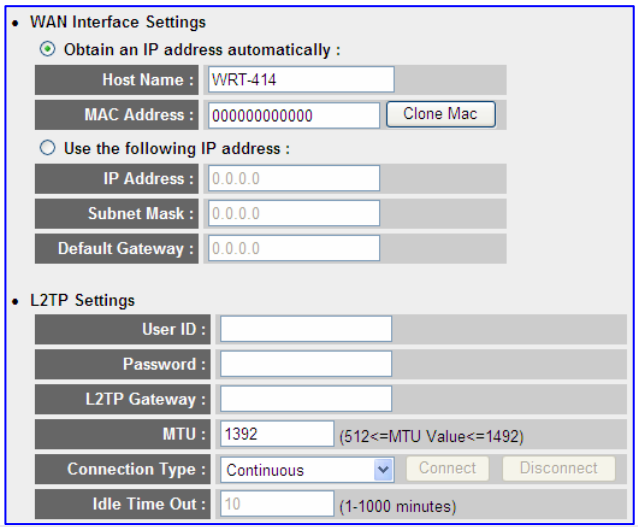
Параметр	Описание
Connection ID	Это Идентификатор выданный Провайдером. Данная настройка является дополнительной и обычно не используется.
BEZEQ-ISRAEL	Данная настройка является дополнительной и используется провайдерами BEZEQ в Израиле.
Connection Type (Тип подключения)	Если выбрать **Continuous**: Ваш роутер будет постоянно подключен к сети Интернет. При разрыве подключения он автоматически переподключится к PPPoE Серверу провайдера.
	Если выбрать **Connect On Demand**: Ваш роутер будет автоматически подключаться к PPPoE серверу провайдера при детектировании сетевой активности пользователей в сегменте LAN (обращении к внешним ресурсам). Подключение будет разорвано, если пауза в сетевой активности превысит значение, введенное в поле **Idle Time**. При возобновлении сетевой активности роутер опять автоматически переподключится к PPPoE Серверу провайдера.
	Если выбрать **Manual**: роутер подключится к PPPoE серверу провайдера только после нажатия кнопки **Connect**. Подключение будет разорвано, если пауза в сетевой активности превысит значение, введенное в поле **Idle Time**. При возобновлении сетевой активности роутер не подключится к PPPoE Серверу провайдера, а будет ожидать нажатия кнопки **Connect**.
Idle Time* (в минутах)	определяет максимальное время задержки на отключения от сети Интернет при отсутствии активности подключения. По истечении этого времени произойдет автоматическое отключение от PPPoE сервера.

*** Внимание!: С некоторыми Интернет провайдерами, программами и активным сетевым оборудованием функция Idle Time может работать некорректно. Например: даже когда вы не используете Интернет, некоторые программы могут самостоятельно посылать пакеты, что приведёт к постоянному обнулению счетчика и отключение никогда не произойдет.**

*Нажмите кнопку **OK**, после завершения настройки. Роутер сохранит изменения и откроет окно: **Save Setting Successfully**. Нажмите кнопку **Apply** для перезагрузки роутера и активации сделанных изменений. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет. Для тонкой настройки роутера обратитесь к разделам 4–7.*

3.5 L2TP (xDSL)

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section.



Параметр	Описание
Obtain an IP address	Провайдер выдает Вам IP адрес и другие параметры сетевого окружения автоматически, для соединения с L2TP сервером.
Use the following IP address	Вы должны ввести IP адрес и другие параметры сетевого окружения самостоятельно, для соединения с L2TP сервером.
IP Address	Статический IP адрес, выделенный Вам Интернет провайдером, для подключения к L2TP серверу.
Subnet Mask	Маска подсети, используемая Интернет провайдером (например, 255.255.0.0)
Gateway	Шлюз по умолчанию (Интернет провайдера)
User ID	Введите имя пользователя предоставленное Вам провайдером
Password	Введите пароль предоставленный Вам провайдером
L2TP Gateway	Если в вашей локальной сети есть L2TP шлюз, то здесь необходимо ввести его IP адрес. Во всех остальных случаях тут необходимо указать IP адрес L2TP шлюза Вашего Интернет Провайдера.
Connection Type (Тип подключения)	Если выбрать **Continuous**: Ваш роутер будет постоянно подключен к сети Интернет. При разрыве подключения он автоматически переподключится к PPPoE Серверу провайдера.

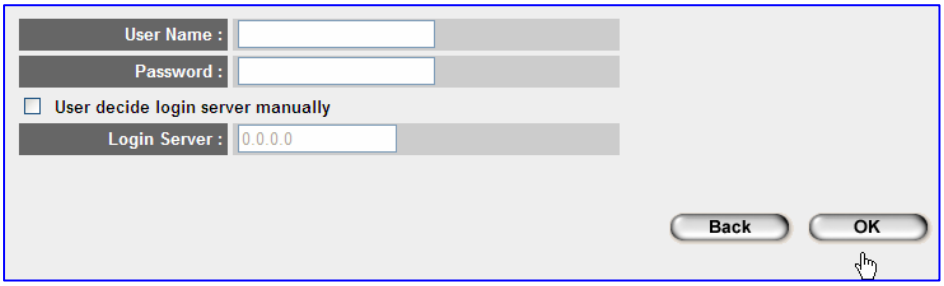
Параметр	Описание
	Если выбрать **Connect On Demand**: Ваш роутер будет автоматически подключаться к PPPoE серверу провайдера при детектировании сетевой активности пользователей в сегменте LAN (обращении к внешним ресурсам). Подключение будет разорвано, если пауза в сетевой активности превысит значение, введенное в поле **Idle Time**. При возобновлении сетевой активности роутер опять автоматически переподключится к PPPoE Серверу провайдера.
	Если выбрать **Manual**: роутер подключится к PPPoE серверу провайдера только после нажатия кнопки **Connect**. Подключение будет разорвано, если пауза в сетевой активности превысит значение, введенное в поле **Idle Time**. При возобновлении сетевой активности роутер не подключится к PPPoE Серверу провайдера, а будет ожидать нажатия кнопки **Connect**.
Idle Time* (в минутах)	определяет максимальное время задержки на отключения от сети Интернет при отсутствии активности подключения. По истечении этого времени произойдет автоматическое отключение от PPPoE сервера.

*** Внимание!: С некоторыми Интернет провайдерами, программами и активным сетевым оборудованием функция Idle Time может работать некорректно. Например: даже когда вы не используете Интернет, некоторые программы могут самостоятельно посылать пакеты, что приведёт к постоянному обнулению счетчика и отключение никогда не произойдет.**

*Нажмите кнопку **OK**, после завершения настройки. Роутер сохранит изменения и откроет окно: **Save Setting Successfully**. Нажмите кнопку **Apply** для перезагрузки роутера и активации сделанных изменений. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет. Для тонкой настройки роутера обратитесь к разделам 4–7.*

3.6 Telstra Big Pond

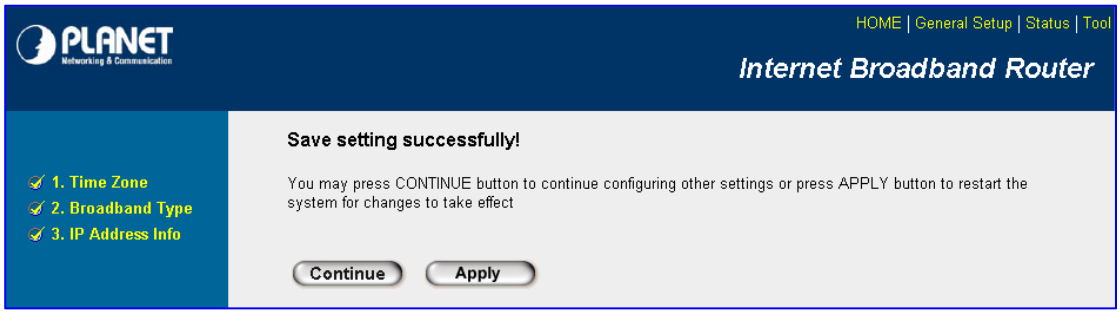
Select Telstra Big Pond if you are live in Australia and your ISP requires this protocol to connect to the Internet. Your ISP should provide all the information required in this section.



Parameters	Description
User Name	Enter the User Name provided by your ISP for the connection.
Password	Enter the Password provided by your ISP for the connection.
User Decide login server manually	If you ISP has provide the login server IP address to you, please check this box and enter the Login Server IP address below.
Login Server	Please enter the Login Server IP address here.

*Нажмите кнопку **OK**, после завершения настройки. Роутер сохранит изменения и откроет окно: **Save Setting Successfully**. Нажмите кнопку **Apply** для перезагрузки роутера и активации сделанных изменений. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет. Для тонкой настройки роутера обратитесь к разделам 4–7.*

3.7 Save Settings Successfully (Сохранение и активация настроек)



Если Вы нажали кнопку **OK**, после завершения настройки типа подключения, то увидите это окно. Нажмите кнопку **Continue** для выполнения других настроек или **Apply** для перезагрузки роутера и активации сделанных изменений. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет. Для тонкой настройки роутера обратитесь к разделам 4–7.

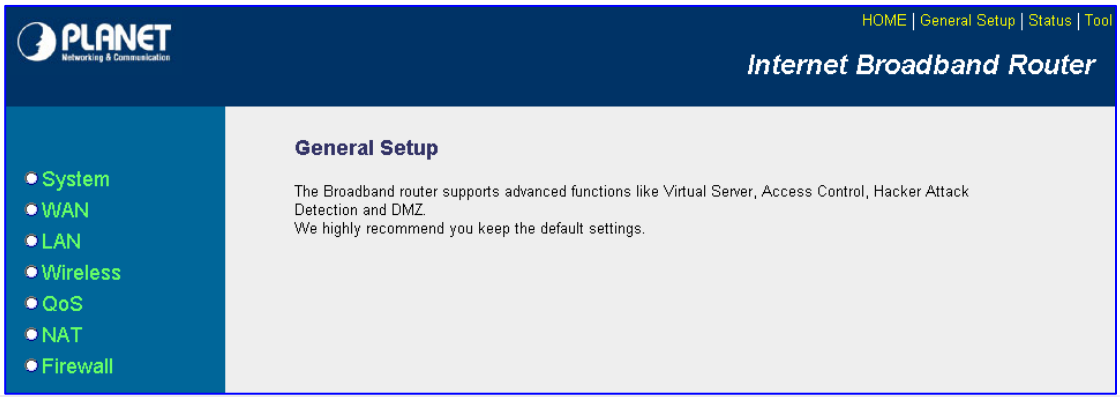
Вы будете видеть это окно каждый раз при изменении любых настроек оборудования. Для активации изменений необходимо нажать **Apply**.

Раздел 4 Основные Настройки

Нажмите кнопку **General Setup,** и откроется страница, показанная на скриншоте.

Если вы до этого воспользовались меню **Quick Setup Wizard** то вам, скорее всего, не потребуется выполнять никаких дополнительных настроек в меню General Setup чтобы начать использовать Интернет. Единственной необходимой настройкой может оказаться меню **WAN ⇨ DNS**, чтобы указать IP адрес дополнительного DNS сервера, а также меню **System ⇨ Password Settings** (пароль 1234 используемый в роутере по умолчанию желательно изменить на другой, особенно если вы хотите разрешить удалённое управление роутером). Все остальные настройки можно оставить по умолчанию, если вы не используете какие-либо специфические сервисы и протоколы.

Раздел меню General Setup содержит расширенные настройки позволяющие настроить Ваш Широкополосный Маршрутизатор в соответствии с Вашими потребностями: Трансляция адресов, Проброс портов, Виртуальный Сервер, Контроль доступа, Защита от атак Хакеров, Специальные Приложения, Демилитаризованная зона (DMZ) и другие функции.

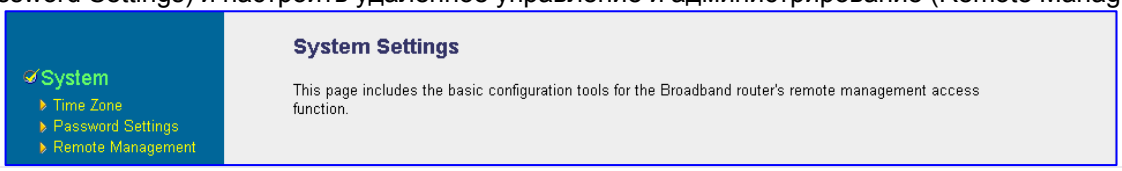


Раздел меню	Описание
4.1 System	В этом меню можно настроить Параметры Сервера Времени (Time Zone), Изменить пароль (Password Settings) и настроить удаленное управление и администрирование (Remote Management).
4.2 WAN	В этом меню можно настроить тип подключения WAN порта в соответствии с требованиями Интернет провайдера (аналогично меню Quick Setup Wizard) и выполнить настройку DNS и DDNS
4.3 LAN	Этот раздел меню позволит изменить настройку IP адреса маршрутизатора (LAN) и класса подсети используемого при подключении к портам LAN локальными хостами в качестве шлюза по умолчанию, а также изменить настройки встроенного в маршрутизатор DHCP сервера.
4.4 Wireless	Включение или выключение встроенной беспроводной точки доступа и настройка её параметров (режимы работы, шифрование, настройки защиты и контроль доступа)
4.5 QoS	**(Quality of Service - гарантированное качество услуг):** в применении к данной модели маршрутизатора термин обозначает, что данные для которых назначен класс обслуживания будут передаваться максимально быстро и стабильно в соответствии с выделенной для них максимальной или гарантированной полосой пропускной способности. Эта функция позволяет зарезервировать для определенных видов входящего и исходящего трафика заданную полосу пропускания с привязкой к диапазонам IP адресов и видам трафика. При настройке следует учитывать максимальную пропускную способность Вашего канала и очерёдность выставления правил (максимальный приоритет имеет первое правило).
4.6 NAT	Здесь можно настроить Проброс портов (Port Forvarding), Виртуальный Сервер (Virtual Server) и настройку роутера для работы со специальными приложениями и сервисами (Special Applications functions, ALG Setting). Также в этом меню можно отключить трансляцию сетевых адресов (NAT). В этом случае Вам станет доступно меню для организации статических маршрутов (Static Route), а остальные меню будут недоступны.
4.7 Firewall	Меню Межсетевого Экрана (Firewall) позволяет настроить Контроль доступа (Access Control), функцию блокировки URL или содержимого (URL Blocking), детектирование атак хакеров (DoS) и демилитаризованную зону (DMZ).

Выберите нужный пункт меню и перейдите к его подробному описанию

4.1 Меню System

В этом меню можно настроить Параметры Сервера Времени (Time Zone), Изменить пароль (Password Settings) и настроить удаленное управление и администрирование (Remote Management).

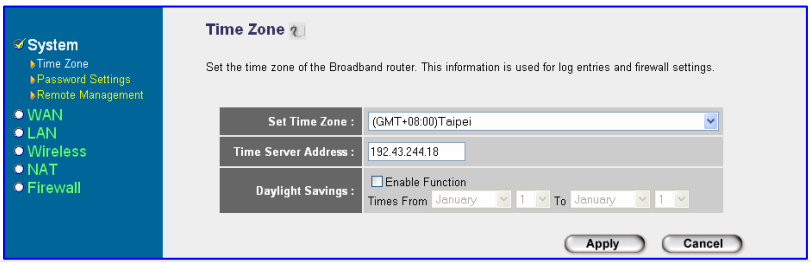


Раздел меню	Описание
3.1.1 **Time Zone** (временная зона)	В этом меню необходимо выбрать и настроить временную зону в соответствии с вашим часовым поясом. Например, для Москвы это +3.
3.1.2 **Password Settings** (Изменение пароля)	Этот раздел меню позволяет изменить пароль, используемый в роутере по умолчанию для доступа к WEB интерфейсу управления. В целях безопасности Вашей сети рекомендуется изменить пароль, особенно если вы хотите разрешить удалённое управление роутером. Если Вы забудете пароль, то получить доступ к WEB интерфейсу роутера можно будет, только сбросив все настройки кнопкой **RESET**.
3.1.3 **Remote Management** (Удаленное управление)	Этот раздел меню позволяет разрешить удаленное управление и администрирование маршрутизатором со стороны WAN порта (то есть из сети Интернет) и настроить дополнительные параметры.

Выберите нужный пункт меню и перейдите к его подробному описанию

4.1.1 Временные зоны (Time Zone)

В этом меню можно настроить временную зону в соответствии с вашим часовым поясом. Например, для Москвы это +3.

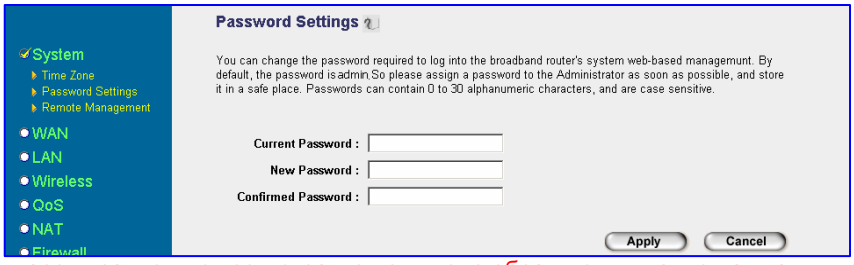


Параметр	Описание
Set Time Zone	Выбор часового пояса.
Time Server Address	IP адрес сервера времени. Измените этот IP адрес, если указанный по умолчанию не работает. По умолчанию настроено обновление времени с сервера http://www.ntp.org
Enable Daylight Savings	Роутер умеет учитывать переход на летнее время и обратно. Если Вы хотите использовать эту функцию, то поставьте галочку и настройте даты перехода на летнее время и обратно в двух следующих строках меню.
Start Daylight Savings Time	Начало периода "Летнее Время"
End Daylight Savings Time	Конец периода "Летнее Время"

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет.*

4.1.2 Изменение пароля (Password Setup)

Этот раздел меню позволяет изменить пароль, используемый в роутере по умолчанию для доступа к WEB интерфейсу управления. В целях безопасности Вашей сети рекомендуется изменить пароль, особенно если вы хотите разрешить удалённое управление роутером. Если Вы забудете пароль, то получить доступ к WEB интерфейсу роутера можно будет, только сбросив все настройки кнопкой **RESET**. Поэтому обязательно запишите и сохраните введенный пароль в безопасном месте. Пароль может содержать 0 до 30 алфавитно-цифровых символов латинского алфавита (нельзя использовать спецсимволы и символы кириллицы) в верхнем или нижнем регистре (большие или маленькие буквы).



Поскольку пароль зависим от регистра, то при вводе обратите внимание на клавишу **Caps Lock**.

Параметр	Описание
Current Password	Введите старый пароль
Внимание!: Пароль по умолчанию **admin**	
New Password	Введите новый пароль
Confirmed Password	Повторите ввод нового пароля (пароли в полях New Password и Confirmed Password должны совпадать).

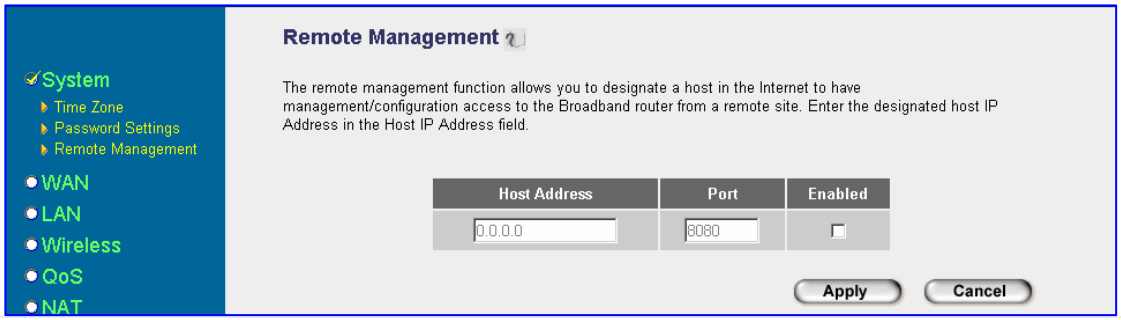
Внимание!: Если Вы забудете пароль, то получить доступ к WEB интерфейсу роутера можно будет, только сбросив все настройки кнопкой **RESET**. (кнопка расположена на задней стенке маршрутизатора).

Полный сброс настроек – если вы забыли настройки (Имя пользователя и пароль) или имеются проблемы с работой оборудования, и вы не можете найти причину, то нажмите и удерживайте кнопку **reset** больше 5 секунд. Отпустите кнопку и дождитесь перезагрузки роутера. Все настройки будут сброшены (включая IP адрес, Имя пользователя и пароль) на значения по умолчанию.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет.*

4.1.3 Удаленное администрирование (Remote Management)

Этот раздел меню позволяет разрешить удаленное управление и администрирование маршрутизатором со стороны WAN порта (то есть из сети Интернет) и настроить дополнительные параметры.

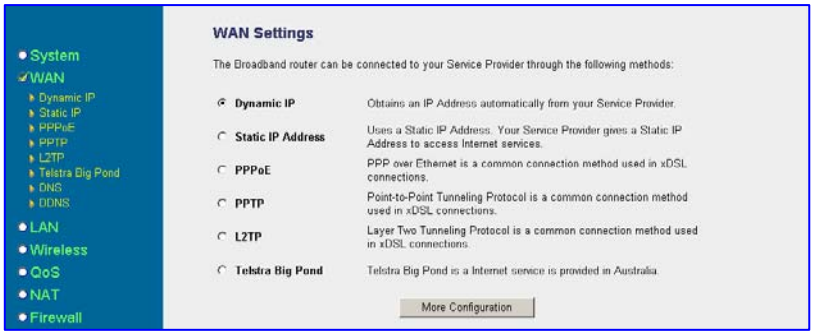


Параметр	Описание
Enabled	Поставьте галочку в окошке **Enabled,** чтобы активизировать функцию удаленного администрирования.
Host Address	Определённый IP адрес, с которого будет разрешено удаленное администрирование и управление маршрутизатором. То есть подключиться к WEB интерфейсу роутера удаленно можно будет только с указанного в настройках IP адреса. Если ввести **0.0.0.0**, то подключиться к WEB интерфейсу роутера можно будет с любого адреса при условии что удаленной стороне известны порт и пароль.
Внимание!: Чтобы подключиться к WEB интерфейсу маршрутизатора со стороны WAN порта необходимо ввести WAN IP адрес (например, 10.0.0.1) в адресной строке WEB браузера и через двоеточие номер порта (например, 8080) http://10.0.0.1:8080 (пример команды). После этого необходимо будет ввести Имя пользователя и пароль, которые используются на маршрутизаторе.	
Port	Номер порта для удаленного администрирования.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет.*

4.2 Подключение к Интернет (WAN)

В этом разделе меню вы можете настроить параметры сетевого окружения WAN интерфейса для подключения к Интернет. Для этого необходимо обратиться к настройкам, выданным Вам Интернет провайдером. Также здесь настраиваются дополнительные DNS сервера и сервер Динамических Доменных Имен (DDNS).



Раздел меню	Описание
4.2.1 Dynamic IP	Интернет провайдер автоматически назначает IP адрес (ражим DHCP клиент)
4.2.2 Static IP address	Интернет провайдер выдал Вам статический IP адрес
4.2.3 PPPoE	Интернет провайдер осуществляет подключение по протоколу Point-to-Point Protocol over Ethernet (PPPoE).
4.2.4 PPTP	Интернет провайдер осуществляет подключение по протоколу Point-to-Point Tunneling Protocol (PPTP).
4.2.5 L2TP	Интернет провайдер осуществляет подключение по протоколу L2TP
4.2.6 Telstra Big Pond	Интернет провайдер осуществляет подключение по протоколу Telstra Big Pond
4.2.7 DNS	Меню дополнительной настройки Сервера Доменных Имен (DNS)
4.2.8 DDNS	Меню настройки Сервера Динамических Доменных Имен (DDNS)

Для перехода в нужный раздел меню выберите нужный пункт в левой колонке WEB интерфейса роутера, нажав на нем левую кнопку мышки, или поставьте точку напротив нужного пункта в основном окне WEB интерфейса и нажмите кнопку ***More Configuration***

4.2.1 Режим DHCP клиент (Dynamic IP)

В режиме **DHCP клиент** роутер получает IP адрес и все необходимые дополнительные параметры сетевого окружения от DHCP сервера Интернет провайдера.
Смотрите **Раздел 3.1 “Кабельный Модем”** для более детальной информации.

4.2.2 Статический IP Адрес (Static IP Address)

Если для подключения к Интернет провайдер Выдал Вам статический IP адрес, то необходимо выбрать тип подключения Fixed-IP xDSL. Введите параметры сетевых настроек в соответствующие строки и нажмите OK.
Смотрите **Раздел 3.2 “Фиксированный IP Адрес”** для более детальной информации.

4.2.3 PPPoE (PPP over Ethernet)

Обычно этот режим используется при широкополосном подключении через ADSL модем. Также его используют некоторые провайдеры кабельных сетей. Этот режим позволяет автоматически получить все необходимые настройки подключения от PPPoE сервера, используя выданные провайдером имя пользователя и пароль. Для настройки этого типа подключения нужно включить этот режим и ввести в соответствующие строки Имя пользователя и пароль, выданные Вам Интернет провайдером. При вводе имени пользователя и пароля следует обязательно соблюдать регистр букв (он учитывается при проверке вашей учетной записи).
Смотрите **Раздел 3.3 “PPPoE”** для более детальной информации.

4.2.4 PPTP

Протокол PPTP - позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например Интернет. Для подключения PPTP необходимо знать IP-адрес сервера для соединения, имя пользователя и пароль. Протокол PPTP маршрутизатор использует для подключения к PPTP Серверу Провайдера, через который пользователю предоставляется доступ к ресурсам сети Интернет. Подробности по настройке подключения уточните у своего Интернет провайдера.
Смотрите **Раздел 3.4 “PPTP”** для более детальной информации.

Также роутер может выполнять подключение по протоколам L2TP и Telstra Big Point. Эти разделы частично оставлены без перевода и комментариев потому, что Российские провайдеры не используют эти типы подключения.

4.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to section 4.2.5 for more settings of this option.

4.2.6 Telstra Big Pond

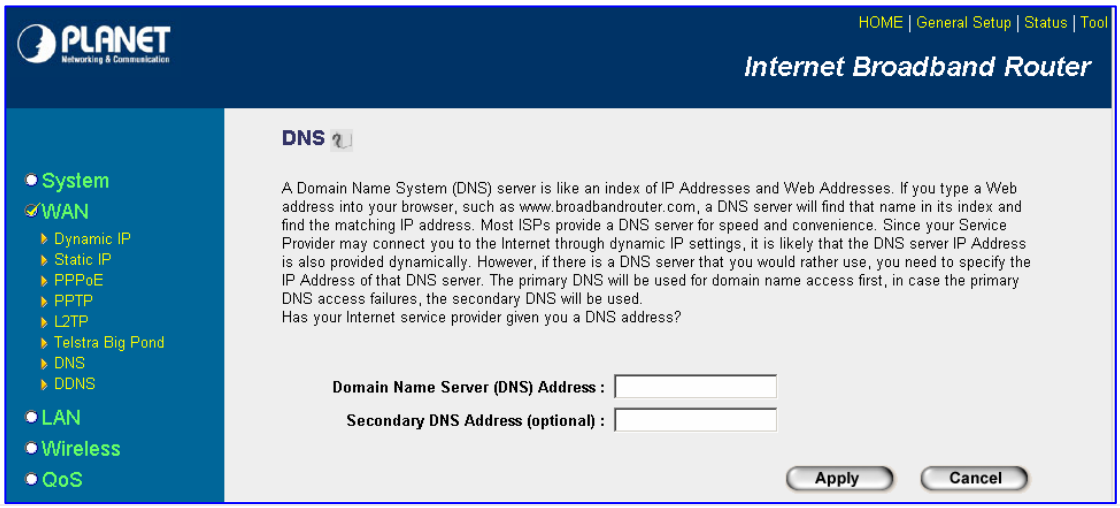
Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Telstra Big Pond protocol is used by the ISP in Australia. Your ISP should provide all the information required in this section. Please refer to section 4.2.6 for more settings of this option.

4.2.7 DNS

Нормальную работу большинства системных служб обеспечивает сервер DNS, который способен преобразовывать имя хоста в IP адрес. Это распределенная иерархическая база данных, содержащая информацию об именах серверов Интернета и позволяющая по имени системы определить ее IP адрес. Иерархическая организация DNS наглядно проявляется в структуре доменного адреса. Каждый из разделенных точками компонентов адреса соответствует домену (или зоне), где за поддержание порядка несет ответственность та или иная организация. Первым (справа) идет так называемый домен верхнего уровня, например .ru или .corn. За созданием и работой доменов верхнего уровня следит международная некоммерческая организация ICANN (www.icann.org). Домены верхнего уровня существуют практически для всех признанных ООН государств и территорий. Все они состоят из двух букв, а их поддержкой в каждой стране по поручению ICANN занимается специальная организация. В России такой организацией является РосНИИРОС. Кроме доменов для стран, существует ряд глобальных доменов верхнего уровня, а также может использоваться локальный домен организации или предприятия. Использование DNS позволяет обеспечить удобное обращение к нужным хостам в локальной сети или в сети Интернет и обеспечить быстрый поиск необходимого хоста или сервера. Если есть DNS сервер, который Вы предпочитаете использовать, то в этом меню следует указать его IP адрес.

Если Вы используете тип подключения **Static IP** (IP адрес WAN порта настроенный вручную), то следует обязательно указать IP адрес DNS сервера для правильной работы вашего подключения к Интернет.

В случае неполадок на основном DNS сервере (сервер не отвечает) система может автоматически перенаправить запрос резервному DNS серверу. Для этого следует указать IP адрес другого DNS сервера в строке **Secondary DNS Address.**

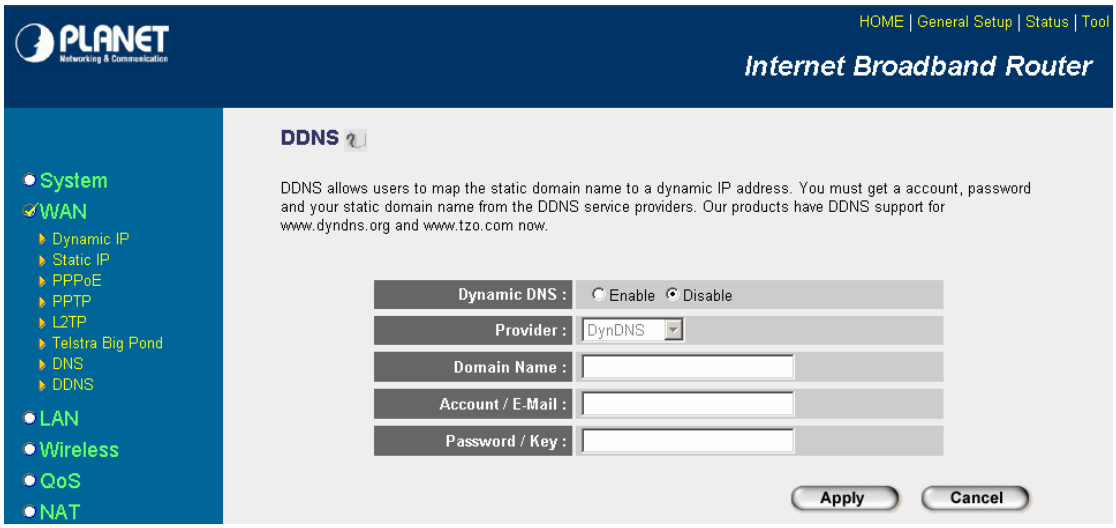


Параметр	Описание
Domain Name Server (DNS) Server	IP адрес Сервера Доменных Имен (DNS server) выданный Вам Интернет Провайдером или специфический IP адрес Вашего DNS сервера.
Secondary DNS Address (optional)	IP адрес резервного Сервера Доменных Имен (DNS server) выданный Вам Интернет Провайдером или специфический IP адрес Вашего резервного DNS сервера.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.2.8 DDNS

Сервер Динамических Доменных Имен (DDNS) (требует регистрации на одном из сайтов поддерживаемых маршрутизатором и обеспечивающих службу DDNS) позволит Вам использовать псевдоним, который сопоставляет Ваш динамический IP адрес к статическому Имени Хоста, позволяя Вам обращаться к оборудованию из сети Интернет по Доменному Имени присвоенному Вашему хосту. Обычно используется, когда Интернет Провайдер выделил Вам реальный динамический IP адрес. Когда эта функция используется, адрес IP на Сервере Dynamic DNS будет автоматически сопоставлен с Вашим текущим динамическим IP адресом, выданным в данный момент времени провайдером и эта информация будет периодически обновляться.

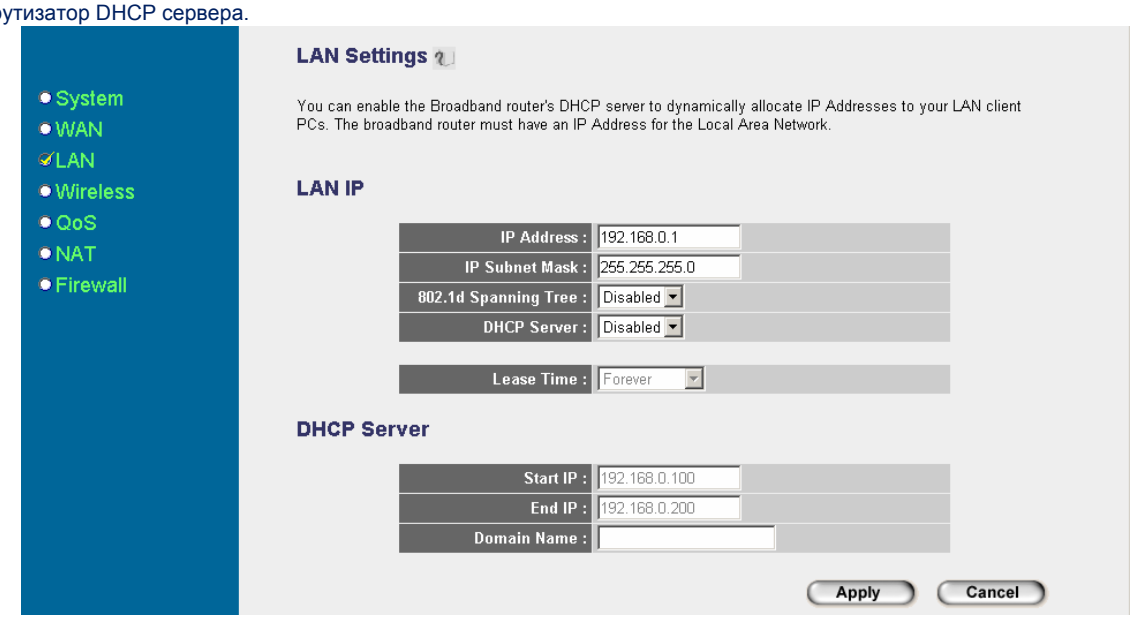


Параметр	Описание
Enable/Disable	Включить или Выключить функцию DDNS у маршрутизатора
Provider	Выбор службы DDNS
Domain name	Ваше постоянное Доменное Имя присвоенное Вам на сайте Службы DDNS
Account/E-mail	Имя Вашей учетной записи или адрес электронной почты по которому Вы зарегистрированы на сайте Службы DDNS (зависит от выбранного поставщика Службы DDNS)
Password/Key	Пароль, выданный Вам поставщиком службы DDNS

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.3 Локальная сеть (LAN)

Этот раздел меню позволит изменить настройку IP адреса маршрутизатора (LAN) и класса подсети используемого при подключении к портам LAN локальными хостами в качестве шлюза по умолчанию, а также изменить настройки встроенного в маршрутизатор DHCP сервера.



Параметр	По умолчанию	Описание
LAN IP		
IP address	192.168.0.1	IP адрес LAN порта маршрутизатора (Для пользователей локальной сети он является **Шлюзом по Умолчанию**)
IP Subnet Mask	255.255.255.0	Специфическая маска для вашей локальной сети
802.1d Spanning Tree	Disabled	Если 802.1d функция Spanning Tree включена, то маршрутизатор будет использовать протокол Spanning Tree, который позволяет избежать зацикливания сетевых пакетов в сегменте LAN.
DHCP Server	Enabled	Включить или отключить DHCP Сервер. Встроенный DHCP сервер может присваивать IP адреса и раздавать всем хостам в Вашей локальной сети параметры сетевого окружения (маска подсети, шлюз по умолчанию, DNS сервер). Чтобы включить DHCP сервер необходимо в строке **DHCP server** выбрать **enablad** и нажать **allpy**. **End IP** – конечный IP адрес выдаваемый DHCP сервером в аренду **Domain Name** – Имя домена. В большинстве случаев это поле можно оставитиь путым.
Lease Time		Время жизни зарезервированного IP адреса (выданного в аренду). Если в течении этого времени хост вновь не станет активным, то IP адрес будет освобожден и может быть назначен другому хосту в Вашей локальной сети.
Start IP	начальный IP адрес выдаваемый DHCP сервером в аренду	
End IP	конечный IP адрес выдаваемый DHCP сервером в аренду	
Domain Name	Доменное Имя для Вашей локальной сети. В большинстве случаев это поле можно оставитиь путым.	
Вы можете задать произвольное количество IP адресов автоматически раздаваемых DHCP сервером в аренду изменяя диапазон Start IP и End IP		
Внимание!: По умолчанию Диапазон IP адресов Выдаваемых в аренду выглядит так: начальный IP **192.168.0.100** и до конечного IP **192.168.0.200**. Если Вам необходимо настроить хост в локальной сети со статическими параметрами сетевого окружения, то следует использовать диапазон адресов неиспользуемый DHCP сервером и не занятый каким либо другим хостом. Если не соблюдать это простое правило, то Вы рискуете получить конфликт сетевых адресов в вашей локальной сети.		

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

ВАЖНО!: Многие Интернет провайдеры предоставляют клиенту локальные IP адреса (из диапазона не маршрутизируемых в сети Интернет). К таким адресам относятся:

Сеть/ класс	Префикс	Начальный IP	Конечный IP	Broadcast	Максимально возможное число хостов	Маска
10.0.0.0 / A	**8**	**10.0.0.1**	**10.255.255.254**	**10.255.255.255**	**16777214**	**255.0.0.0**
172.16.0.0 / B	**12**	**172.16.0.1**	**172.31.255.254**	**172.31.255.255**	**1048574**	**255.240.0.0**
192.168.0.0 / C	**16**	**192.168.0.1**	**192.168.255.254**	**192.168.255.255**	**65534**	**255.255.0.0**

При настройке интерфейсов LAN и WAN обязательно убедитесь, что диапазон IP адресов в локальной сети маршрутизатора (порты LAN) и диапазоны IP адресов локальной сети провайдера (со стороны порта WAN) не пересекаются. При необходимости измените настройки LAN интерфейса, выбрав из таблицы диапазон IP адресов не используемый провайдером. Маску подсети и другие параметры можно рассчитать с помощью бесплатной программы LanCalculator (http://lantricks.com/).

4.4 Беспроводной Интерфейс (Wireless)

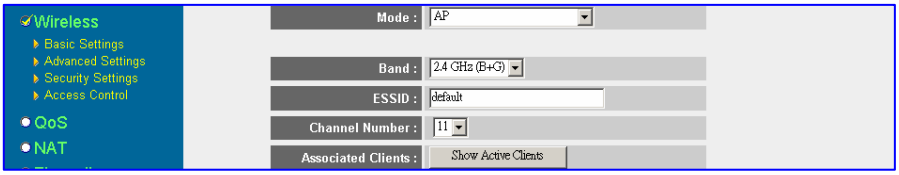
На этой странице можно включить или выключить беспроводной интерфейс маршрутизатора (по умолчанию включен).

Параметр	Описание
Enable/Disable	Включить или Выключить беспроводной интерфейс

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

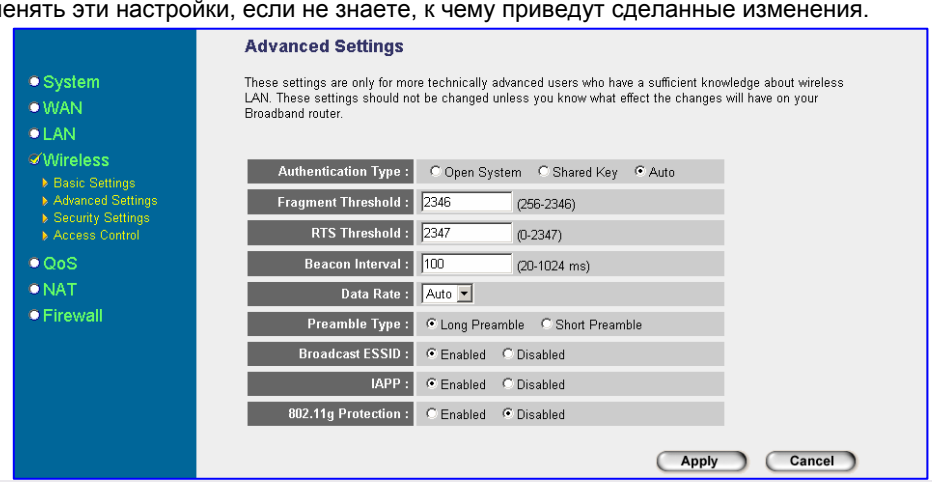
4.4.1 Основные настройки (Basic Settings)

WRT-414 может работать не только в режиме Точки доступа (Access Point), но и имитировать беспроводную сетевую карту компьютера (режимы Station-Ad Hoc и Station-Infrastructure), работать в режиме беспроводного моста (Bridge-Point to Point, Point to Multi-point) и в совмещенном режиме Bridge-WDS. Пожалуйста, обратитесь к "**Раздел 5 Настройка беспроводного подключения (Wireless Configuration)**" для получения дополнительной информации по настройке в различных режимах и их использованию. По умолчанию WRT-414 работает в режиме Точки доступа.



4.4.2 Расширенные настройки (Advance Settings)

Не следует изменять эти настройки, если не знаете, к чему приведут сделанные изменения.



Параметр	Описание
Authentication Type (Тип идентификации)	**Auto** – Автоматически **Open System** – открытая система **Shared Key** – совместно используемый ключ Если установлено "**Auto**", то все беспроводные клиенты смогут сами выбрать режим подключения ("**Open System**" или "**Shared Key**".). Если вы выберите тип идентификации Open System или Shared Key, то беспроводные клиенты смогут подключиться, только используя установленный Вами режим.
Fragment Threshold (Порог фрагментации)	Эта величина устанавливает максимальный размер беспроводных пакетов — пакеты большего размера разбиваются и передаются как отдельные фрагменты. В случае превышения указанного значения порога фрагментации пакета данных, беспроводное устройство будет разбивать пакеты на части меньшего размера перед отправкой. Значение порога фрагментации должно быть в пределах от 256 до 2346 байтов. Разбивка пакетов используется в сетях с большой нагрузкой или в условиях сильных помех в радиоэфире. Небольшое снижение порога фрагментации в сетях, работающих в таких условиях, поможет улучшить производительность. Однако снижение порога в сетях с малой нагрузкой и небольшими помехами может вызвать обратный эффект и привести к уменьшению пропускной способности сети. Поэтому в большинстве случаев рекомендуется указывать максимально возможное значение порога фрагментации.

Параметр	Описание
RTS Threshold (запрос на отправку)	**RTS - Request to Send** - это механизм, предусматривающий посылку беспроводным устройством запроса получателю на получение разрешения отправить пакет данных, превышающий установленный размер. Значение порога RTS следует выбирать в пределах от 0 до 2347 байтов. Если Вы укажете значение порога RTS равным нулю, пакеты данных будут отправляться беспроводным устройством только при условии получения подтверждения от устройства получателя. Для достижения наибольшей производительности, в настройках беспроводного устройства рекомендуется указывать максимально возможное значение порога RTS. **Режим Точки доступа**. Для обеспечения эффективной работы точек доступа, они должны быть освобождены от необходимости спрашивать разрешение у своих клиентов на отправку данных. Для точек доступа устанавливается, как правило, максимально возможное значение порога RTS.
Beacon Interval (Радиомаяк)	Точки доступа периодически подают сигналы с целью синхронизации подключенных к ним беспроводных устройств и оценки качества сигнала. Вы можете установить периодичность подачи сигнала в пределах от 20 до 1024 миллисекунд. По умолчанию используется период длиной 100 миллисекунд.
Data Rate (Скорость передачи данных)	Этот параметр позволяет настроить максимальную скорость передачи данных передачи данных. При установке Auto будет использоваться максимально возможная передачи пакетов данных. **Внимание!** Не следует путать этот параметр с реальной пропускной способностью беспроводного канала, так как это значение Data Rate устанавливает скорость канала с учётом всех служебных данных. Вполне естественно, что на практике таких значений вы никогда не получите. Реальная пропускная способность канала примерно в два раза ниже и зависит от множества факторов.
Preamble Type (Тип Заголовка)	Это параметр, который достаточно сильно влияет на скорость работы сети - он управляет размером заголовка пакетов, по которому производится коррекция CRC (циклическая проверка четности с избыточностью). Для удаленных и развитых сетей следует использовать режим **"Long preamble"(Длинный Заголовок)**, так как он обеспечит большую надежность передачи данных. **Short Preamble** (**Короткий Заголовок)** больше подходит для небольших сетей с малым количеством устройств и позволит немного повысить скорость передачи данных.
Broadcast ESSID	Рассылка широковещательного идентификатора беспроводной сети (SSID). Идентификационный код беспроводной сети - Service Set Identifier (SSID) используется для того, чтобы отличить друг от друга соседние беспроводные сети. SSID должен быть уникальным и неповторяющимся. Код SSID может включать до 30 знаков из любой комбинации заглавных и прописных букв латинского алфавита и цифр, например: **PlanetWAP415**. Код SSID должен быть одинаковым для всех устройств Вашей беспроводной сети. **Внимание!** *Настройка точек доступа предусматривает возможность отключения широковещательной рассылки идентификационного кода SSID, что делает точку доступа невидимой в эфире. Однако преимущества такого метода обеспечения безопасности сомнительны, поскольку остается возможность определения идентификатора сети в пакетах «probe response». Поэтому скрытие SSID, по большому счету, нельзя отнести к эффективным мерам защиты беспроводных сетей. Он выполняет роль именно идентификатора, который беспроводные устройства прикрепляют к заголовкам пересылаемых пакетов данных. В отличие от самих данных, которые перед отправкой по беспроводной сети могут быть зашифрованы с помощью WEP шифрования, код SSID не подвергается шифрованию и может быть перехвачен любым сетевым устройством или сканером в радиоэфире. Поэтому использование длинных и сложных кодов SSID не играет никакой роли в плане обеспечения безопасности передаваемой информации.*
IAPP	В соответствии с предварительной спецификацией стандарта IEEE 802.11f представляет собой протокол обмена служебной информацией между точками доступа (Inter-Access Point Protocol, IAPP), что необходимо для построения распределенных беспроводных сетей передачи данных. Если в Вашей беспроводной сети работает несколько точек доступа, то при включении этой функции они смогут обмениваться информацией о подключенных беспроводных клиентах, что позволит организовать роуминг в вашей беспроводной сети и прозрачно подключать клиентов при переходе в зону действия другой точки доступа. Для повышения защищенности беспроводной сети рекомендуется выключить.
802.11g Protection	Или говоря по другому, **CTS (Clear to Send)** это сигнал управления последовательным устройством, передаваемый от DCE (устройство передачи данных) к DTE (терминальное оборудование) и показывающий, что DTE может продолжать передачу данных. Включение этого режима приведет к снижению пропускной способности из за необходимости передачи большого количества дополнительной служебной информации (подтверждение для каждого фрейма). **По умолчанию:** Выключено.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.4.3 Шифрование (Security)

При проектировании и построении беспроводной сети необходимо уделить особое внимание вопросам безопасности, так как не только легко перехватить незащищенные данные, передаваемые по беспроводным каналам, но и получить полный доступ к подобному устройству и соответственно ко всем ресурсам Вашей локальной сети, в которую включено данное устройство.

Беспроводной роутер поддерживает несколько видов защиты Вашей беспроводной сети с использованием различных методов и алгоритмов шифрования и идентификации (WEP, 802.1x, 802.1x с WEP, WPA-PSK и WPA RADIUS). Использование того или иного вида шифрования позволит значительно снизить риск перехвата информации и несанкционированного подключения к

Вашей беспроводной сети. Наиболее простой и одновременно наименее защищенный протокол шифрования это WEP с длинной ключа 64 бит. Его следует использовать только в том случае, если подключаемое оборудовапние не поддерживает других алгоритмов шифрования.

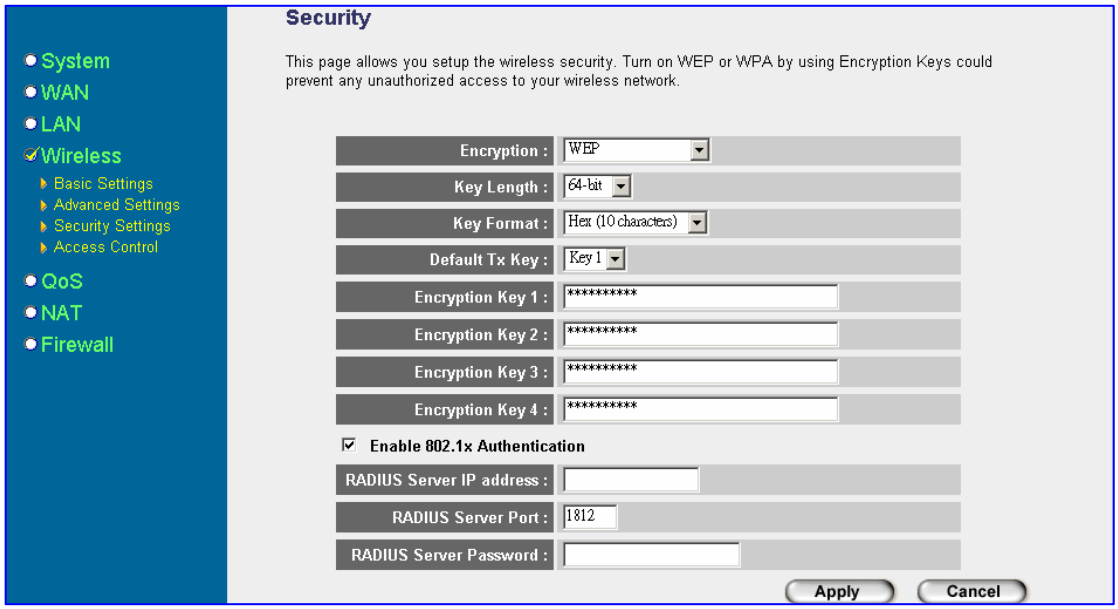
Протоколы защиты WEP (Wired Equivalent Privacy), WPA и WPA2, обеспечивают единую инфраструктуру для управления доступом, защиты и шифрования данных, пересылаемых между беспроводной точкой доступа и беспроводным клиентом. Для защиты подключения на точке доступа необходимо активизировать WEP или WPA. При возможности выбора между тремя технологиями следует исходить из принципа, что WPA2 предпочтительнее WPA, а WPA предпочтительнее WEP.
В основе протокола WPA, который пришел на смену WEP, лежит подмножество стандарта IEEE 802.11i, а WPA2 основан на окончательной редакции стандарта IEEE 802.11i. В WPA применяется несколько способов и алгоритмов, в частности TKIP (Temporal Key Integrity Protocol) и AES (Advanced Encryption Standard), для повышения надежности методов управления ключами и шифрования. Большинство современных беспроводных устройств совместимы с WPA, а в некоторых старых моделях можно обновить встроенное программное обеспечение, дополнив его функциями WPA (по этому вопросу необходимо проконсультироваться у поставщика оборудования). Но следует помнить, что выбор WPA возможен, только если точка доступа и все клиенты совместимы с WPA.
WEP и WPA шифруют данные, пересылаемые между Точкой доступа и удаленными клиентами. То есть, ключ (набор символов), известный как беспроводной Точке доступа, так и клиенту, используется для шифрования и восстановления данных, пересылаемых между этими устройствами. Взломщик, завладевший ключом, может расшифровать данные, пересылаемые между беспроводными AP и клиентом, или установить соединение с беспроводной Точкой доступа.
Существенный недостаток WEP это необходимость вручную вводить ключ, используемый для шифрования, как на беспроводной Точке, так и на клиенте.
Для устранения недостатков WEP шифрования протокол WPA дополнен функциями управления ключом. Как и в WEP, ключ здесь используется для шифрования данных. Однако он вводится один раз, а впоследствии с помощью этого ключа WPA генерирует настоящий ключ для шифрования данных. WPA периодически меняет ключ. Следовательно, в случае взлома ключа шифрования, тот будет полезен только до тех пор, пока беспроводная Точка доступа и клиент автоматически не изменят его.
Оптимальный режимом для пользователей малого или домашнего офиса является WPA Pre-Shared Key (WPA-PSK), который обеспечивает достаточно надежную защиту и прост в настройке. Для средних и крупных предприятий предпочтителен режим WPA RADIUS с обязательным сервером RADIUS (Remote Authentication Dial-In User Service или Служба Удаленной Аутентификации Пользователей по коммутируемым линиям).
Для настройки использования режима WPA-PSK нужно выбрать параметр WPA Pre-Shared Key. В точке доступа реализованы три алгоритма WPA: TKIP, AES и совмещенный. TKIP - это промежуточная мера, предназначенная для того, чтобы устранить многочисленные проблемы WEP до широкого распространения протокола следующего поколения WPA (WPA2). В TKIP используется тот же алгоритм шифрования, что и в WEP, но многие изъяны WEP устранены благодаря динамической смене ключа шифрования данных, шифрованию данных настройки, представленных обычным текстом в WEP, и проверке целостности сообщений. AES - это новый, исключительно надежный алгоритм шифрования, базируемый на стандарте 802.11i и WPA2. Однако он пока не реализован во всех аппаратных средствах и программном обеспечении. По возможности следует выбирать AES.
После выбора режима работы вводится ключ WPA Shared Key. Необходимо ввести один и тот же ключ на всех клиентах, которые устанавливают связь с точкой доступа. Следует выбирать длинный, трудно разгадываемый ключ. Длинна ключа не менее 8 символов, но не более 63 символов ASCII. Рекомендуемая длина ключа не более 20 символов. Не рекомендуется вводить ключ длиной больше 20 ASCII символов, так как длинный ключ может существенно замедлить работу маршрутизатора.
Если клиенты несовместимы с WPA, лучше использовать WEP, чем вовсе отказаться от защиты. Для настройки WEP в следует указать режим безопасности Shared Key (Меню Advanced Setting), выбрать ключ для использования в качестве стандартного ключа передачи (ключ с номером от 1 до 4) и длину WEP ключа (64 или 128) с представлением в шестнадцатеричном или ASCII-формате. Ключ следует ввести в поле Key, которое соответствует выбранному стандартному ключу передачи. Например, если выбран 64-х разрядный шестнадцатеричный ключ, то можно ввести строку из десяти шестнадцатеричных цифр. Эту конфигурацию WEP-ключа необходимо повторить во всех клиентах, поэтому следует выбирать вариант настройки, приемлемый для всех устройств.
Процедура настройки WEP шифрования может различается между продуктами разных поставщиков в большей степени, чем настройка WPA, поэтому рекомендации по WEP труднее адаптировать к конкретной ситуации.

Обратите внимание, что по умолчанию шифрование выключено! Для включения шифрования выберите необходимый режим в поле **Encryption** и выполните необходимую настройку.

4.4.3.1 WEP

Если выбрано WEP шифрование с длиной ключа 128 или 64 бита, то необходимо ввести WEP ключи, чтобы зашифровать данные. Ключ может содержать произвольные алфавитно-цифровые данные (ASCII) или шестнадцатеричные значения алфавитно-цифровых данных (HEX). Вы можете ввести четыре WEP ключа и выбрать один в качестве используемого по умолчанию. Точка доступа позволит подключиться только тем клиентам, у которых в настройках прописан аналогичный ключ шифрования.
Внимание:
Ключи шифрования, используемые беспроводными клиентами должны совпадать с ключем выбранным по умолчанию на точке доступа!
WEP шифрование можно использовать в режимах “Точки Доступа”, “Station-Ad Hoc”, “Station-Infrastructure” и “AP Bridge-WDS”.

Если Вы хотите использовать идентификацию по RADIUS (802.1x), то пожалуйста поставьте галочку в поле, " Enable 802.1x Authentication " и обратитесь к разделу 4.4.3.2 для детального ознакомления с параметрами настройки.

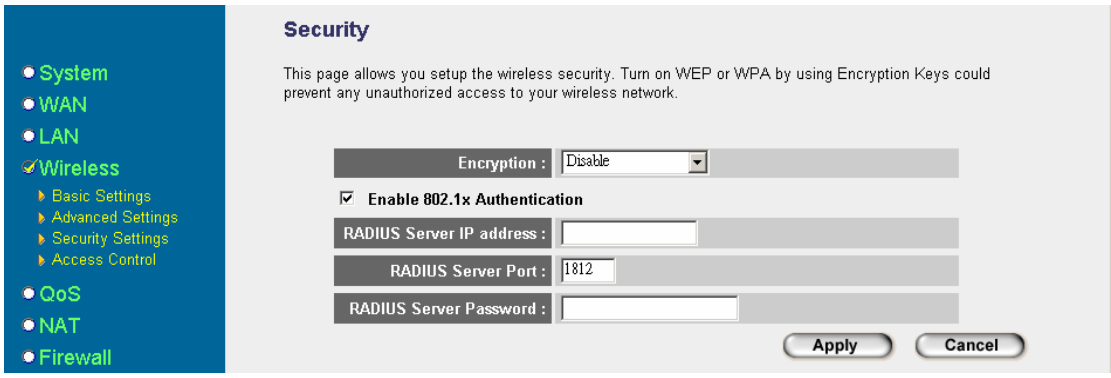


Параметр	Описание
Encryption (шифрование)	В данном случае необходимо выбрать “WEP”.
Key Length (длинна колюча)	длинна ключа 64 или 128 бит. Чем длиннее ключ, тем выше защищенность сети
Key Format (формат ключа)	Вы можете выбрать между ASCII символами (буквенно-цифровай формат) или Hex (шестнадцатеричный формат представления данных) В HEX формате вы можете использовать буквы латинского алфавита от A до F и числа от 0 до 9 для ввода ключа. Чтобы перевести значение ключа ASCII в HEX можно воспользоваться программой просмотра или редакторами умеющими показывать данные в шестнадцатеричном формате. Например, можно использовать Windows Commander. Данные введенные в HEX и аналогичный ему ключ в ASCII являются аналогами.
Default Tx Key (ключ по умолчанию)	Выберите ключ по умолчанию который будет использоваться для шифрования данных. В целях безопасности рекомендуется периодически менять используемые ключи.
Encryption Key 1 - Key 4 (ключи шифрования)	В эти поля необходимо ввести ключи, с помощью которых будет осуществляться шифрование данных 64-х битный ключ: введите 10-ти значное Hex значение (допустимые символы “A-F”, “a-f” и “0-9”) или 5 символов ASCII 128-х битный ключ: введите 26-ти значное Hex значение (допустимые символы “A-F”, “a-f” и “0-9”) или 10 символов ASCII.
Enable 802.1x Authentication	для использования идентификации по RADIUS (802.1x) пожалуйста поставьте галочку в поле, " Enable 802.1x Authentication " и обратитесь к разделу 4.4.3.2 для детального ознакомления с параметрами настройки

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.4.3.2 Идентификация по RADIUS (802.1x)

IEEE 802.1x – это протокол идентификации. Каждый пользователь должен использовать зарегистрированную на RADIUS сервере учетную запись, чтобы подключиться к Точке доступа до получения доступа к беспроводной сети (WLAN). Идентификация обрабатывается на RADIUS сервере. Этот режим позволяет с высокой надежностью подтвердить подлинность пользователя по стандарту IEEE 802.1x, но не выполняет шифрование данных передаваемый во время сеанса связи. Поэтому данный режим рекомендуется использовать совместно с WEP шифрованием.



Параметр	Описание
Encryption (шифрование)	В данном случае необходимо выбрать **Enable 802.1x Authentication**, а поле Encryptyon должно иметь значение “**Disable**”.
Enable 802.1x Authentication	Поставьте галочку в поле **Enable 802.1x Authentication**.
RADIUS Server IP Address	Введите IP адрес RADIUS Сервера
RADIUS Server Port	Введите другой номер порта для вашего Radius Сервера или оставьте принятый по умолчанию (1812)
RADIUS Server Password	Введите пароль, который настроен на Radius Сервере

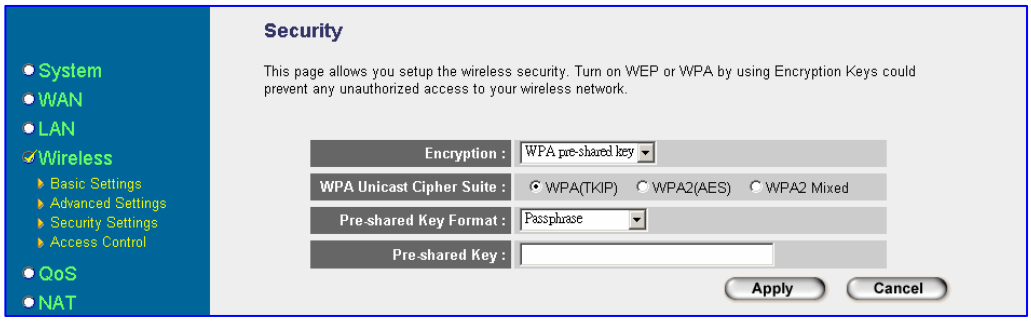
*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.4.3.3 WPA

WPA(Wi-Fi Protected Access) – это шифрование обеспечивающее значительно более высокий уровень защиты для Вашей беспроводной сети и данных,
В отличие от WEP использующего статические ключи шифрования, этот стандарт использует пароль владельца, от которого система производит постоянно изменяющиеся ключи (динамически), используя протокол TKIP. Ключи никогда не используются повторно, что значительно снижает риск того, что хакер сможет их перехватить и воспользоваться ими. WPA также включает в себя поддержку стандарта 802.1x, который позволяет системе проверять, кто подключается к сети используя центральную базу данных известных пользователей (RADIUS).

4.4.3.4 Режим WPA Pre-shared Key

Позволяет настроить подключение беспроводных клиентов без использования RADIUS сервера, на основе пароля с последующей динамической сменой ключа шифрования. Используется для организации небольших беспроводных сетей. Устойчивость к взлому выше, чем у WEP, но имеются существенные недостатки, влияющие на устойчивость к взлому. Первым недостатком WPA-PSK является то, что используется статическая парольная фраза, которая не меняется с течением времени, следовательно, её можно подобрать за какое-то конечное время. Второй недостаток это то, что контрольная фраза должна быть одинаковой у всех клиентов беспроводной сети.

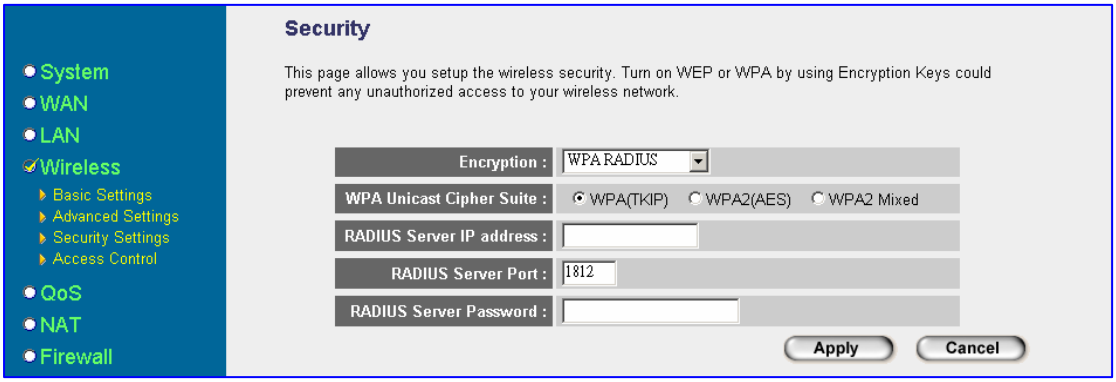


Параметр		Описание
Encryption (шифрование)		В данном случае необходимо выбрать **WPA Pre-Shared key**.
WPA Unicast Cipher Suite	WPA (TKIP)	Протокол TKIP обеспечивает динамический обмен ключами, что повышает защищенность беспроводной сети.
	WPA2 (AES)	Использует протокол CCMP. CCMP основан на методе CCM алгоритма шифрования AES. Все AES-процессы, применяемые в CCMP, используют AES с 128-битным ключом и 128-битным размером блока. Этот алгоритм обеспечивает очень высокий уровень защищенности беспроводной сети.
	WPA2 Mixed	Совмещенный режим обмена ключами с использованием алгоритмов TKIP или AES, выбираемых автоматически.
Pre-shared Key Format		Вы можете выбрать между ASCII символами (буквенно-цифровай формат) или Hex (шестнадцатеричный формат представления данных) В HEX формате вы можете использовать буквы латинского алфавита от A до F и числа от 0 до 9 для ввода ключа. Чтобы перевести значение ключа ASCII в HEX можно воспользоваться программой просмотра или редакторами умеющими показывать данные в шестнадцатеричном формате. Например, можно использовать Windows Commander. Данные введенные в HEX и аналогичный ему ключ в ASCII являются аналогами.
Pre-shared Key		В эти поля необходимо ввести ключи, с помощью которых будет осуществляться шифрование данных 64-х битное Hex значение ключа (допустимые символы “A-F”, “a-f” и “0-9”) или минимум 8 символов ASCII (не рекомендуется вводить ключ длиной больше 20 ASCII символов, так как длинный ключ может существенно замедлить работу маршрутизатора)

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.4.3.5 WPA RADIUS

802.1x обеспечивает аутентификацию удаленных клиентов и выдачу им временных ключей для шифрования данных. Ключи (в зашифрованном виде) высылаются клиенту на незначительный промежуток времени, после которого генерируется и высылается новый ключ. Алгоритм шифрования не изменился – тот же RC4, но постоянная смена ключей очень сильно затрудняет вероятность взлома. Поддержка этого протокола есть только в операционных системах (от Microsoft) Windows XP. Этот протокол требует обязательного наличия RADIUS-сервера.

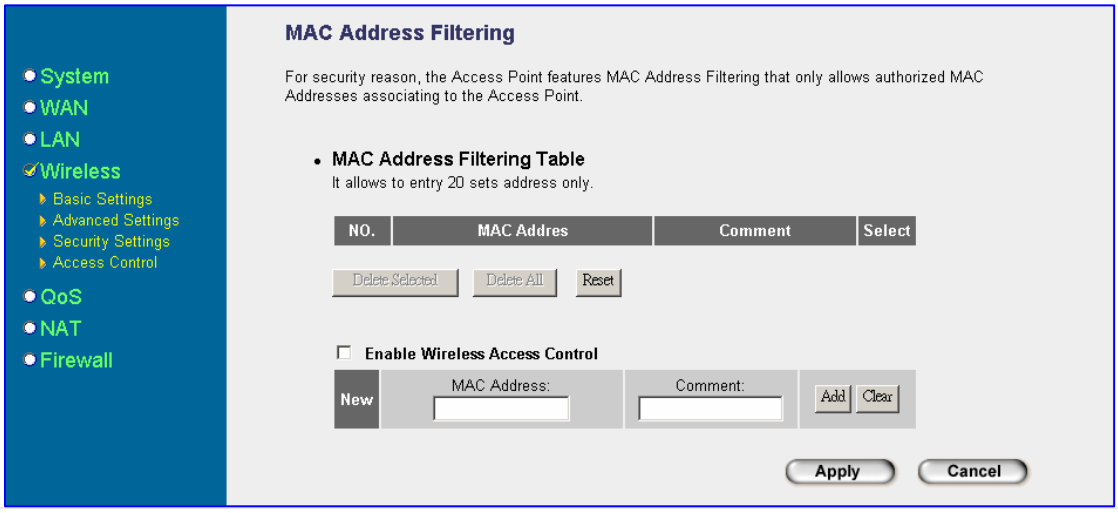


Параметр		Описание
Encryption (шифрование)		В данном случае необходимо выбрать **WPA RADIUS**.
WPA Unicast Cipher Suite	WPA (TKIP)	Протокол TKIP обеспечивает динамический обмен ключами, что повышает защищенность беспроводной сети.
	WPA2 (AES)	Использует протокол CCMP. CCMP основан на методе CCM алгоритма шифрования AES. Все AES-процессы, применяемые в CCMP, используют AES с 128-битным ключом и 128-битным размером блока. Этот алгоритм обеспечивает очень высокий уровень защищенности беспроводной сети.
	WPA2 Mixed	Совмещенный режим обмена ключами с использованием алгоритмов TKIP или AES, выбираемых автоматически.
RADIUS Server IP Address		Введите IP адрес RADIUS Сервера
RADIUS Server Port		Введите другой номер порта для вашего Radius Сервера или оставьте принятый по умолчанию (1812)
RADIUS Server Password		Введите пароль, который настроен на Radius Сервере

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.4.4 Контроль доступа (Access Control)

WRT-414 поддерживает Фильтрацию по MAC Адресам, которая не позволит подключиться пользователям не занесенным в Лист контроля доступа получить доступ к Вашей беспроводной сети.



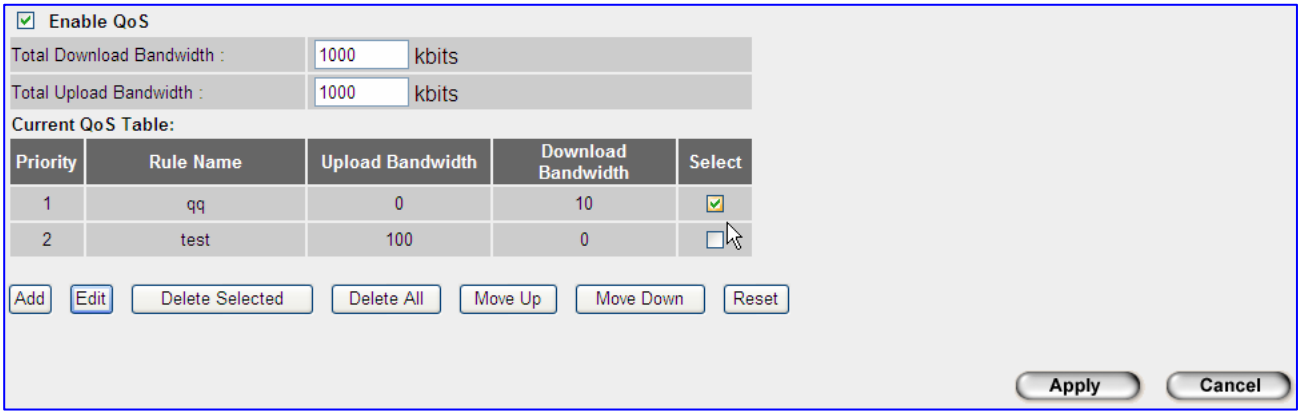
Параметр	Описание
Enable Wireless Access Control	Включить или выключить функцию фильтрации по MAC адресам.
Добавление MAC адреса в таблицу	Введите MAC адрес устройства в поле “**MAC Address**” без двоеточий или дефисов и добавьте необходимый комментарий в поле“Comment”. После этого нажмите кнопку **Add**. Запись будет добавлена в таблицу “MAC Address Filtering Table”.

Параметр	Описание
Удаление выбранного MAC адреса из таблицы	Выделите нужные записи в поле Select, поставив галочки напротив нужных записей, и нажмите **Delete Selected**.
Удаление всех MAC адресов из таблицы	Нажмите **Delete All** для удаления всех записей из таблицы.
Reset (сброс)	Нажмите **Reset** для снятия выделения со всех выбранных записей таблицы

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.5 QoS (Quality of Service - качество обслуживания)

В применении к данному маршрутизатору этот термин означает, что роутер можно настроить для обеспечения приоритета определенным сетевым протоколам или соединениям (передавать их пакеты в первую очередь). Например, весьма логично дать высокий приоритет VoIP пакетам и низкий пакетам клиента файлообменной сети. Приоритет для правил назначается в зависимости от их положения в списке правил. Наивысший приоритет имеет первое правило, самый низкий приоритет у последнего правила.



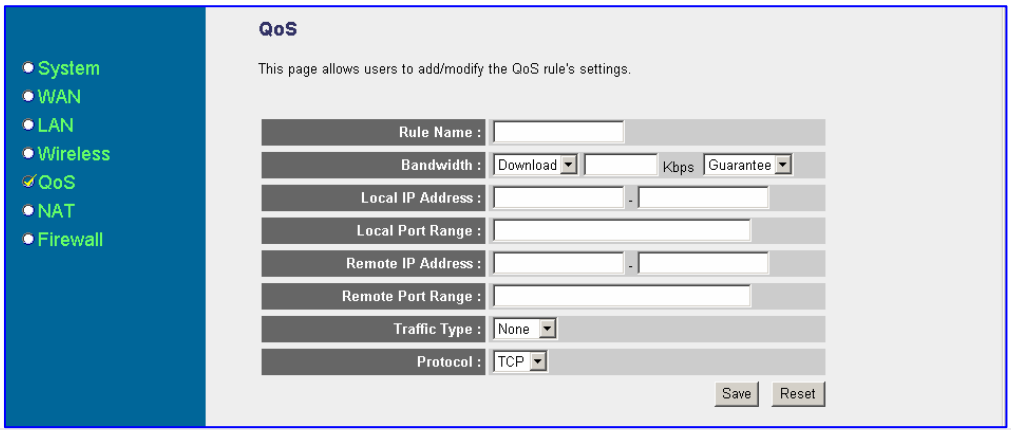
Параметр	Описание
Enable QoS	Включить Качество обслуживания (поставить галочку)
Total Download Bandwidth	Суммарная пропускная способность для входящего трафика (введите реальное значение)
Total Upload Bandwidth	Суммарная пропускная способность для исходящего трафика (введите реальное значение)
Add	Добавление нового правила QoS, нажмите кнопку и обратитесь к разделу 4.5.1 для получения более подробной информации
Edit	Редактирование выбранного правила QoS. Поставьте галочку напротив нужного правила, нажмите кнопку Edit и обратитесь к разделу 4.5.1 для получения более подробной информации
Delete Selected	Удаление выбранного правила QoS. Выделите нужные записи в поле Select, поставив галочки напротив нужных записей, и нажмите **Delete Selected**
Delete All	Нажмите **Delete All** для удаления всех записей из таблицы.
Move Up	Перемещение правила вверх для назначения ему более высокого приоритета
Remove Down	Перемещение правила вниз для назначения ему более низкого приоритета
Reset (сброс)	Нажмите **Reset** для снятия выделения со всех выбранных записей таблицы

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.5.1 Добавление, редактирование и удаление правил QoS

Вы можете классифицировать правила по IP адресу или диапазону IP адресов отправителя, диапазону адресов или IP адресу получателя, типу трафика, протоколу (TCP или UDP), номеру порта или диапазону портов отправителя и номеру порта или диапазону портов получателя. Параметры, которые Вы оставляете пустыми, будут игнорироваться (то есть подразумевается всего возможного диапазона для данного параметра). Качество обслуживания будет применено к пакетам проходящим через маршрутизатор и соответствующим одному из установленных правил. К пакетам трафика, совпавшим по условиям классификации с первым подходящим по параметрам правилом (проверяется от правил со старшим приоритетом к правилам с низшим приоритетом), будет обработан в соответствии с этим правилом. Это позволяет ограничить пропускную способность, для пакетов, которые соответствуют этому правилу или обеспечить гарантированную пропускную способность для таких пакетов.

После нажатия Add или Edit в меню QoS откроется окно настройки правил QoS.

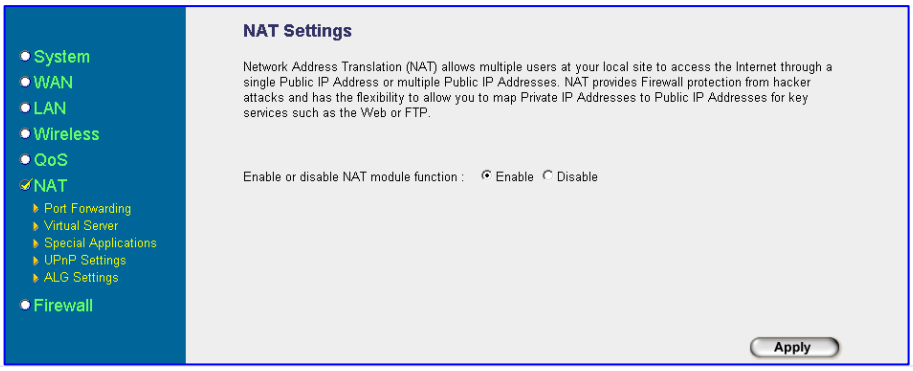


Параметр	Описание
Rule Name	Имя правила QoS. Вы можете ввести произвольное имя в латинской раскладке длинной не более 15 символов.
Bandwidth	Вы можете ограничить максимальную пропускную способность, используемую в соответствии с этим правилом, выбрав **Maximum**. Вы также можете гарантированную пропускную способность для этого правила, выбрав **Guarantee**. При настройке правил пропускной способности следует учитывать, что предел пропускной способности вводится в Килобитах в секунду(Кбит/с или Kbps). Не путайте с Килобайтами в секунду (КБайт/с или KBps)! **1KBps равен 8Kbps**. Когда Вы вводите пропускную способность, пожалуйста удостоверьтесь что используете правильные единицы измерения. Например, если Вы хотите ограничить скорость загрузки до 50KBps из Интернета, то в это поле следует ввести 400Kbps.
Local IP Address	Введите локальный IP адрес хоста или диапазон локальных IP адресов.
Local Port Range	Введите номер локального порта или диапазон локальных портов.
Remote IP Address	Введите IP адрес удаленного сайта или диапазон IP адресов находящихся во внешней сети (WAN).
Remote Port Range	Введите номер порта или диапазон портов.
Traffic Type	Выберите тип трафика для пакетов, к которым применяется это правило. Здесь перечислено несколько популярных приложений, выбор которых позволит упростить настройку и не вводить номера портов. Вы можете получить аналогичный результат, используя номера портов для исходящего и входящего трафика.
Protocol	Выберите тип транспортного протокола (TCP или UDP).

*Нажмите кнопку **Save**, после завершения настройки. Роутер сохранит изменения для правила и снова откроется страницы со списком правил QoS. После этого нажмите кнопку **Apply**, для завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.6 Трансляция сетевых адресов (NAT)

В режиме NAT все пользователи используют локальные IP адреса и при обращении к сети Интернет они скрыты из вне благодаря механизму Трансляции Сетевых адресов (NAT). Трансляция сетевых Адресов позволяет пользователям получить совместный, защищенный доступ к ресурсам сети Интернет используя один WAN порт маршрутизатора (один внешний IP адрес, выделенный провайдером для подключения к Интернету). При работе в режиме NAT широкополосный маршрутизатор обеспечивает надежную защиту Вашего сетевого подключения и обеспечивает поддержку дополнительных сервисов позволяющих осуществить проброс портов и обеспечить работу специальных приложений и протоколов, расположенных на хостах в локальной сети.
Вы можете отключить NAT. В этом случае WRT-414 будет работать как обычный роутер, транслируя пакеты из одной сети в другую. В этом режиме Вы можете прописать статические маршруты для правильной маршрутизации между разными локальными сетями.



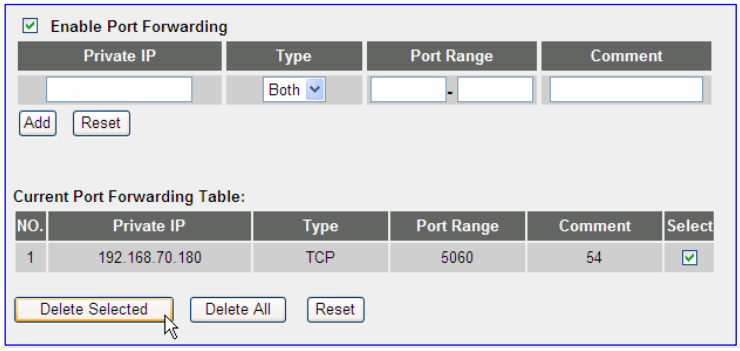
Параметр	Описание
Enable/Disable	Включение или выключение Трансляции Сетевых Адресов (NAT). По умолчанию включено.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

Раздел Меню	Описание
4.6.1 Port Forwarding	Вы можете использовать различные службы (например, электронная почта, FTP, Web и т.д.) расположенные за NAT на разных хостах в вашей локальной сети и использующих различные сервисы к которым нужно разрешить доступ из Внешней сети (Интернет или Интранет). Перенаправление Портов позволяет Вам переадресовывать запросы различных сервисов из внешней сети (WAN) к определенному диапазону портов на нужный IP адрес LAN. Поле Type позволяет выбрать вид транспортного протокола (UDP,TCP или оба).
4.6.2 Virtual Server	Виртуальный сервер позволит Вам перенаправить обращение (из Интернет) к определенному номеру внешнего порта WAN, на нужный номер внутреннего порта LAN на указанный хост. Обычно это преобразование вида "Один ко многим", то есть к нескольким хостам в локальной сети, но в данной модели SOHO маршрутизатора Вы можете указать только один IP адрес локального хоста. В отличеи от Перенаправления портов в этом меню нельзя указать диапазон портов, зато можно указать различные порты для внешнего и внутреннего интерфейса маршрутизатора.
4.6.3 Special Applications	Некоторые приложения требуют параллельных соединений. Это Интернет Игры, видео конференц-связь, IP телефония и другие. В этом меню Вы можете настроить маршрутизатор, для правильной работы таких приложений.
4.6.4 ALG Setting	**Служба шлюза уровня приложения** Эта служба предназначена для поддержки подключений, которые позволяют сетевым протоколам проходить через брандмауэр и функционировать в случае использования общего доступа к подключению Интернета. В этом меню можно выбрать специальные приложения, которые нуждаются “в Шлюзе Уровня Приложения”.
4.6.5 UpnP Setting	Эта технология реализована во всех современных ОС Windows. Подробную информацию о ней можно получить тут: UPnP . Режим UPnP не только обеспечивает поддержку принципа "включай и работай". Этот режим позволяет реализовать поддержку нулевой конфигурации, "невидимое" сетеобразование, и автоматическое подключение и настройку различного сетевого оборудования поддерживающего эту технологию. Устройство поддерживающее данную технологию может динамически присоединиться к сети, получить адрес IP, сообщить свои возможности, и узнать о присутствии и возможностях других устройств автоматически и наладить взаимодействие без участия пользователя и дополнительной настройки.

4.6.1 Перенаправление Портов (Port Forwarding)

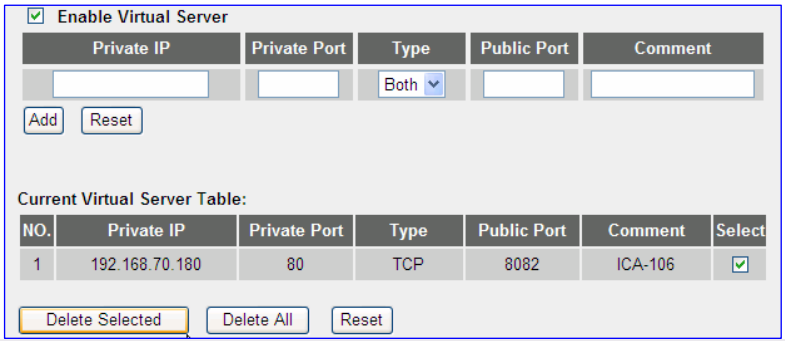
Вы можете использовать различные службы (например, электронная почта, FTP, Web и т.д.) расположенные за NAT на разных хостах в вашей локальной сети и использующих различные сервисы к которым нужно разрешить доступ из Внешней сети (Интернет или Интранет). Перенаправление Портов позволяет Вам переадресовывать запросы различных сервисов из внешней сети (WAN) к определенному диапазону портов на нужный IP адрес LAN. Поле Type позволяет выбрать вид транспортного протокола (UDP,TCP или оба).



Параметр	Описание
Enable Port Forwarding	Включить перенаправление портов (поставьте галочку)
Private IP	Приватный IP адрес хоста, расположенный в локальной сети (порты LAN) за NAT.
Внимание!: Локальному хосту должен быть присвоен статический IP адрес, чтобы перенаправление портов работало правильно вне зависимости от динамически раздающихся адресов встроенным DHCP сервером. Если этого не сделать, то есть вероятность что данный хост со временем получит другой IP адрес и перенаправление портов перестанет работать.	
Type	Поле Type позволяет выбрать вид транспортного протокола (UDP,TCP или оба) для перенаправления портов. Выберите TCP, UDP или both (оба типа) для перенаправления пакетов соответствующего типа.
Port Range	Диапазон портов (начальный и конечный порт) для перенаправления.
Comment	Описание настройки (опциональное поле).
Add	Эта кнопка позволяет добавить новое правило в таблицу перенаправления портов.
Reset (под верхней таблицей)	Отмена добавления правила (очистка всех полей верхнего меню). Действует только на вновь вводимое правило, до нажатия кнопки Add
Select	Поставьте галочку в строках правил, которые необходимо выбрать
Delete Selected	Эта кнопка позволяет удалить выбранные правила (отмеченные галочкой в поле Select)
Delete All	Эта кнопка позволяет удалить одновременно все настроенные правила.
Reset (под нижней таблицей)	Удаляет выделение для всех выбранных правил (снимает все галочки в поле Select)

4.6.2 Виртуальный Сервер (Virtual Server)

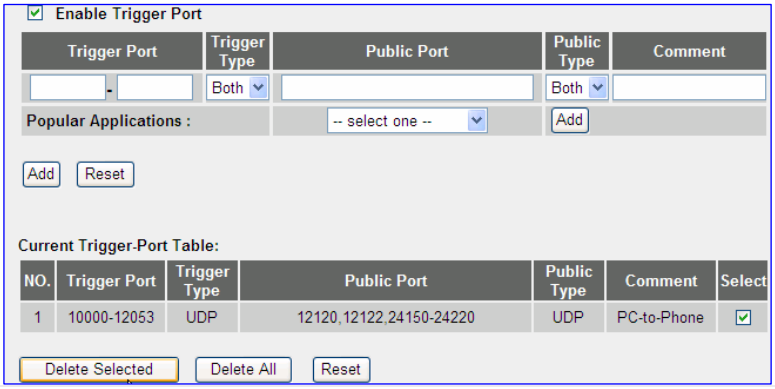
Виртуальный сервер позволит Вам перенаправить обращение (из Интернет) к определенному номеру внешнего порта WAN, на нужный номер внутреннего порта LAN на указанный хост. Обычно это преобразование вида "Один ко многим", то есть к нескольким хостам в локальной сети, но в данной модели SOHO маршрутизатора Вы можете указать только один IP адрес локального хоста. В отличие от Перенаправления портов в этом меню нельзя указать диапазон портов, зато можно указать различные порты для внешнего и внутреннего интерфейса маршрутизатора. (Смотрите Список Терминов для получения дополнительной справки по номерам портов)



Параметр	Описание
Enable Virtual Server	Включить перенаправление портов (поставьте галочку)
Private IP	Приватный IP адрес хоста, расположенный в локальной сети (порты LAN) на который будут перенаправлены пакеты с публичного порта.
Внимание!: Локальному хосту должен быть присвоен статический IP адрес, чтобы Виртуальный Сервер работал правильно вне зависимости от динамически раздающихся адресов встроенным DHCP сервером. Если этого не сделать, то есть вероятность что данный хост со временем получит другой IP адрес и перенаправление портов перестанет работать.	
Private Port	Номер внутреннего порта (для приватного IP адреса хоста) на который необходимо перенаправить пакеты при обращении к публичному порту маршрутизатора.
Type	Поле Type позволяет выбрать вид транспортного протокола (UDP,TCP или оба) для виртуального сервера. Выберите TCP, UDP или both (оба типа) для перенаправления пакетов соответствующего типа.
Public Port	Номер внешнего порта (публичного WAN IP маршрутизатора) с которого необходимо перенаправить пакеты на приватный порт для указанного в настройках IP адреса.
Comment	Описание настройки (опциональное поле).
Add	Эта кнопка позволяет добавить новое правило в таблицу Виртуального Сервера.
Reset (под верхней таблицей)	Отмена добавления правила (очистка всех полей верхнего меню). Действует только на вновь вводимое правило, до нажатия кнопки Add
Select	Поставьте галочку в строках правил, которые необходимо выбрать
Delete Selected	Эта кнопка позволяет удалить выбранные правила (отмеченные галочкой в поле Select)
Delete All	Эта кнопка позволяет удалить одновременно все настроенные правила.
Reset (под нижней таблицей)	Удаляет выделение для всех выбранных правил (снимает все галочки в поле Select)

4.6.3 Специальные Приложения (Special Applications)

Некоторые приложения требуют параллельных соединений. Это Интернет Игры, видео конференц-связь, IP телефония и другие. В этом меню Вы можете настроить маршрутизатор, для правильной работы таких приложений.



Параметр	Описание
Enable Trigger Port	Включить поддержку специальных приложений (поставьте галочку)
Trigger Port	Диапазон исходящих номеров портов используемых специальными приложениями.

Параметр	Описание
Trigger Type	Поле Trigger Type позволяет выбрать вид транспортного протокола (UDP,TCP или оба) для специальных приложений. Выберите TCP, UDP или both (оба типа) для обработки пакетов соответствующего типа.
Public Port	Номер входящего порта или диапазон внешних портов (публичного WAN IP маршрутизатора) с которого необходимо обрабатывать пакеты для специальных приложений. Например: 2300-2400, 47624
Внимание!: Отдельные номера портов необходимо отделить запятой. Например: 47624, 5775, 6541 и т.д. Диапазон портов вводится через дефис. Например: 2300-2400	
Public Type	Поле Public Type позволяет выбрать вид транспортного протокола (UDP,TCP или оба) входящих пакетов специальных приложений. Выберите TCP, UDP или both (оба типа) для обработки пакетов соответствующего типа.
Comment	Описание настройки (опциональное поле).
Popular applications	Здесь можно выбрать из списка одно из нескольких наиболее популярных приложений которые требуют параллельных соединений. Выберите нужное приложение, если оно имеется в списке, и нажмите **Add** (справа от раскрывающегося меню выбора). Информация о необходимых настройках для данного приложения будет автоматически скопирована в соответствующие поля таблицы.
Add	Эта кнопка позволяет добавить новое правило в таблицу.
Reset (под верхней таблицей)	Отмена добавления правила (очистка всех полей верхнего меню). Действует только на вновь вводимое правило, до нажатия кнопки Add
Select	Поставьте галочку в строках правил, которые необходимо выбрать
Delete Selected	Эта кнопка позволяет удалить выбранные правила (отмеченные галочкой в поле Select)
Delete All	Эта кнопка позволяет удалить одновременно все настроенные правила.
Reset (под нижней таблицей)	Удаляет выделение для всех выбранных правил (снимает все галочки в поле Select)

Пример использования Специальных Приложений

Если Вы используете приложения, которые требуют параллельных соединений, то определите порт (исходящий) сопоставленный с портами используемым приложением в поле "Trigger Port". Выберите тип протокола (TCP или UDP) и введите публичные порты, связанные с триггерным портом, чтобы открыть их для входящего трафика.

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

В показанном примере используется пользовательский триггерый порт 28800 (исходящий) для MSN Game Zone для которого маршрутизатор разрешает входящие пакеты с портов 2300-2400 и 47624, которые будут перенаправлены конечному пользователю (хосту, использующему данное приложение).

Внимание!: Только один клиент в локальной сети может использовать специальное приложение. Одновременная работа нескольких клиентов в локальной сети с одним и тем же приложением, использующим одну настройку Special Applications.

4.6.4 Служба Уровня Приложения (ALG Settings)

Эта служба предназначена для поддержки подключений, которые позволяют сетевым протоколам проходить через брандмауэр и функционировать в случае использования общего доступа к подключению Интернета. В этом меню можно выбрать специальные приложения, которые нуждаются “в Шлюзе Уровня Приложения”.

Enable	Name	Comment
☑	Amanda	Support for Amanda backup tool protocol.
☑	Egg	Support for eggdrop bot networks.
☑	FTP	Support for FTP.
☑	H323	Support for H323/netmeeting.
☑	IRC	Allows DCC to work though NAT and connection tracking.
☑	MMS	Support for Microsoft Streaming Media Services protocol.
☑	Quake3	Support for Quake III Arena connection tracking and nat.
☑	Talk	Allows netfilter to track talk connections.
☑	TFTP	Support for TFTP.
☑	Starcraft	Support for Starcraft/Battle.net game protocol.
☑	MSN	Support for MSN file tranfer.

Параметр	Описание
Enable	Поставьте галочку напротив нужных приложений, чтобы обеспечить их правильную работу за NAT. **По умолчанию:** выбраны все приложения

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.6.5 Универсальный PnP (UPnP)

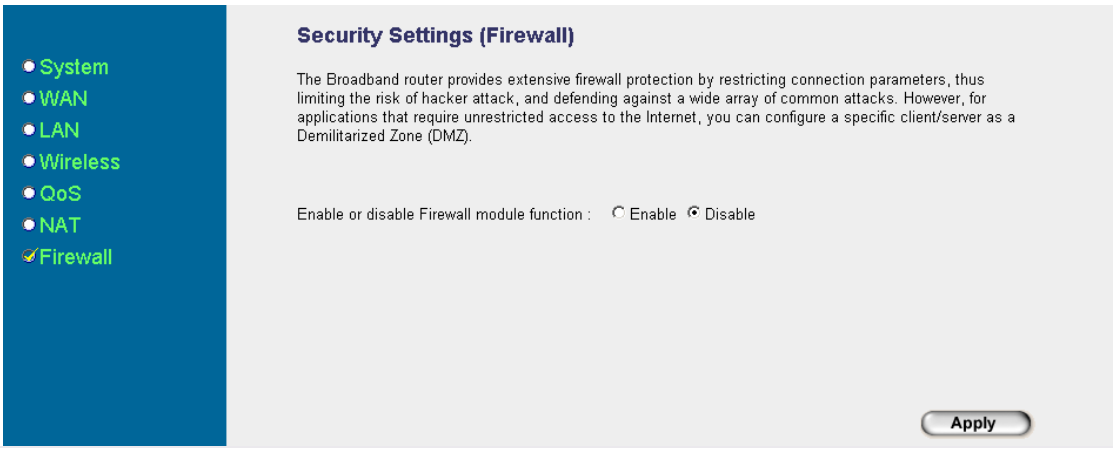
Эта технология реализована во всех современных ОС Windows. Подробную информацию о ней можно получить тут: UPnP . Режим UPnP не только обеспечивает поддержку принципа "включай и работай". Этот режим позволяет реализовать поддержку нулевой конфигурации, "невидимое" сетеобразование, и автоматическое подключение и настройку различного сетевого оборудования поддерживающего эту технологию. Устройство, поддерживающее данную технологию, может динамически присоединиться к сети, получить адрес IP, сообщить свои возможности, и узнать о присутствии и возможностях других устройств автоматически и наладить взаимодействие без участия пользователя и дополнительной настройки.
Для включения выберите **Enable**, а для отключения **Disable**.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

4.7 Межсетевой Экран (Firewall)

Меню Межсетевого Экрана (Firewall) позволяет настроить Контроль доступа (Access Control), функцию блокировки URL или содержимого (URL Blocking), детектирование атак хакеров (DoS) и демилитаризованную зону (DMZ).

Внимание!: Для включения межсетевого экрана выберите **Enable** и нажмите **Apply**

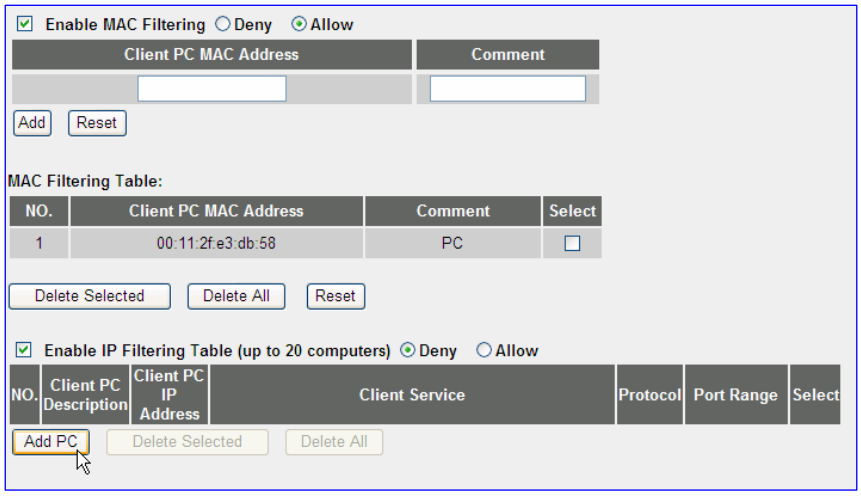


Параметр	Описание
4.7.1 Access Control	Контроль доступа по MAC адресам позволяет Вам определять, какие хосты в локальной сети смогут или не смогут получить доступ к ресурсам сети Интернет (привязка по MAC адресу). Также можно разрешить для определённых хостов (до 20) только ограниченный набор сервисов, привязав их по IP адресу. Например, только ftp и http.
4.7.2 URL Blocking	Это меню позволяет заблокировать нежелательные сайты по URL или нежелательное содержимое. **Внимание!:** при вводе правила нельзя использовать кириллицу. Такое правило будет сохранено, но маршрутизатор не сможет обработать запрос, и не заблокирует подобное содержимое сайта.
4.7.3 DoS	Выбор видов атак, которые будет обрабатывать межсетевой экран роутера.
4.7.4 DMZ	Демилитаризованная зона. Эта функция позволяет переадресовать все пакеты, приходящие на порт WAN маршрутизатора, указанному хосту в локальной сети (локальный IP адрес).

Выберите нужный пункт меню и перейдите к его подробному описанию

4.7.1 Контроль доступа (Access Control)

Контроль доступа позволяет Вам определять, какие хосты в локальной сети смогут или не смогут получить доступ к ресурсам сети Интернет (привязка по MAC адресу не более 20 хостов). Также можно разрешить для определённых хостов (не более 20 хостов) только ограниченный набор сервисов, привязав их по IP адресу. Например, только ftp и http.



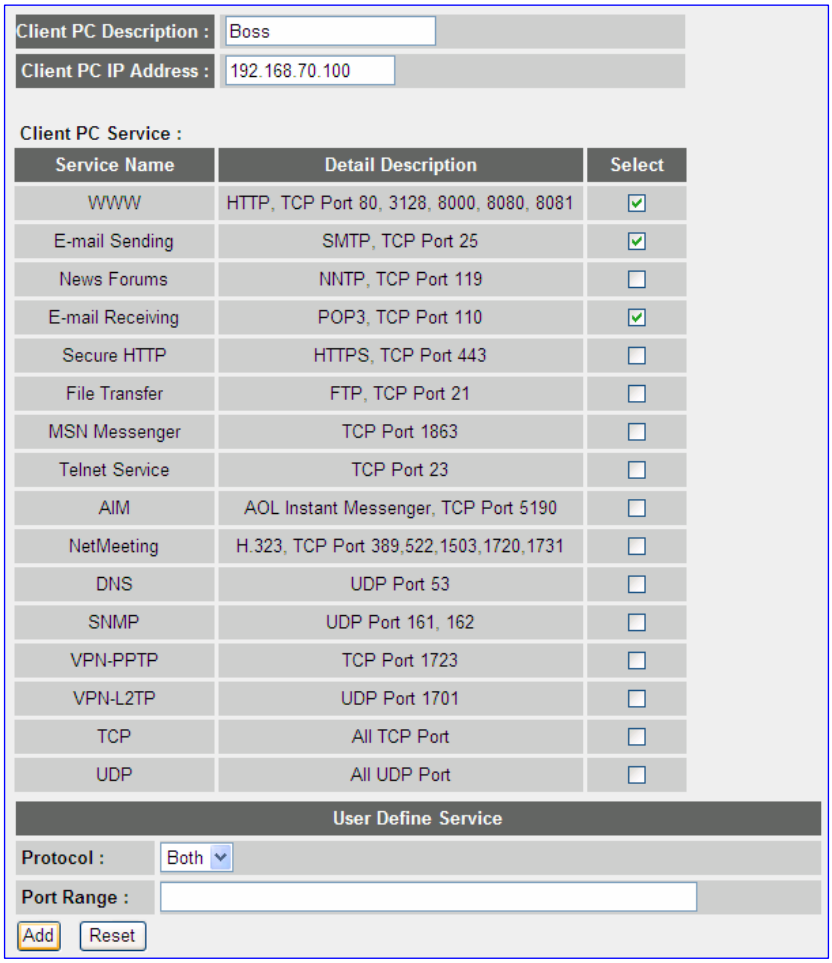
Параметр	Описание
Фильтрация по MAC	Выберите “**Enable MAC Filtering**” для включения режима фильтрации по MAC адресам.
Добавление правила	В поле “Client PC MAC Address” впишите MAC адрес хоста (без разделителей), а в поле “Comment” произвольный текст, который позволит Вам в будущем идентифицировать правило. Нажмите кнопку “Add”. Вы можете выбрать один из двух видов действий для фильтрации по MAC адресам. Режим разрешения (**Allow**) или запрета (**Deny**) доступа с указанных MAC адресов к ресурсам сети Интернет. **Вы можете создать до 20 правил фильтрации по MAC адресам.** **Внимание!:** при вводе правила фильтрации по MAC следует учесть, что режим запрета или разрешения доступа действует на все введённые MAC адреса одновременно. Вы не можете одновременно разрешить одним хостам доступ в Интернет, а другим запретить. Можно выполнить только одно из двух действий.
Удаление правила	
Delete Selected	Эта кнопка позволяет удалить выбранные правила (отмеченные галочкой в поле Select)
Delete All	Эта кнопка позволяет удалить одновременно все настроенные правила.
Reset	Удаляет выделение для всех выбранных правил (снимает все галочки в поле Select)
Фильтрация по IP	Выберите “IP Filtering Table” для включения режима фильтрации по IP адресам.
Добавление правила	Нажмите кнопку **Add PC** – откроется новое окно добавления правила фильтрации по IP. Смотрите подробное описание ниже. Вы можете выбрать один из двух видов действий для фильтрации по IP адресам. Режим разрешения (**Allow**) или запрета (**Deny**) доступа с указанных IP адресов к ресурсам сети Интернет. **Внимание!:** при вводе правила фильтрации по IP следует учесть, что режим запрета или разрешения доступа действует на все введённые IP адреса одновременно. Вы не можете одновременно разрешить одним хостам доступ в Интернет, а другим запретить. Можно выполнить только одно из двух действий. Но в то же самое время, можно разрешить или запретить (одно из двух) для разных IP адресов различные протоколы.
Удаление правила	
Delete Selected	Эта кнопка позволяет удалить выбранные правила (отмеченные галочкой в поле Select)
Delete All	Эта кнопка позволяет удалить одновременно все настроенные правила.

Добавление правила фильтрации по IP (Add PC)

Параметр	Описание
Client PC Description	произвольный текст, который позволит Вам в будущем идентифицировать правило
Client PC IP Addresses	Введите IP адрес хоста, для которого необходимо применить это правило Контроля доступа. **Вы можете создать до 20 правил фильтрации по IP адресам.** **Внимание!:** Локальному хосту должен быть присвоен статический IP адрес, чтобы фильтрация по IP адресам работала правильно вне зависимости от динамически раздающихся адресов встроенным DHCP сервером. Если этого не сделать, то есть вероятность что данный хост со временем получит другой IP адрес и правила фильтрации по IP адресам для этого хоста перестанет работать.
Client PC Service	Выберите стандартные сервисы, которые необходимо разрешить для данного IP адреса.
Protocol	Выберите TCP, UDP или both (оба типа) для обработки пакетов соответствующего типа. (настройка связана с меню Port Range (см. следующую строку таблицы).
Port Range	Вы можете назначить до пяти диапазонов портов. Маршрутизатор будет разрешать или запрещать (в зависимости от выбранного действия) при обращении хоста к ресурсам сети Интернет с этих портов. Эта настройка позволяет фильтровать порты Сервисов, которых нет в меню Client PC Service.
Apply Changes	Нажмите “**Apply Changes**” для сохранения настроек
Reset	Нажмите “**Reset**” для отмены сохранения правила.

Пример фильтра для пользователя Boss.

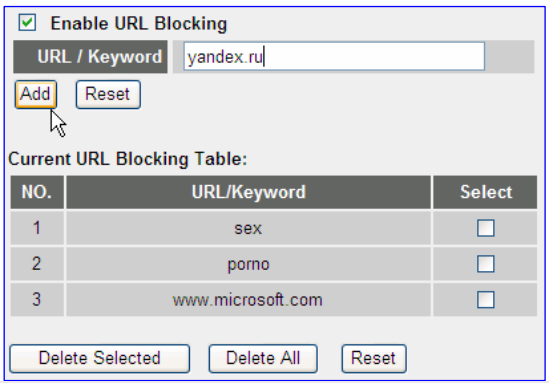
В строке **Enable MAC Filtering** установлено Deny (запретить). Это означает что пользователь Boss (IP адрес 192.168.70.100) не сможет пользоваться браузером, отправлять и принимать почту. Но он сможет воспользоваться всеми остальными сервисами (например, ICQ, MSN, Skype и многие другие сервисы будут работать без проблем). Если это действительно Босс, то сисадмина видимо скоро попросят написать заявление на увольнение…



4.7.2 Блокировка URL (URL Blocking)

Это меню позволяет заблокировать нежелательные сайты по URL или доступ к сайтам с нежелательным содержимым.

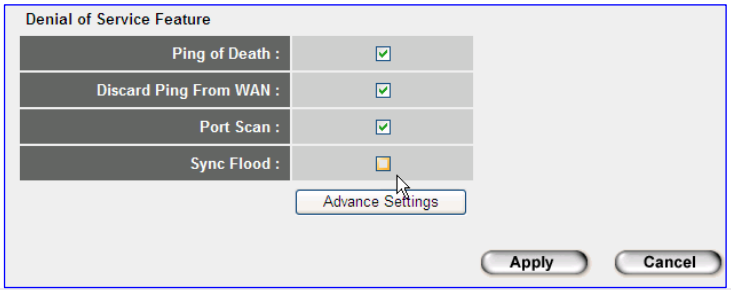
Внимание!: при вводе правила нельзя использовать кириллицу. Такое правило будет сохранено, но маршрутизатор не сможет обработать запрос, и не заблокирует подобное содержимое сайта.



Параметр	Описание
Enable URL Blocking	Включить или отключить фильтрацию URL
Добавление правила	В строку “URL/Keyword” введите доменное имя адреса сайта (можно ввести часть имени) или ключевое слово и нажмите “**Add**”. После добавления записи сайты имеющие в доменном имени введенную фразу или текст будут заблокированы и все пользователи локальной сети не смогут получить доступ к подобным ресурсам. Также будет заблокирована возможность поиска в поисковых системах браузера при совпадении даже части фразы в строке поисковика с введенной в таблицу **Current URL Blocking Table**
Удаление правила	
Delete Selected	Эта кнопка позволяет удалить выбранные правила (отмеченные галочкой в поле Select)
Delete All	Эта кнопка позволяет удалить одновременно все настроенные правила.

4.7.3 Отказ в Обслуживании (DoS)

Выбор видов атак, которые будет обрабатывать межсетевой экран роутера и настройка реакции на различные виды атак.

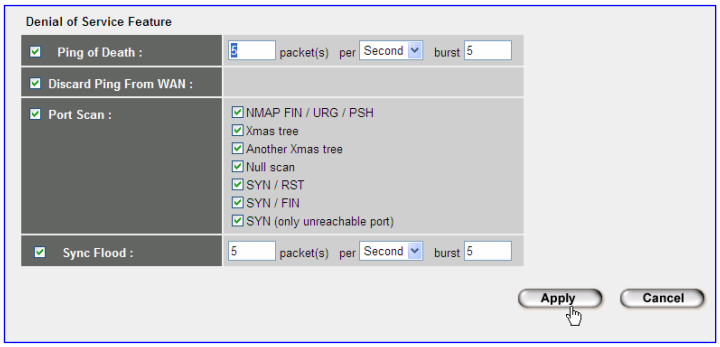


Параметр	Описание
Ping of Death	Защита роутера от атак Ping of Death
Discard Ping From WAN	Отключение ответа WAN порта роутера на запросы ping
Port Scan	Защита роутера от сканирования его портов
Sync Flood	Защита роутера от атак Sync Flood
Advance Setting	Расширенные настройки защиты, позволяющие настроить реакцию роутера на те или иные виды атак

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

Меню Advance Setting

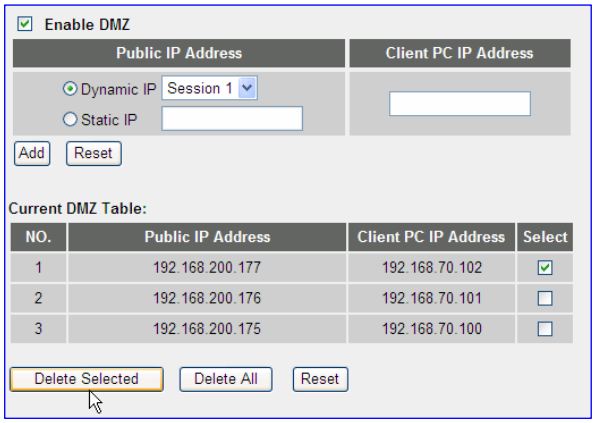
Здесь можно сделать тонкую настройку реакции межсетевого экрана на те или иные виды атак. Измените необходимые параметры настроек и нажмите **Apply** для сохранения изменений.



4.7.4 Демилитаризованная зона (DMZ)

Демилитаризованная зона – это зона, в которой не действуют правила и политики межсетевого экрана (свободное прохождение любых пакетов в обе стороны). Эта функция позволяет переадресовать все пакеты, приходящие на порт WAN маршрутизатора, указанному хосту в локальной сети (локальный IP адрес).

Если возникли проблемы с работой сетевых приложений на одном из хостов в сети, которые не могут нормально функционировать, находясь за межсетевым экраном с NAT(например, Игры), то Вы можете открыть этот хост для неограниченного двухстороннего доступа в Интернет, используя функцию DMZ. Различие между Виртуальным сервером и функцией DMZ состоит в том, что Виртуальный Сервер переадресовывает пакеты с определенных портов на указанный порт локального хоста. Функция DMZ позволяет присвоить определенному хосту в локальной сети реальный WAN IP адрес из внешней сети и пересылать все пакеты, при обращении к любым портам такого устройства, в обе стороны без ограничений.



ВАЖНО! Здесь следует отметить один немаловажный момент. Обычно порт DMZ в более дорогих маршрутизаторах реализован в виде отдельного интерфейса и специфика его работы отличается от описанной здесь тем, что пакеты через такой порт проходят в обе стороны, без фильтрации межсетевым экраном, но хосты расположенные в сегменте DMZ при этом находятся за NAT и им не сопоставлены внешние (реальные) IP адреса. В таких маршрутизаторах подобную функцию выполняет Mapping IP (по сути это является более правильной терминологией данного сервиса). Например BM-500, MH-2000, CS-500 и т.п. (*примечание автора перевода*)

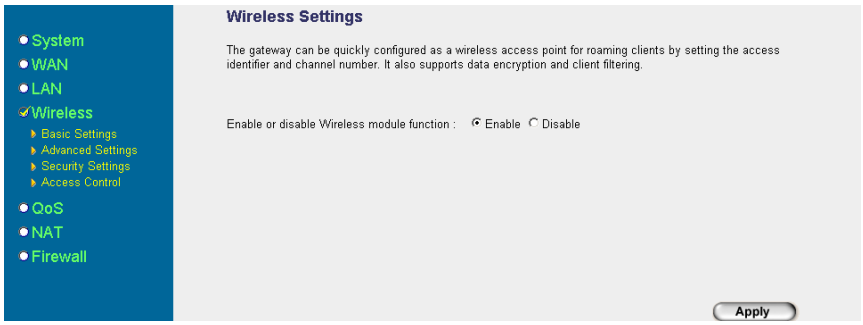
Параметр	Описание
Enable DMZ	Установка флажка включает DMZ
Public IP Address	IP адрес WAN порта роутера (если выбрано Dynamic IP) или любой другой внешний WAN IP адрес (если выбрано Static IP) выданный Вам Интернет провайдером.
Client PC IP Address	IP адрес хоста в локальной сети для которого необходимо настроить DMZ
Delete Selected	Эта кнопка позволяет удалить выбранные правила (отмеченные галочкой в поле Select)
Delete All	Эта кнопка позволяет удалить одновременно все настроенные правила.
Reset	Удаляет выделение для всех выбранных правил (снимает все галочки в поле Select)

Внимание!:

- Если настройки Virtual Server и DMZ будут конфликтовать между собой, то настройки, сделанные для функции Virtual Server, будут иметь приоритет над функцией DMZ.
- Локальному хосту должен быть присвоен статический IP адрес, чтобы DMZ работал правильно вне зависимости от динамически раздающихся адресов встроенным DHCP сервером. Если этого не сделать, то есть вероятность что данный хост со временем получит другой IP адрес и DMZ перестанет работать.

Раздел 5 Настройка беспроводного интерфейса (Wireless Configuration)

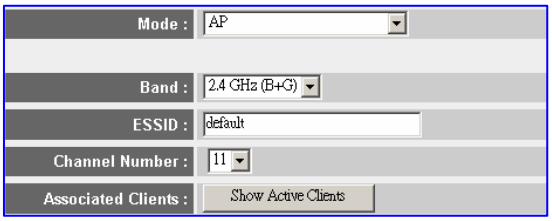
На этой странице можно включить или выключить беспроводной интерфейс маршрутизатора (по умолчанию включен). Обратитесь к соответствующим разделам, расположенным ниже, чтобы правильно настроить беспроводной интерфейс для соответствующего режима работы.

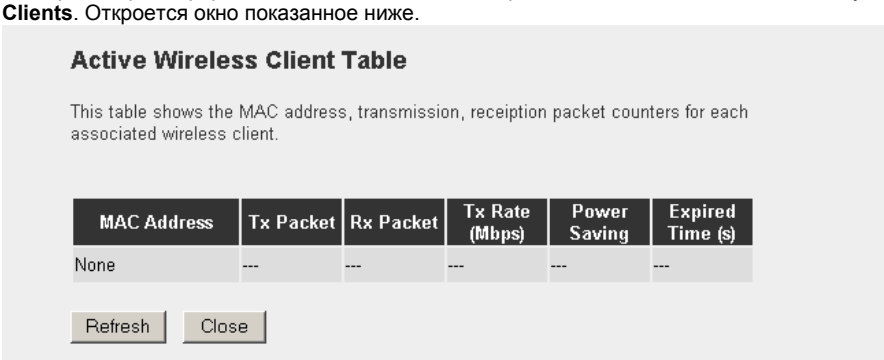


5.1 Режим работы Точка Доступа (AP Mode)

Этот режим используется по умолчанию. Фактически этот режим является преобразователем среды между клиентами беспроводной локальной сети (WLAN) и обычной проводной локальной сетью (LAN). Беспроводные клиенты (адаптеры или другие точки доступа) смогут подключиться к этой Точке Доступа, используя режим Infrastructure.

Внимание! Если используется шифрование, то в настройках подключения беспроводных клиентов необходимо выполнить соответствующие настройки.

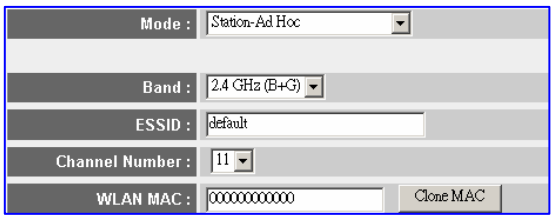


Параметр	Описание
Mode (Режим работы)	Для этого режима следует выбрать **AP**
Band (вид поддержки беспроводных клиентов стандартов 802.11b/g)	Выберите режим работы в зависимости от используемого у Вас беспроводного оборудования. **2.4GHz (B):** разрешено подключение беспроводных клиентов только стандарта 802.11b. **2.4GHz (G):** разрешено подключение беспроводных клиентов только стандарта 802.11g. **2.4GHz (B+G):** совмещенный режим. Разрешено подключение беспроводных клиентов стандартов 802.11b/g одновременно. При одновременном подключении клиентов 802.11b и 802.11g неизбежно произойдет снижение пропускной способности для всех подключенных клиентов. Поэтому этот режим рекомендуется использовать только при наличии в беспроводных клиентов не поддерживающих 802.11g.
ESSID (Идентификатор беспроводной сети)	ESSID (до 32-х печатных символов ASCII) это уникальное имя, сопоставленное данной беспроводной сети. Идентификатор предотвращает случайное объединение двух пересекающихся беспроводных локальных сетей. Пожалуйста, удостоверьтесь, что установили одинаковые идентификаторы ESSID для всех клиентов в Вашей сети WLAN. Значение по умолчанию "**default**" рекомендуется изменить на уникальное имя.
Channel Number (Номер канала)	Если в зоне действия Вашей беспроводной сети есть другие сети, то измените номер канала так, чтобы они оказывали друг на друга минимальное воздействие. Точка доступа позволяет использовать каналы с 1 по13. В стандарте 802.11b/g реально существует всего три канала оказывающих друг на друга минимальное воздействие. Это 1, 6 и 11 каналы. Если вы обнаружили беспроводные сети в зоне действия вашей сети или вам нужно сделать несколько беспроводных сетей с пересекающимися радиусами действия, то старайтесь использовать один из указанных каналов (не используемых в других беспроводных сетях). Этим Вы сможете снизить взаимные помехи беспроводных сетей друг на друга. Условие справедливо только в случае использования в соседних беспроводных сетях одного или двух из трех перечисленных каналов.
Associated Clients (Подключенные беспроводные клиенты)	Для просмотра информации о подключенных беспроводных клиентах нажмите кнопку **Show Active Clients**. Откроется окно показанное ниже.  Для обновления информации нажмите **Refresh**, чтобы закрыть окно нажмите **Close**.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

5.2 Режим работы Station-Ad Hoc

В режиме "Ad-hoc" каждое устройство или станция могут связываться непосредственно друг с другом, без использования точки доступа (AP). Режим "Ad-hoc" называют также "режим равный-с-равным" (peer-to-peer). В этом режиме WRT-414 выступает в качестве беспроводной станции. Этот режим позволяет расположить за точкой доступа(LAN порты маршрутизатора) персональный компьютер или создать небольшую локальную сеть (не более 5 хостов), без использования дополнительных Точек доступа.

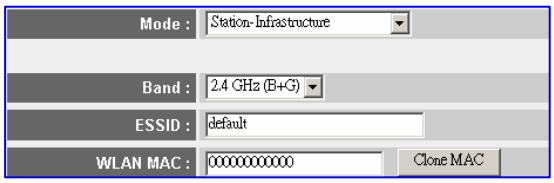


Параметр	Описание
Mode (Режим работы)	Для этого режима следует выбрать **Station-Ad Hoc**
Band (вид поддержки беспроводных клиентов стандартов 802.11b/g)	Выберите режим работы в зависимости от используемого у Вас беспроводного оборудования. **2.4GHz (B):** разрешено подключение беспроводных клиентов только стандарта 802.11b. **2.4GHz (G):** разрешено подключение беспроводных клиентов только стандарта 802.11g. **2.4GHz (B+G):** совмещенный режим. Разрешено подключение беспроводных клиентов стандартов 802.11b/g одновременно. При одновременном подключении клиентов 802.11b и 802.11g неизбежно произойдет снижение пропускной способности для всех подключенных клиентов. Поэтому этот режим рекомендуется использовать только при наличии в беспроводных клиентов не поддерживающих 802.11g.
ESSID (Идентификатор беспроводной сети)	ESSID (до 32-х печатных символов ASCII) это уникальное имя, сопоставленное данной беспроводной сети. Идентификатор предотвращает случайное объединение двух пересекающихся беспроводных локальных сетей. Пожалуйста, удостоверьтесь, что установили одинаковые идентификаторы ESSID для всех клиентов в Вашей сети WLAN. Значение по умолчанию "**default**" рекомендуется изменить на уникальное имя.
Channel Number (Номер канала)	Если в зоне действия Вашей беспроводной сети есть другие сети, то измените номер канала так, чтобы они оказывали друг на друга минимальное воздействие. Точка доступа позволяет использовать каналы с 1 по13. В стандарте 802.11b/g реально существует всего три канала оказывающих друг на друга минимальное воздействие. Это 1, 6 и 11 каналы. Если вы обнаружили беспроводные сети в зоне действия вашей сети или вам нужно сделать несколько беспроводных сетей с пересекающимися радиусами действия, то старайтесь использовать один из указанных каналов (не используемых в других беспроводных сетях). Этим Вы сможете снизить взаимные помехи беспроводных сетей друг на друга. Условие справедливо только в случае использования в соседних беспроводных сетях одного или двух из трех перечисленных каналов.
WLAN MAC	**Параметр по умолчанию**: маршрутизатор будет использовать свой MAC Адрес при обращении к беспроводной сети. **Если нажать кнопку "MAC Clone"**: будет использоваться MAC Адрес персонального компьютера, то MAC адрес компьютера с которого производилась настройка, клонируется в данное поле и будет использоваться при обращении к беспроводной сети.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

5.3 Режим работы Station-Infrastructure

В режиме "Infrastructure" каждое устройство или станция могут связываться друг с другом через Точку доступа (AP). В режиме "Infrastructure" (или по-другому клиент/сервер) беспроводная сеть состоит как минимум из одной точки доступа (Access Point), подключенной к проводной сети, и некоторого числа беспроводных оконечных станций. Такая конфигурация носит название базового набора служб (Basic Service Set, BSS). В этом режиме WRT-414 выступает в качестве беспроводной станции. Этот режим позволяет расположить за точкой доступа(LAN порты маршрутизатора) персональный компьютер или создать небольшую локальную сеть (не более 5 хостов), без использования дополнительных Точек доступа.

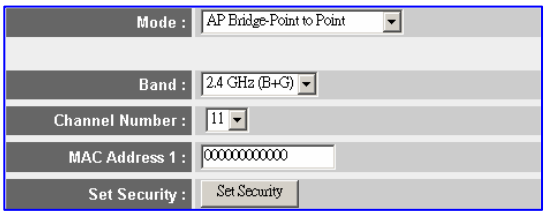


Параметр	Описание
Mode (Режим работы)	Для этого режима следует выбрать **Station-Infrastructure**
Band (вид поддержки беспроводных клиентов стандартов 802.11b/g)	Выберите режим работы в зависимости от используемого у Вас беспроводного оборудования. **2.4GHz (B):** разрешено подключение беспроводных клиентов только стандарта 802.11b. **2.4GHz (G):** разрешено подключение беспроводных клиентов только стандарта 802.11g. **2.4GHz (B+G):** совмещенный режим. Разрешено подключение беспроводных клиентов стандартов 802.11b/g одновременно. При одновременном подключении клиентов 802.11b и 802.11g неизбежно произойдет снижение пропускной способности для всех подключенных клиентов. Поэтому этот режим рекомендуется использовать только при наличии в беспроводных клиентов не поддерживающих 802.11g.
ESSID (Идентификатор беспроводной сети)	ESSID (до 32-х печатных символов ASCII) это уникальное имя, сопоставленное данной беспроводной сети. Идентификатор предотвращает случайное объединение двух пересекающихся беспроводных локальных сетей. Пожалуйста, удостоверьтесь, что установили одинаковые идентификаторы ESSID для всех клиентов в Вашей сети WLAN. Значение по умолчанию "**default**" рекомендуется изменить на уникальное имя.

Параметр	Описание
Channel Number (Номер канала)	Если в зоне действия Вашей беспроводной сети есть другие сети, то измените номер канала так, чтобы они оказывали друг на друга минимальное воздействие. Точка доступа позволяет использовать каналы с 1 по13. В стандарте 802.11b/g реально существует всего три канала оказывающих друг на друга минимальное воздействие. Это 1, 6 и 11 каналы. Если вы обнаружили беспроводные сети в зоне действия вашей сети или вам нужно сделать несколько беспроводных сетей с пересекающимися радиусами действия, то старайтесь использовать один из указанных каналов (не используемых в других беспроводных сетях). Этим Вы сможете снизить взаимные помехи беспроводных сетей друг на друга. Условие справедливо только в случае использования в соседних беспроводных сетях одного или двух из трех перечисленных каналов.
WLAN MAC	**Параметр по умолчанию**: маршрутизатор будет использовать свой MAC Адрес при обращении к беспроводной сети. **Если нажать кнопку "MAC Clone"**: будет использоваться MAC Адрес персонального компьютера, то MAC адрес компьютера с которого производилась настройка, клонируется в данное поле и будет использоваться при обращении к беспроводной сети.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

5.4 Режим работы AP Bridge: Точка - Точка



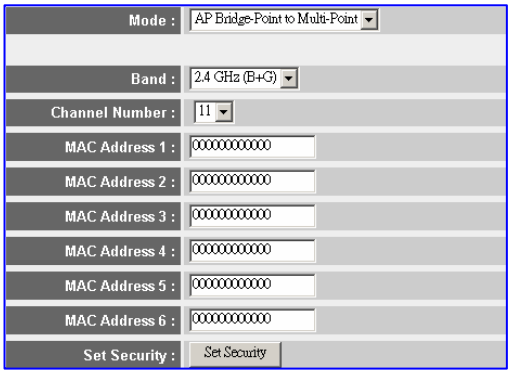
Этот режим позволяет соединить две проводные локальные сети через беспроводной мост. В этом режиме работы беспроводные клиенты (беспроводные устройства в режимах Ad-Hoc и Infrastructure) не смогут подключаться к точке доступа, так как она работает только как прозрачный мост и настраивается на удаленную точку доступа работающую в аналогичном режиме. Достоинством такого режима работы является использование всей доступной пропускной способности беспроводного канала для связывания двух локальных сетей.

Обязательным условием нормальной работы беспроводного моста является установка на другой стороне точки доступа поддерживающий этот режим. Для создания беспроводного моста рекомендуется использовать точки доступа одного производителя. Рекомендуемые модели точек доступа Planet WAP-4033 или WAP-4035. В этом режиме рекомендуется использовать внешние направленные антенны, подключенные вместо штатной антенны, для улучшения качества сигнала и снижения наводок.

Параметр	Описание
Mode (Режим работы)	Для этого режима следует выбрать **AP Bridge - Point to Point**
Band (вид поддержки беспроводных клиентов стандартов 802.11b/g)	Выберите режим работы в зависимости от используемого у Вас беспроводного оборудования. **2.4GHz (B):** разрешено подключение беспроводных клиентов только стандарта 802.11b. **2.4GHz (G):** разрешено подключение беспроводных клиентов только стандарта 802.11g. **2.4GHz (B+G):** совмещенный режим. Разрешено подключение беспроводных клиентов стандартов 802.11b/g одновременно. При одновременном подключении клиентов 802.11b и 802.11g неизбежно произойдет снижение пропускной способности для всех подключенных клиентов. Поэтому этот режим рекомендуется использовать только при наличии в беспроводных клиентов не поддерживающих 802.11g.
Channel Number (Номер канала)	Если в зоне действия Вашей беспроводной сети есть другие сети, то измените номер канала так, чтобы они оказывали друг на друга минимальное воздействие. Точка доступа позволяет использовать каналы с 1 по13. В стандарте 802.11b/g реально существует всего три канала оказывающих друг на друга минимальное воздействие. Это 1, 6 и 11 каналы. Если вы обнаружили беспроводные сети в зоне действия вашей сети или вам нужно сделать несколько беспроводных сетей с пересекающимися радиусами действия, то старайтесь использовать один из указанных каналов (не используемых в других беспроводных сетях). Этим Вы сможете снизить взаимные помехи беспроводных сетей друг на друга. Условие справедливо только в случае использования в соседних беспроводных сетях одного или двух из трех перечисленных каналов.
MAC Address 1	Сюда необходимо ввести **MAC** адрес точки доступа, с которой будет настроен беспроводной мост.
Set Security (Настройка защиты)	Для защиты беспроводного моста рекомендуется использовать шифрование. Чтобы выполнить настройку шифрования нажмите кнопку Set Security и обратитесь к разделу 5.7 “Настройка шифрования для режима моста”.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

5.5 Режим работы AP Bridge: Точка - Много точек



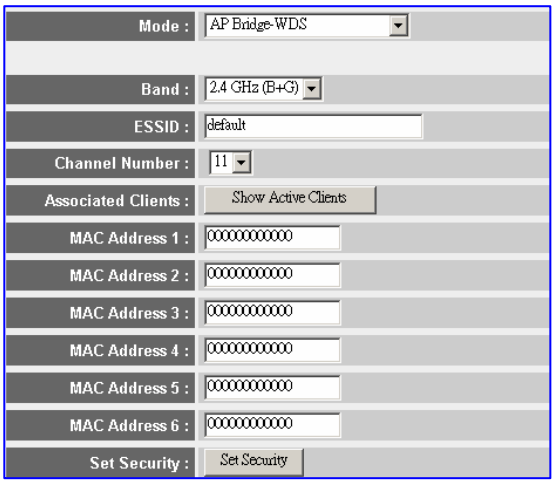
Этот режим позволяет соединить до шести проводных локальных сетей через беспроводные мосты. В этом режиме работы беспроводные клиенты (беспроводные устройства в режимах Ad-Hoc и Infrastructure) не смогут подключаться к точке доступа, так как она работает только как прозрачные мосты и настраивается на удаленные точки доступа, работающие в аналогичном режиме. Достоинством такого режима работы является использование всей доступной пропускной способности беспроводного канала для связывания локальных сетей.

Обязательным условием нормальной работы беспроводного моста является установка на другой стороне точки доступа поддерживающий этот режим. Для создания беспроводного моста рекомендуется использовать точки доступа одного производителя. Рекомендуемые модели точек доступа Planet WAP-4033 или WAP-4035. В этом режиме рекомендуется использовать внешние направленные или секторные антенны, подключенные вместо штатной антенны, для улучшения качества сигнала и снижения наводок.

Параметр	Описание
Mode (Режим работы)	Для этого режима следует выбрать **AP Bridge - Point to Multi-Point**
Band (вид поддержки беспроводных клиентов стандартов 802.11b/g)	Выберите режим работы в зависимости от используемого у Вас беспроводного оборудования. **2.4GHz (B):** разрешено подключение беспроводных клиентов только стандарта 802.11b. **2.4GHz (G):** разрешено подключение беспроводных клиентов только стандарта 802.11g. **2.4GHz (B+G):** совмещенный режим. Разрешено подключение беспроводных клиентов стандартов 802.11b/g одновременно. При одновременном подключении клиентов 802.11b и 802.11g неизбежно произойдет снижение пропускной способности для всех подключенных клиентов. Поэтому этот режим рекомендуется использовать только при наличии в беспроводных клиентов не поддерживающих 802.11g.
Channel Number (Номер канала)	Если в зоне действия Вашей беспроводной сети есть другие сети, то измените номер канала так, чтобы они оказывали друг на друга минимальное воздействие. Точка доступа позволяет использовать каналы с 1 по13. В стандарте 802.11b/g реально существует всего три канала оказывающих друг на друга минимальное воздействие. Это 1, 6 и 11 каналы. Если вы обнаружили беспроводные сети в зоне действия вашей сети или вам нужно сделать несколько беспроводных сетей с пересекающимися радиусами действия, то старайтесь использовать один из указанных каналов (не используемых в других беспроводных сетях). Этим Вы сможете снизить взаимные помехи беспроводных сетей друг на друга. Условие справедливо только в случае использования в соседних беспроводных сетях одного или двух из трех перечисленных каналов.
MAC Address 1-6	Сюда необходимо ввести **MAC** адреса точек доступа, с которыми будут настроены беспроводные мосты.
Set Security (Настройка защиты)	Для защиты беспроводного моста рекомендуется использовать шифрование. Чтобы выполнить настройку шифрования нажмите кнопку Set Security и обратитесь к разделу 5.7 “Настройка шифрования для режима моста”.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

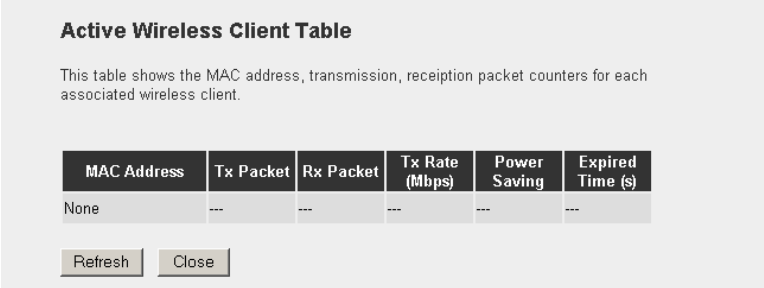
5.6 Режим работы AP Bridge - WDS (совмещенный режим)



Этот режим позволяет соединить до шести проводных локальных сетей через беспроводные мосты и одновременно подключать беспроводных клиентов (беспроводные устройства в режиме Infrastructure). Достоинством такого режима работы является использование одного устройства как для организации беспроводных мостов, так и использование её в качестве обычной точки доступа (режим AP). Недостатком данного режима работы является значительное снижение пропускной способности (примерно вдвое).

Обязательным условием нормальной работы беспроводного моста является установка на другой стороне точки доступа поддерживающий этот режим. Для создания беспроводного моста рекомендуется использовать точки доступа одного производителя. Рекомендуемые модели точек доступа Planet WAP-4033 или WAP-4035. В этом режиме рекомендуется использовать внешние направленные или секторные антенны, подключенные вместо штатной антенны, для улучшения качества сигнала и снижения наводок.

Параметр	Описание
Mode (Режим работы)	Для этого режима следует выбрать **AP Bridge - WDS**

Параметр	Описание
Band (вид поддержки беспроводных клиентов стандартов 802.11b/g)	Выберите режим работы в зависимости от используемого у Вас беспроводного оборудования. **2.4GHz (B):** разрешено подключение беспроводных клиентов только стандарта 802.11b. **2.4GHz (G):** разрешено подключение беспроводных клиентов только стандарта 802.11g. **2.4GHz (B+G):** совмещенный режим. Разрешено подключение беспроводных клиентов стандартов 802.11b/g одновременно. При одновременном подключении клиентов 802.11b и 802.11g неизбежно произойдет снижение пропускной способности для всех подключенных клиентов. Поэтому этот режим рекомендуется использовать только при наличии в беспроводных клиентов не поддерживающих 802.11g.
ESSID (Идентификатор беспроводной сети)	ESSID (до 32-х печатных символов ASCII) это уникальное имя, сопоставленное данной беспроводной сети. Идентификатор предотвращает случайное объединение двух пересекающихся беспроводных локальных сетей. Пожалуйста, удостоверьтесь, что установили одинаковые идентификаторы ESSID для всех клиентов в Вашей сети WLAN. Значение по умолчанию "**default**" рекомендуется изменить на уникальное имя.
Channel Number (Номер канала)	Если в зоне действия Вашей беспроводной сети есть другие сети, то измените номер канала так, чтобы они оказывали друг на друга минимальное воздействие. Точка доступа позволяет использовать каналы с 1 по13. В стандарте 802.11b/g реально существует всего три канала оказывающих друг на друга минимальное воздействие. Это 1, 6 и 11 каналы. Если вы обнаружили беспроводные сети в зоне действия вашей сети или вам нужно сделать несколько беспроводных сетей с пересекающимися радиусами действия, то старайтесь использовать один из указанных каналов (не используемых в других беспроводных сетях). Этим Вы сможете снизить взаимные помехи беспроводных сетей друг на друга. Условие справедливо только в случае использования в соседних беспроводных сетях одного или двух из трех перечисленных каналов.
MAC Address 1-6	Сюда необходимо ввести **MAC** адреса точек доступа, с которыми будут настроены беспроводные мосты.
Set Security (Настройка защиты)	Для защиты беспроводного моста рекомендуется использовать шифрование. Чтобы выполнить настройку шифрования нажмите кнопку Set Security и обратитесь к разделу 5.7 "Настройка шифрования для режима моста".
Associated Clients (Подключенные беспроводные клиенты)	Для просмотра информации о подключенных беспроводных клиентах нажмите кнопку **Show Active Clients**. Откроется окно показанное ниже.  Для обновления информации нажмите **Refresh**, чтобы закрыть окно нажмите **Close**.

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

5.7 Настройка шифрования для режима моста

Для режимов работы **Bridge-Point to Point**, **Bridge-Point to Multi-Point** и **Bridge-WDS** режим шифрования настраивается в этом окне, а не в меню ***Advanced Setting***. Нажмите кнопку **Set Security,** выберите тип шифрования и произведите необходимые настройки.

Внимание!!!

В режимах беспроводных мостов нельзя использовать идентификацию **WPA RADIUS и 802.1x**!!!

Параметр	Описание
Encryption (шифрование)	В данном случае необходимо выбрать один из доступных видов шифрования: **WEP 64bits**, **WEP 128bits**, **WPA (TKIP)** или **WPA2 (AES).** По умолчанию шифрование не используется.
WEP Key Format (формат ключа)	Вы можете выбрать между ASCII символами (буквенно-цифровай формат) или Hex (шестнадцатеричный формат представления данных) В HEX формате вы можете использовать буквы латинского алфавита от A до F и числа от 0 до 9 для ввода ключа. Чтобы перевести значение ключа ASCII в HEX можно воспользоваться программой просмотра или редакторами умеющими показывать данные в шестнадцатеричном формате. Например, можно использовать Windows Commander. Данные введенные в HEX и аналогичный ему ключ в ASCII являются аналогами.

Параметр	Описание
WEP Key (ключ шифрования)	В это поле необходимо ввести ключ, с помощью которого будет осуществляться шифрование данных: 64-х битный ключ: введите 10-ти значное Hex значение (допустимые символы “A-F”, “a-f” и “0-9”) или 5 символов ASCII 128-х битный ключ: введите 26-ти значное Hex значение (допустимые символы “A-F”, “a-f” и “0-9”) или 10 символов ASCII.
Enable 802.1x Authentication	для использования идентификации по RADIUS (802.1x) пожалуйста, поставьте галочку в поле, " Enable 802.1x Authentication ” и обратитесь к разделу **4.4.3.2** для детального ознакомления с параметрами настройки
Pre-shared Key Format	Вы можете выбрать между ASCII символами (буквенно-цифровай формат) или Hex (шестнадцатеричный формат представления данных) В HEX формате вы можете использовать буквы латинского алфавита от A до F и числа от 0 до 9 для ввода ключа. Чтобы перевести значение ключа ASCII в HEX можно воспользоваться программой просмотра или редакторами умеющими показывать данные в шестнадцатеричном формате. Например, можно использовать Windows Commander. Данные введенные в HEX и аналогичный ему ключ в ASCII являются аналогами.
Pre-shared Key	В эти поля необходимо ввести ключи, с помощью которых будет осуществляться шифрование данных 64-х битное Hex значение ключа (допустимые символы “A-F”, “a-f” и “0-9”) или минимум 8 символов ASCII (не рекомендуется вводить ключ длиной больше 20 ASCII символов, так как длинный ключ может существенно замедлить работу маршрутизатора)

*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

Часть 6 Состояние Устройства (Status)

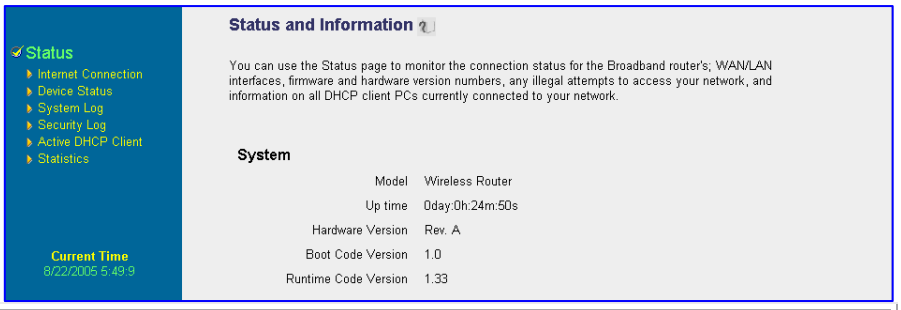
Раздел Status позволяет оперативно получать информацию о текущем состоянии интерфейсов и служб маршрутизатора, просматривать системный лог и лог межсетевого экрана о предпринятых попытках атак, подключенных DHCP клиентах, статистику пакетов и общую информацию о версии ПО и времени работы с момента последней перезагрузки.

Наименование раздела	Описание
6.1 Status	Общая информация о роутере (модель роутера, версия загрузчика, версия ПО, аппаратная версия, время непрерывной работы)
6.2 Internet Connection	Информация о типе используемого подключения для порта WAN и его текущие настройки
6.3 Device Status	Информация о настройках порта LAN
6.4 System Log	Информация системного журнала
6.5 Security Log	Информация о попытках любых зафиксированных атак на маршрутизатор
6.6 DHCP Client Table	Информация об активных DHCP клиентах
6.7 Statistics	Статистика принятых и отправленных пакетов

Выберите нужный пункт меню и перейдите к его подробному описанию

6.1 Состояние (Status)

При нажатии на кнопку STATUS в верхнем правом углу экрана откроется меню с общей информацией о роутере (модель роутера, версия загрузчика, версия ПО, аппаратная версия, время непрерывной работы)



Параметр	Описание
Uptime	Время непрерывной работы с момента последней перезагрузки
Hardware Version	Аппаратная версия
Boot Code Version	Версия загрузчика
Runtime Code Version	Версия Программного обеспечения

6.2 Подключение к Интернет (Internet Connection)

Информация о типе используемого подключения для порта WAN и его текущие настройки. Если роутер использует Static IP, то будут показаны настройки, сделанные для WAN порта. Если используется любой другой тип подключения (DHCP client, PPPoE, PPTP, L2TP), то настройки будут показаны только при наличии подключения к серверу.

Attain IP Protocol :	PPTP connected
IP Address :	192.168.10.172
Subnet Mask :	255.255.255.255
Default Gateway :	192.168.200.250
MAC Address :	00:11:2F:E3:DB:58
Primary DNS :	192.168.200.250
Secondary DNS :	193.178.158.1

Параметр	Описание
Attain IP Protocol	Протокол, используемый для подключения к Интернет провайдеру
IP Address	IP адрес WAN порта маршрутизатора
Subnet Mask	Маска подсети
Default Gateway	Шлюз по умолчанию (Интернет провайдера)
MAC Address	MAC адрес WAN порта маршрутизатора
Primary DNS	IP адрес первичного DNS сервера провайдера
Secondary DNS	IP адрес резервного DNS сервера провайдера

6.3 Состояние интерфейсов устройства (Device Status)

Информация о настройках проводного (LAN) и беспроводного (WLAN) интерфейса, которые были сделаны в соответствующих разделах при настройке маршрутизатора.

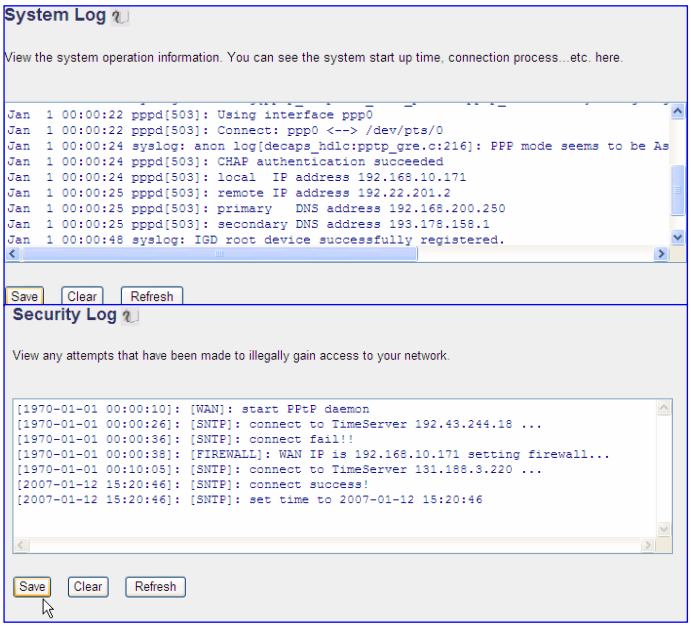
Wireless Configuration	
Mode	AP
ESSID	default
Channel Number	11
Security	Disable
Associated Clients	0
BSSID	00:30:4f: 78:87:88
LAN Configuration	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Disabled
MAC Address	00:30:4f: 78:87:88

Параметр	Описание
Конфигурация Беспроводного интерфейса (Wireless Configuration)	
Mode	Установленный режим работы (Access Point, Station - Ad-Hoc, Station – Infrastructure, Bridge - Point to Point, Bridge - Point to MultiPoint, Bridge - WDS)
ESSID	Идентификатор беспроводной сети
Channel Number	Номер беспроводного канала
Security	Используемое шифрование данных
Associated Clients	Число подключенных беспроводных клиентов
BSSID	MAC адрес беспроводного адаптера
Конфигурация Проводного интерфейса (LAN Configuration)	
IP Address	IP адрес LAN порта маршрутизатора (для устройств в локальной сети это шлюз по умолчанию)
Subnet Mask	Маска подсети
DHCP Server	Состояние встроенного DHCP сервера (включен или выключен)
MAC Address	MAC адрес LAN порта маршрутизатора

6.4 Системный журнал System Log

В этом журнале фиксируются все системные события. Вы можете сохранить эту информацию на жестком диске компьютера, нажав кнопку Save и указав директорию и Имя файла для сохранения. Кнопка Clear позволяет очистить лог. Кнопка Refresh обновляет информацию лога.

Внимание!: Информация лога хранится только до перезагрузки устройства. После перезагрузки вся информация будет потеряна.

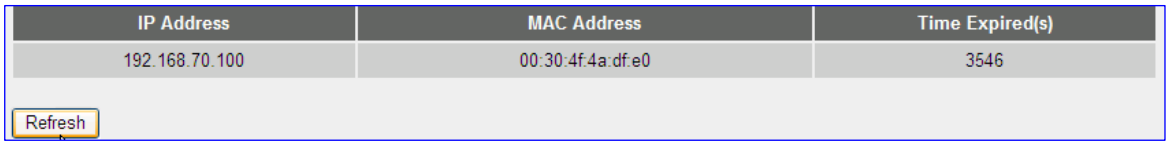


6.5 Журнал Защиты (Security Log)

Здесь фиксируются все события о попытках атак и попыток сканировании портов маршрутизатора, а также информация о работе межсетевого экрана и SNTP сервера. Вы можете сохранить эту информацию на жестком диске компьютера, нажав кнопку Save и указав директорию и Имя файла для сохранения. Кнопка Clear позволяет очистить лог. Кнопка Refresh обновляет информацию лога.

6.6 Таблица активных DHCP клиентов (Active DHCP Client)

Информация об активных DHCP клиентах.

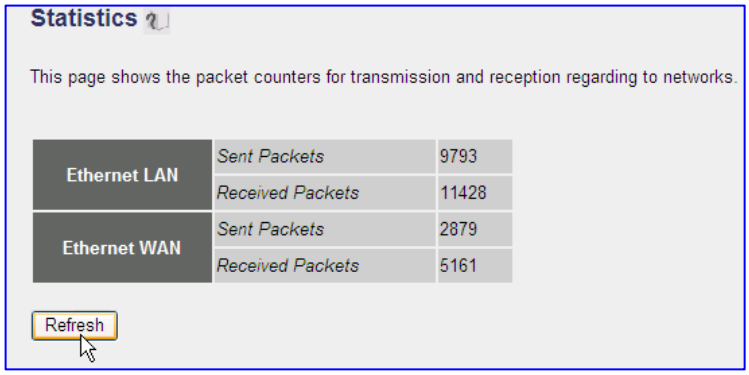


IP Address	MAC Address	Time Expired(s)
192.168.70.100	00:30:4f:4a:df:e0	3546

Refresh

6.7 Статистика (Statistics)

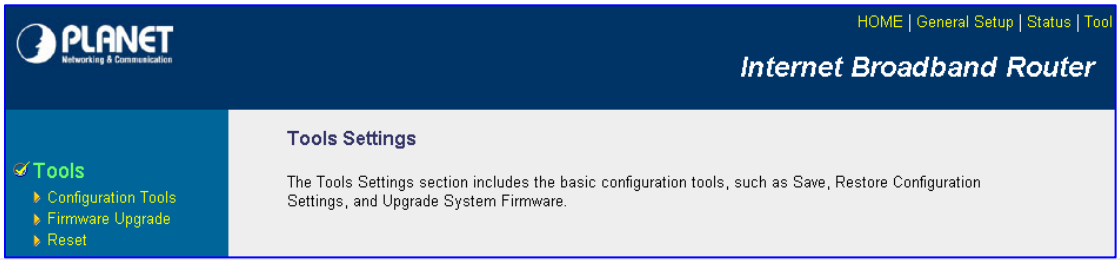
Статистика о принятых и отправленных пакетах для интерфейсов WAN и LAN.



Часть 7 Расширенное Администрирование (Tools)

Раздел расширенного администрирования позволяет выполнить ряд дополнительных служебных функций. Пользоваться этими возможностями рекомендуется только подготовленным пользователям, так как ошибочные действия могут привести к неправильной работе маршрутизатора или к его повреждению (особенно это касается раздела меню Firmware Upgrade).

В этом разделе можно выполнить сохранение настроенной конфигурации и восстановление ранее сохраненной конфигурации; обновить программное обеспечение сбросить все настройки роутера на значения по умолчанию и произвести принудительную перезагрузку роутера.



Параметр	Описание
7.1 Сохранение конфигурации	В этом разделе меню можно выполнить сохранение и восстановление конфигурации, а также выполнить сброс всех настроек роутера на значения по умоланию.
7.2 Обновление прошивки	В этом разделе описана процедура обновления программного обеспечения роутера
7.4 Нестабильная работа	В этом разделе дано краткое описание решения проблем со стабильностью работы
7.4 Аппаратный Сброс	В этом разделе описана процедура принудительной перезагрузки роутера.

Выберите нужный пункт меню и перейдите к его подробному описанию

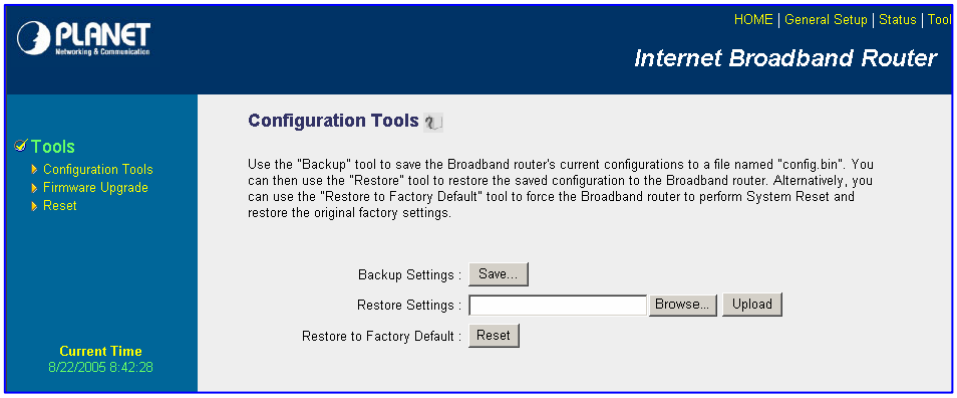
7.1 Инструмент Конфигурация (Configuration Tools)

Для сохранения настроенной конфигурации используйте **Backup Setting**. Нажмите кнопку **Save** и выберите диск, папку и имя файла под которым Вы хотите сохранить текущую конфигурацию. Сохранение конфигурации позволит вам быстро восстановить настройки в случае возникновения проблем с проблем с работой оборудования или после сброса настроек. Также эта функция очень удобна при необходимости периодически изменять конфигурацию оборудования.

Для восстановления ранее сохраненной конфигурации используйте **Restore Setting**. Нажмите кнопку **Browse…** и выберите диск, папку и имя файла под которым Вы ранее сохранили конфигурацию. Нажмите кнопку **Upload**. Маршрутизатор загрузит выбранную конфигурацию и автоматически перезагрузится.

Секция **Restore to Factory Defaults** позволяет сбросить все настройки роутера на фабричные значения по умолчанию. Для сброса настроек нажмите кнопку **Reset** и на запрос роутера о подтверждении выбранного действия нажмите кнопку **OK**. Маршрутизатор сбросит все настройки и автоматически перезагрузится.

Внимание!: Во время восстановления конфигурации и сброса настроек нельзя выключать питание маршрутизатора и выполнять отключение и подключение интерфейсных кабелей! Дождитесь окончания процедуры восстановления конфигурации или сброса настроек.

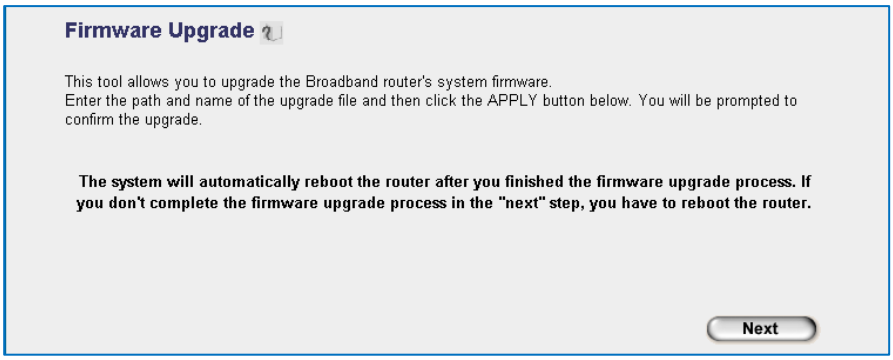


*Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.*

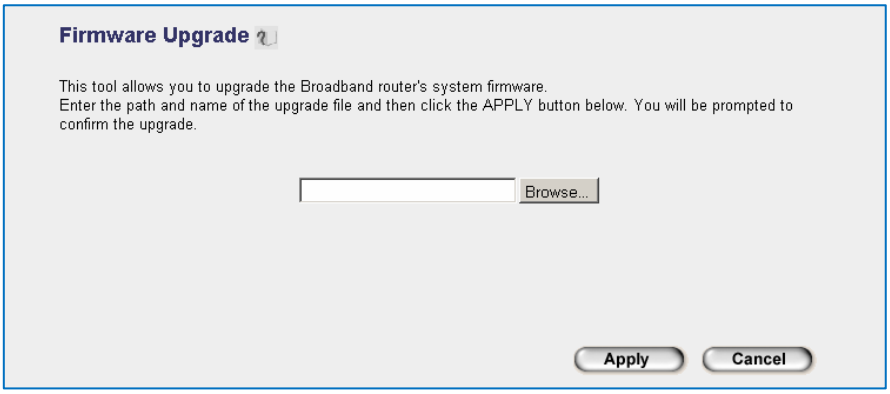
7.2 Обновление прошивки (Firmware Upgrade)

В этом разделе вы сможете обновить программное обеспечение роутера. Для обновления прошивки выполните следующие действия:

- Загрузите архив с прошивкой с FTP производителя оборудования и сохраните его на локальном диске
- Разархивируйте загруженный файл.
- Откройте раздел **Firmware Upgrade** и нажмите **Next**



- Нажмите кнопку Обзор и выберите файл с прошивкой (расширение bin)



- Нажмите **Apply**. Появится всплывающее окно с требованием подтвердить выбранное действие.
- Нажмите **Ok** – запустится процедура обновления прошивки.

Внимание!:

- Во время обновления программного обеспечения маршрутизатора нельзя выключать питание и выполнять отключение и подключение интерфейсных кабелей! Дождитесь окончания процедуры обновления прошивки.
- При обновлении прошивки желательно обеспечить бесперебойное питание маршрутизатора и компьютера, с которого осуществляется загрузка нового программного обеспечения. Компьютер желательно подключить к маршрутизатору напрямую, избегая промежуточных коммутаторов.
- Не рекомендуется (хотя это возможно) удаленное обновление программного обеспечения маршрутизатора.
- Обязательно убедитесь, что загружаете именно тот файл с программным обеспечением, который предназначен для вашего маршрутизатора.
- До обновления программного обеспечения желательно сохранить настроенную конфигурацию в файл и сбросить настройки роутера на значения по умолчанию. В последствии загрузите сохраненную конфигурацию.
- Нельзя обновлять прошивку оборудования, если маршрутизатор работает нестабильно (периодически зависает). За дополнительной информацией обратитесь к разделу 7.3

Соблюдение этих правил позволит избежать проблем при обновлении программного обеспечения роутера.

7.3 Решение проблем с нестабильной работой

Если Ваше оборудование вдруг стало работать нестабильно, то выполните следующие действия:

- Попробуйте перезагрузить маршрутизатор.
- Уточните у провайдера об отсутствии проблем с подключением.
- Проверьте правильность настроек.

- Убедитесь в отсутствии на компьютерах вирусов и вредоносных программ. Такие программы могут инициировать флуд (массовую рассылку пакетов), что может вызывать срабатывание Межсетевого экрана, который заблокирует подключение к Интернет. Описание термина флуд смотрите в Глоссарии сетевых терминов.
- Убедитесь в исправности сетевых адаптеров, кабелей, разъёмов, соединителей и их правильном и надежном подключении.
- Проверьте источник питания и напряжение в сети
- Попробуйте сбросить все настройки и ввести их заново
- Обратите внимание на температурный режим. Оборудование нельзя устанавливать в теплых местах (на батареи отопления или оборудование, нагревающееся при работе) и в местах, где возможно прямое попадание солнечных лучей.
- Обратите внимание на вентиляцию. Нельзя закрывать вентиляционные отверстия на корпусе оборудования.
- Обратите внимание на настройки ключей шифрования для беспроводного интерфейса (при использовании WPA). Если вы ввели ключ длиннее 20 символов, то работа маршрутизатора может существенно замедлиться.

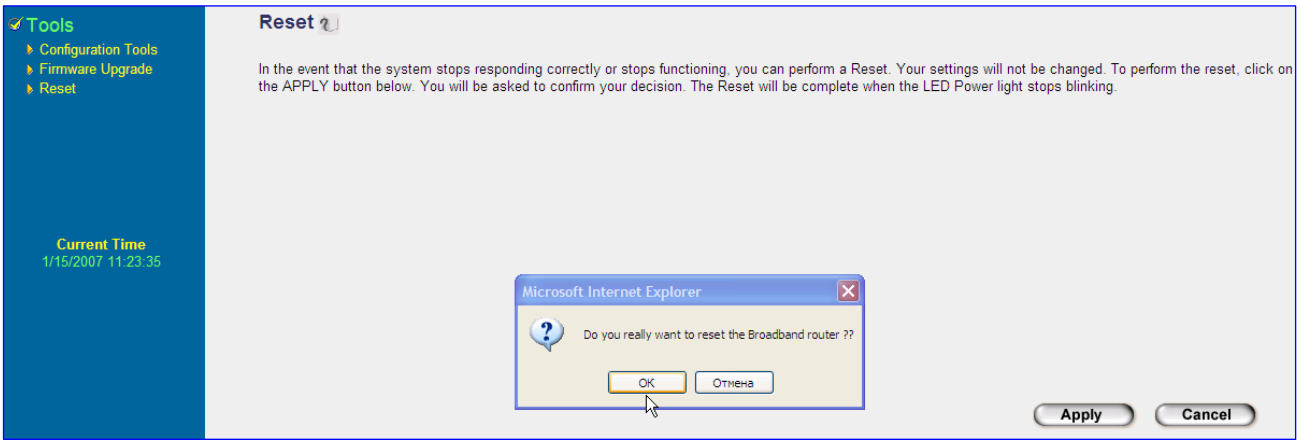
Если ни одно из вышеописанных действий не помогло, то рекомендуется обратиться в сервисный центр.

Внимание!:

- Нельзя обновлять прошивку оборудования, если маршрутизатор работает нестабильно (периодически зависает).

7.4 Сброс (Reset)

Если в работе оборудования возникли проблемы, то можно перезагрузить маршрутизатор через WEB интерфейс.



Откройте меню **Reset** и нажмите **Apply**. Появится окно с подтверждением действия. Нажмите **OK**. Маршрутизатор прервет все текущие подключения и выполнит перезагрузку.

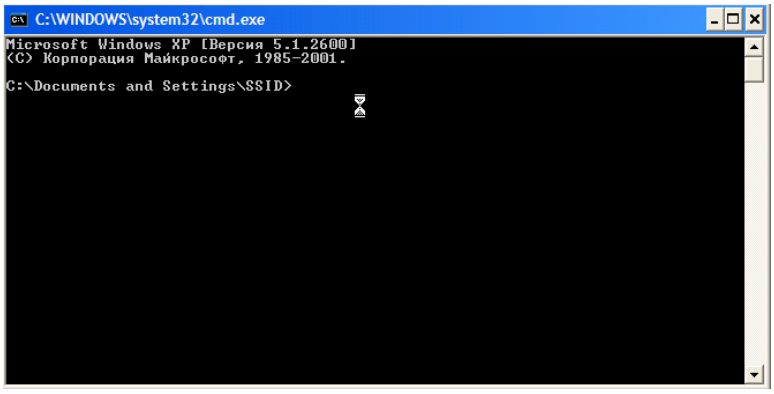
Внимание!:

- Все настройки, сделанные Вами на маршрутизаторе не изменятся! Этот режим позволяет просто перезагрузить маршрутизатор.
- Аналогичное действие можно выполнить, нажав кратковременно кнопку Reset (меньше 4-х секунд) на задней стенке маршрутизатора.

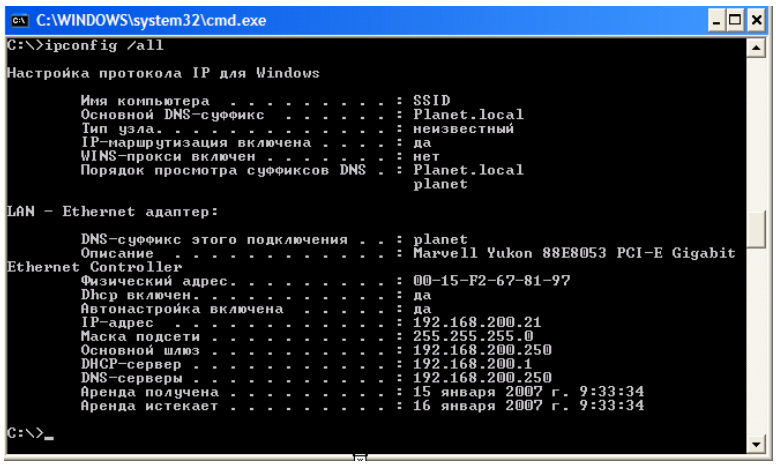
Приложение A CMD (Консоль)

Как посмотреть в Windows MAC и IP адрес сетевого подключения Вашего компьютера и другие параметры сетевого подключения?

1) откройте окно командной строки (Пуск ⇨ Выполнить… ⇨ cmd ⇨ нажмите Enter)



2) наберите **ipconfig /all** и нажмите **Enter**



- IP адрес Вашего компьютера это строка **IP-адрес** (192.168.200.21)
- Маска подсети 255.255.255.0
- Шлюз по умолчанию (Default Gateway) для вашего подключения это строка **Основной шлюз** (192.168.0.1)
- MAC адрес Вашего компьютера (Physical Address) это строка **Физический адрес** (00-15-F2-67-81-97)

Приложение B Часто задаваемые вопросы (FAQ)

Вопрос: Можно ли запускать программы через беспроводную сеть?

Ответ: Если приложение предназначено для работы через локальную сеть (например, сетевая версия 1С), что подразумевает сетевую версию программы, то никаких проблем нет, так как беспроводная сеть является фактически продолжением вашей локальной сети. Для получения этой информации обратитесь к руководству пользователя по данной программе.

Вопрос: Можно ли запускать сетевые игры, чтобы совместно играть с другими пользователями моей беспроводной и проводной локальной сети?

Ответ: Да, если игра поддерживает сетевой режим. Для получения этой информации обратитесь к руководству пользователя по данной игре.

Вопрос: Что такое стандарт IEEE 802.11g?

Ответ: стандарт беспроводной связи 802.11g, который позволяет передавать данные на скоростях до 54 Мбит в секунду, что почти в 5 раз быстрее нынешнего 802.11b. При этом 802.11g будет совместим с более старыми беспроводными технологиями, что позволит компаниям и пользователям не менять оборудование и, возможно, увеличить количество беспроводных соединений как дома, так и в офисах. Новый стандарт, как и нынешний 802.11b работает на частоте в 2.4 ГГц, что позволяет сделать стандарты совместимыми, в отличие от 802.11a, который использует диапазон 5ГГц.

Вопрос: Какие возможности IEEE 802.11 реализованы в изделии?

Ответ: Изделие поддерживает функции IEEE 802.11:

- Протокол CSMA/CA plus Acknowledge
- Многоканальный Роуминг (Multi-Channel Roaming)
- Автоматический выбор скорости (Automatic Rate Selection)
- RTS/CTS
- Фрагментация (Fragmentation)
- Управление питанием (Power Management)

Вопрос: Что такое Роуминг?

Ответ: В соответствии с предварительной спецификацией стандарта IEEE 802.11f представляет собой протокол обмена служебной информацией между точками доступа (Inter-Access Point Protocol, IAPP), что необходимо для построения распределенных беспроводных сетей передачи данных.

Если в Вашей беспроводной сети работает несколько точек доступа, то при включении этой функции они смогут обмениваться информацией о подключенных беспроводных клиентах, что позволит организовать роуминг в вашей беспроводной сети и прозрачно подключать клиентов при переходе в зону действия другой точки доступа. Перед включением роуминга необходимо убедиться, что в предполагаемой зоне перемещения мобильного пользователя все Точки Доступа и Мобильный пользователь используют одинаковые номера каналов, идентификаторы, находятся в одной локальной сети (LAN) и т.п..

Вопрос: Сможет мой компьютер с беспроводной карточкой подключиться к точке доступа WRT-414 при работе её в режиме WDS?

Ответ: Да, режим WDS подразумевает работу точки доступа в совмещенном режиме, что позволяет как организовывать беспроводные мосты, так и одновременно подключать беспроводных клиентов работающих в режиме Инфраструктура (Infrastructure). Обратите внимание, что при подключении в качестве беспроводного клиента в режиме WDS вы потеряете примерно 50% пропускной способности канала. Это правила также справедливо для режима Повторитель (Repeater) на обычных точках доступа (например, WAP-4033,4035).

Вопрос: Почему реальная скорость передачи данных сильно отличается от указанной на упаковке?

Ответ: Пропускная способность - это количество бит переданных из одного места в другое за определённый промежуток времени. Для беспроводного сетевого оборудования обычно измеряется в мегабитах в секунду (Мбит/с). Значение указанное на упаковке показывает "сырую" скорость с учётом всех служебных данных. Вполне естественно, на практике таких значений вы никогда не получите. На упаковке указывается скорость канала передачи данных, которая включает в себя помимо самого трафика большое количество служебных пакетов информации, непрерывная передача которых необходима для обеспечения работы беспроводной сети. В таблице показана скорость канала и ориентировочная (максимально достижимая) реальная скорость передачи данных для разных стандартов беспроводной связи:

Протокол	Частотный диапазон	Max Tx Rate	Max Transmit rate
802.11a	5 ГГц	54 Mbps	22-25 Mbps
802.11b	2.4 ГГц	11 Mbps	5.7 Mbps
802.11g	2.4 ГГц	54 Mbps	22-25 Mbps

Max Tx Rate - скорость подключения радио
Max Transmit rate – ориентировочная максимально возможная скорость передачи данных

Список терминов

A

Access Point (Точка Доступа) - устройство

Точка доступа обеспечивает прозрачное подключение беспроводных клиентов (Беспроводные сетевые адаптеры, телефоны, камеры и т.п.) для объединения их в единую локальную сеть, включающую в себя беспроводных (WLAN) и проводных (LAN) клиентов с возможностью совместного использования ресурсов такой локальной сети. Фактически для беспроводных клиентов точка доступа является преобразователем среды передачи данных (из WLAN в LAN) и коммутатором для подключенных беспроводных клиентов (направляя пакеты данных нужному узлу). Беспроводные пользователи могут свободно перемещаться в зоне действия такой беспроводной сети.

Access Point (Точка Доступа) – режим работы

Этот режим работы подразумевает подключение беспроводных клиентов (Беспроводные сетевые адаптеры, телефоны, камеры и т.п.) работающих в режиме Инфраструктура (Infrastructure).

Administrator Network (Администратор сети)

Сетевой администратор – это человек, который управляет локальной сетью в пределах организации. Работа администратора заключается в обеспечении гарантированной защиты сети, её модернизации и конфигурировании, наблюдение за сетевой активностью пользователей, разрешении и предотвращении конфликтов в сетевом окружении, резервном копирование баз данных и другой информации, контроль за состоянием аппаратных средств и программного обеспечения на современном уровне и другие аспекты, зависящие от специфики обслуживаемой сети и задач.

Authentication (Установление подлинности, Идентификация)

Идентификация используется для проверки целостности передаваемого сообщения или подтверждения прав пользователя, сервиса устройства на получения доступа к тем или иным ресурсам.

B

Broadcast (Широковещание)

Система доставки пакетов, при которой копия каждого пакета передается всем хостам, подключенным к сети. Примером широковещательной сети является Ethernet. См. также multicast. Передача сообщения всем "слушающим " адресатам.

Beacon Interval (Радиомаяк, Интервал Маячка)

Точки доступа периодически подают сигналы с целью синхронизации подключенных к ним беспроводных устройств и оценки качества сигнала. Вы можете установить периодичность подачи сигнала в пределах от 20 до 1024 миллисекунд. По умолчанию используется период длиной 100 миллисекунд.

Bridge (Мост)

интеллектуальное устройство, соединяющее две локальные сети или удаленные сегменты в одну сеть. Функционирует на подуровне MAC канального уровня и прозрачен для протоколов боле высоких уровней, т. е. принимает решение о передаче кадра из одного сегмента в другой только на основании информации из заголовка канального уровня, в частности физического (MAC) адреса получателя. Кадры, предназначенные для станции из того же сегмента, не передаются через мост.

X

Client (клиент)

Компьютерная система или процесс, запрашивающий сервис у другой системы или процесса (например, рабочая станция, использующая файлы с сервера) См. также **Server**.

CTS (Clear to Send)

это сигнал управления последовательным устройством, передаваемый от DCE (устройство передачи данных) к DTE (терминальное оборудование) и показывающий, что DTE может продолжать передачу данных.

CRC (циклическая проверка четности с избыточностью)

методика определения ошибок на этапе передачи данных. На основе полиномиального алгоритма вычисляется контрольная сумма передаваемого модуля данных и передается вместе с данными. Получившее пакет устройство заново вычисляет контрольную сумму по тому же алгоритму и сравнивает ее с принятым значением. Отсутствие расхождений говорит о высокой вероятности безошибочной передачи данных.

Δ

Default Gateway (Шлюз используемый по умолчанию, Основной шлюз)

шлюз, используемый по умолчанию, соединяющий две или более сети или подсети и позволяющий передавать данные из одной сети в другую. Используемый по умолчанию шлюз является маршрутизатором для локальной подсети.

DHCP (Dynamic Host Configuration Protocol - протокол динамической настройки хостов)

протокол динамического конфигурирования хостов, обеспечивающий передачу конфигурационных параметров клиентам TCP/IP. Протокол DHCP является усовершенствованием BootP и добавляет к этому протоколу возможность повторного использования IP-адресов и ряд новых функций - маски подсетей, используемые по умолчанию маршрутизаторы, серверы DNS.

DMZ (демилитаризованная зона)

Серверы общего доступа в отдельной сети. Фактически это отдельная зона или подсеть к ресурсам который можно обеспечить неограниченный доступ из Внешней сети (Интернет).

DNS (Domain Name System - система доменных имен)

Несмотря на то что каждый сетевой интерфейс компьютера имеет свой собственный IP адрес, пользователи привыкли работать с именами хостов. Существует распределенная мировая база данных TCP/IP, называемая системой имен доменов (DNS - Domain Name System), которая позволяет установить соответствие между IP адресами и именами хостов. Распределенный механизм имен и адресов, используемых в сети Интернет. Используется для преобразования логических имен в IP-адреса. Служба DNS используется в сети Интернет, обеспечивая возможность работы с понятными и легко запоминающимися доменными именами вместо неудобоваримых чисел IP-адреса.

DNS Server IP Address (IP адрес DNS Сервера)

Указывает на IP адрес сервера DNS который будет обрабатывать запросы к удаленным хостам по доменным именам, преобразуя их в IP адреса хостов. Информация о DNS сервере как правило предоставляется Вашим Интернет провайдером. **Например:** набранная в браузере строка http://www.yandex.ru/ (доменное имя сайта) на самом деле аналогична строке http://213.180.204.11/ . Если не указан DNS сервер, либо он в данный момент недоступен, или указан неправильно, то открыть сайт вы сможете, только введя его IP адрес.

Domain (Домен, область)

обозначает группу хостов сети. Деление на группы может осуществляться по физическим (местоположение в сети) или логическим (функциональное предназначение) критериям. В OSI термин домен используется как административное деление сложных распределенных систем, как в MHS Private Management Domain (PRMD) и Directory Management Domain (DMD). В сети Internet - часть иерархии имен. Синтаксически доменное имя Internet содержит последовательность имен (меток), разделенных точками (.) - например, peterburg.net

Domain Name (Доменное Имя)

адрес в интернете, который выдается через службу InterNIC, занимающуюся регистрацией адресов.

DSL Modem (DSL Модем)

DSL это стандарт в дословном переводе означающий Цифровая Абонентская линия (Digital Subscriber Line). DSL Модем предназначен для подключения к Интернет по высокоскоростной цифровой абонентской линии с использованием обычного медного телефонного кабеля.

E

Ethernet

Одна из самых первых технологий, имевшая чрезвычайно большой успех и до сих пор сохраняющая популярность. Разработана фирмами Xerox, Intel и DEC первоначально для передачи данных по коаксиальному кабелю со скоростью 10 Мбит/с (стандарты 10Base2 и 10Base5). Это стандарт организации локальных сетей (ЛВС), описанный в спецификациях IEEE и других организаций. IEEE 802.3. Ethernet использует полосу 10 Мбит/с и метод доступа к среде CSMA/CD. Развитием технологии Ethernet является Fast Ethernet (100 Мбит /сек) и Gigabit Ethernet (1000 Мбит /с). В настоящее время, подавляющее число инсталляций сетей Ethernet осуществляется по витой паре (100BaseT и IEEE802.3ab 1000Base-T) с тенденцией замены магистральных каналов и на Гигабитные и 10 Гигабитные. Кроме того, в качестве среды передачи может использоваться

Ф

Filter (Фильтр)

Это набор правил, которые позволяют разрешить или запретить прохождение определенных протоколов, данных или сервисов на уровне портов через маршрутизатор, которые могут быть применены как для определенного хоста, группы хостов или определенного сервиса или протокола. Например можно запретить соединение по протоколу FTP с определенными серверами или полностью запретить использование этого протокола как одному пользователю в локальной сети, так и всем пользователям одновременно.

Firewall (Брандмауэр или Межсетевой экран)

Означает сочетание программного и аппаратного обеспечения, образующее систему защиты, как правило, от несанкционированного доступа из внешней глобальной сети Интернет во внутреннюю локальную сеть (интрасеть).

Также это понятие можно трактовать как метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами.

Firmware (Встроенное Программное обеспечение оборудования, Прошивка)

Встроенное программное обеспечение расположено в энергонезависимой микросхеме памяти (BIOS ROM). Встроенное программное обеспечение предназначено для выполнения устройством всех возложенных на него функций, описанных в инструкции по эксплуатации, и сохранения сделанных пользователем настроек. Производитель может выпустить обновленную версию программного обеспечения, которая дополняет возможности оборудования и устраняет ошибки, найденные в предыдущей версии. Обновление программного обеспечения является очень ответственной процедурой, при которой есть риск повредить оборудование, поэтому следует строго следовать рекомендациям изготовителя по обновлению программного обеспечения и ознакомиться с информационным файлом (как правило находится в архиве с новой версией прошивки). Наиболее частая ошибка это загрузка прошивки в оборудование от устройства другой аппаратной версии (см. **Аппаратная Версия Устройства**)

Flood (Флуд) (от англ. "Наводнение").

В применении к Интернет этот термин означает переполнение сети путешествующими пакетами информации (фрагментами файлов, запросами и т.д.). Flood - один из способов вывести из строя сервер: он не справится с потоком запросов и остановится или даже выйдет из строя. Вариант такой атаки - многочисленные попытки войти на сервер. Пусть даже эти попытки безуспешны, но их количество может сыграть роковую роль.

Fragmentation (фрагментация)

Процесс деления пакетов или дейтаграмм IP на несколько мелких частей для выполнения требований данной физической сети. Обратный процесс называют дефрагментацией (reassembly). См. также **MTU**.

FTP (File Transfer Protocol, Протокол Передачи Файлов)

Протокол, используемый для копирования файлов с одного хоста на другой через сеть. Протокол FTP определен в STD9 и RFC 959. В локальных сетях FTP является протоколом совместного использования файлов, работающим на уровнях 5 - 7 эталонной модели OSI. Широко используемые в сети Internet протокол (и программа) передачи файлов между хост -компьютерами.

Г

Gateway (Шлюз)

Совокупность аппаратных и программных средств, которая позволяет обмениваться информационными потоками данных между несовместимыми сетями или приложениями. Типичный шлюз включает средства разборки/сборки пакетов, преобразования протоколов и конвертирования среды передачи данных. Такое устройство (или система) конвертирует при передаче данные так, чтобы они удовлетворяли требованиям получателя (сети или приложения или устройства). Шлюз часто используется как синоним узла или маршрутизатора, что является некорректной трактовкой термина! В современном варианте термины "gateway" и "application gateway" используются для обозначения систем, выполняющих преобразование из одного естественного формата в другой. Примером шлюза может служить преобразователь аналогового телефонного сигнала (ТФОП) в один из протоколов IP телефонии, то есть VoIP шлюз (например VIP-480).

GUI (Web-based management Graphical User Interface)

графический пользовательский интерфейс доступ к которому возможен с помощью обычного WEB браузера. Это метод взаимодействия между пользователем и интерфейсом активного сетевого оборудования (хоста), при котором пользователь может вызывать различные функции, указывая на графические элементы (кнопки) вместо ввода команд с клавиатуры.

Н

HOST (Хост):

Компьютер, выполняющий в сети не только функции по передаче данных, но и некоторые другие, связанные с работой прикладных программ. Предоставляет свои информационные и вычислительные ресурсы терминалам. В сети Интернет данный термин трактуется более широко: хост-машиной называется любое активное сетевое устройство, подключенное к сети. Различие делается между хост-машиной и маршрутизатором (router), который в Интернет чаще называется шлюзом (gateway).

Host Name

Уникальный идентификатор, используемый для обозначения каждого хоста (системы) в сети.

HyperText (Гипертекст)

набор Интернет страниц, содержащих перекрестные ссылки на другие страницы, которые позволяют читателю с помощью Интернет Браузера перемещаться по этим страницам

HTTP (HyperText Transport Protocol)

HTTP – это протокол связи, позволяющий соединяться с WEB серверами расположенными в любой точке мира или с локальными серверами. Протокол HTTP устанавливает связь с Web сервером и передает страницы HTML на браузер клиента (например Windows IE). Любой http адрес начинается с префикса **'http://'** (например, *http://planet.com.ru*).

I

IAPP (Беспроводной Роуминг):

В соответствии с предварительной спецификацией стандарта IEEE 802.11f представляет собой протокол обмена служебной информацией между точками доступа (Inter-Access Point Protocol, IAPP), что необходимо для построения распределенных беспроводных сетей передачи данных.

Если в Вашей беспроводной сети работает несколько точек доступа, то при включении этой функции они смогут обмениваться информацией о подключенных беспроводных клиентах, что позволит организовать роуминг в вашей беспроводной сети и прозрачно подключать клиентов при переходе в зону действия другой точки доступа. Перед включением роуминга необходимо убедиться, что в предполагаемой зоне перемещения мобильного пользователя все Точки Доступа и Мобильный пользователь используют одинаковые номера каналов, идентификаторы, находятся в одной локальной сети (LAN) и т.п.

Вот краткий механизм работы беспроводного роуминга:

Точка доступа периодически посылает сигнал Радиомаяка (по умолчанию каждые 100 миллисекунд).

Клиентское оборудование (беспроводные карты) используют этот сигнал для оценки качества связи

Клиенты также могут посылать сигнал радиомаяка, или пробный запрос, в ответ на который точка доступа пошлет радиомаяк

Основываясь на качестве связи, клиент примет решение, с какой точкой доступа лучше работать.

Если он перемещается между ТД, то новая ТД информирует старую через проводное соединение при помощи *Inter Access Point Protocol (IAPP)* о переустановленном соединении клиента в сети.

Следовательно, при правильном размещении точек доступа на территории предприятия, пользователи смогут перемещаться по ней без потери доступа к беспроводной сети

Стандарт 802.11f находится на стадии утверждения и это нужно учитывать при развертывании беспроводной сети, а *Inter Access Point Protocol (IAPP)* - это попытка стандартизовать протокол роуминга. Поэтому в данный момент, роуминг лучше организовывать на продуктах одного производителя.

ICMP (Internet Control Message Protocol, протокол управляющих сообщений Internet)

Протокол, используемый для контроля за ошибками и сообщениями на уровне IP. Представляет собой часть протокола IP. Например ICMP сообщения могут использоваться маршрутизатором для уведомления отправителя что заданный узел недоступен.

Idle Timeout (Период бездействия)

Этот параметр задает максимальный период непрерывного бездействия, по истечении которого пользовательский сеанс прерывается. Атрибут доступен для передачи от сервера к клиентам в пакетах Access-Accept и Access-Challenge.

Формат атрибута Idle-Timeout показан ниже. Поля передаются слева направо.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type        | Length        | Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Value (cont)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = 28

Length = 6

Value Четырехоктетное поле, содержащее 32-битовое беззнаковое целое число, которое определяет максимальное непрерывное время бездействия в секундах, по истечении которого пользователь отключается от сервера NAS.

IEEE 802.11a

Стандарт беспроводных локальных сетей (WLAN), функционирующих в частотном диапазоне 5 ГГц (диапазон ISM). Беспроводные локальные сети стандарта IEEE 802.11a обеспечивают скорость передачи данных до 54 Мбит/с, что примерно в пять раз быстрее сетей стандарта IEEE 802.11b, и позволяют передавать большие объемы данных, чем сети IEEE 802.11b.

IEEE 802.11b

Стандарт IEEE 802.11b является стандартом беспроводных локальных сетей (WLAN), функционирующих в частотном диапазоне 2,4 ГГц (диапазон ISM). Беспроводные сети стандарта IEEE 802.11b характеризуются более широким распространением, чем сети стандартов IEEE 802.11a и IEEE 802.11g. Скорость передачи данных в этих сетях составляет 11 Мбит/с, а радиус действия от 100 до 500 метров. Технология IEEE 802.11b стала первой технологией беспроводных сетей, предложенной потребителям, которая позволила создать беспроводные сети в офисах и жилых помещениях, обеспечивающие мгновенный доступ. На устройства, сертифицированные группой Wi-Fi Alliance, наносится официальный логотип Wi-Fi.

IEEE 802.11g

Стандарт, регламентирующий метод построения беспроводных локальных сетей (WLAN), функционирующих в частотном диапазоне 2,4 ГГц (диапазон ISM). Благодаря применению технологии ортогонального частотного мультиплексирования (OFDM) максимальная скорость передачи данных в беспроводных сетях IEEE 802.11g составляет 54 Мбит/с. Оборудование, поддерживающее стандарт IEEE 802.11g, например, точки доступа беспроводных сетей, обеспечивают одновременное подключение к сети беспроводных устройств стандартов IEEE 802.11g и IEEE 802.11b.

IP (Internet Protocol)

Протокол сетевого уровня из набора протоколов Internet, определенного в RFC 791. Описывает программную маршрутизацию пакетов и адресацию устройств. Стандарт используется для передачи через сеть базовых блоков данных и дейтаграмм IP. Обеспечивает передачу пакетов без организации соединений и гарантии доставки. Протокол был изначально разработан Министерством Обороны США для объединения в сеть разнородных компьютеров.

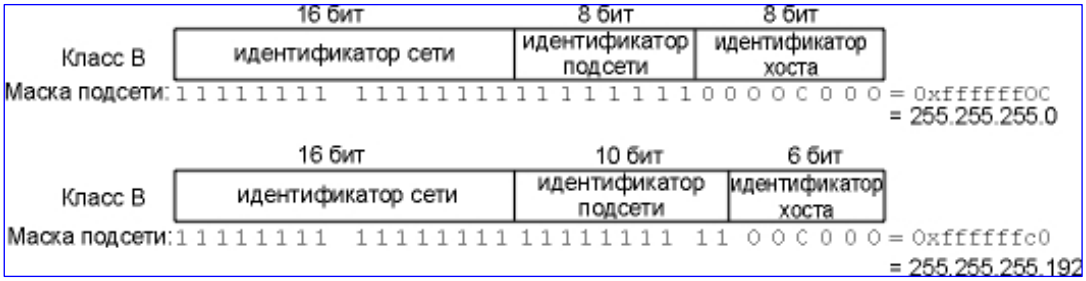
IP Address and Network (Subnet) Mask (IP адрес и маска подсети):

IP-адрес для протокола IP - 32 битовое (4 байта) адрес, определенный в STD 5 (RFC 791) и используемый для представления точек подключения в сети TCP/IP. IP-адрес состоит из номера сети (network portion) и номера хоста (host portion) - такое разделение позволяет сделать маршрутизацию более эффективной. Обычно для записи IP-адресов используют десятичную нотацию с разделением точками. Новая версия протокола IPv6 использует 128-разрядные адреса, позволяющие решить проблему нехватки адресного пространства.

Пример: IP адрес 192.168.0.1. состоит из 2 частей: адрес IP-сети, и номер сети.
Адрес IP - 32-разрядная последовательность двоичных чисел, которая может быть представлена в виде десятичной нотации, разделённой точками: xxx.xxx.xxx.xxx, где каждый “xxx” может быть числом в диапазоне от 000 до 255, или как четырех восьмибитовых декад двоичных числсел, отделенных символом точки: yyyyyyyy. yyyyyyyy. yyyyyyyy. yyyyyyyy, где каждый “y” может или быть 0 или 1.

В дополнение к IP адресу, хосту также необходимо знать, сколько бит будет использовано в качестве идентификатора подсети и сколько бит будет использовано в качестве идентификатора хоста. Это определяется во время загрузки с использованием маски подсети. Маска это 32-битное значение, которое содержит биты, установленные в единицу для идентификатора сети и идентификатора подсети, и биты, установленные в 0 для идентификатора хоста. На рисунке показано формирование маски подсети для двух различных разделений адреса класса B. В верхнем примере происходит разделение на хосте, где идентификатор подсети и идентификатор хоста занимают 8 бит. В нижнем примере показано разделение адреса класса B, при этом идентификатор подсети занимает 10 бит, а идентификатор хоста - 6 бит.

Рисунок: Пример масок подсетей для двух различных подсетей класса B.



Несмотря на то, что IP адреса обычно пишутся в десятичном виде с точками, маски подсети, как правило, пишутся в шестнадцатеричном виде, особенно если разделение происходит не побайтно, а побитно.
После того как хост получил свой IP адрес и маску подсети, он может определить, предназначена ли IP датаграмма для хоста в его собственной подсети, или она адресована хосту в другой подсети его собственной сети, или хосту в другой сети. Зная собственный IP адрес, можно определить, к какому классу он относится: A, B или C (по старшим битам), также можно определить, где проведена граница между идентификатором сети и идентификатором подсети. По маске подсети можно определить, где проведена граница между идентификатором подсети и идентификатором хоста.

ISP (Провайдер Сервиса Интернет)

Провайдер, предоставляющий услуги доступа в Интернет для частных пользователей или организаций.

ISP Gateway Address (Шлюз Интернет Провайдера по умолчанию)

IP адрес маршрутизатора Интернет провайдера или маршрутизатора в вашей внешней локальной сети, который будет являться для Вашего маршрутизатора шлюзом по умолчанию. (дополнительно смотрите описание термина ISP).

Л

LAN (Local Area Network - локальная сеть, ЛВС)

Соединенные вместе скоростным каналом компьютеры и другие активные и пассивные сетевые устройства, расположенные на незначительном удалении один от другого (комната, здание, предприятие), то есть Сеть, объединяющая пользователей в локально ограниченной области. Сеть включает такие элементы, как: серверы, рабочие станции, сетевая операционная система и каналы связи.

М

MAC

Нижний подуровень канального уровня модели OSI. Служит основой многих компьютерных сетевых стандартов.

MAC Address (машинный адрес, канальный адрес)

позволяет однозначно идентифицировать устройство в локальной сети. Машинный адрес обычно имеет 48-битный размер, где старшая половина обозначает производителя сетевого адаптера, а младшая — его серийный номер: например, MAC-адрес *00:30:4A:51:5E:*13 по первым трём числам указывает на фирму PLANET. Традиционно MAC-адрес считался неотъемлемой частью устройства и должен быть уникальным, однако всё чаще в настройках можно встретить опцию для его изменения на произвольное значение; это может быть полезно для прозрачной замены старого оборудования новым. Однако, в случае если в локальной сети будет работать несколько устройств с одинаковыми MAC, то правильная работа сети будет нарушена. Специальный адрес *FF:FF:FF:FF:FF:FF* служит для широковещательной передачи (broadcast), когда кадр копируется во все порты коммутатора, а диапазон *01:00:5E:xx:xx:xx* — для многоадресной передачи (multicast), когда кадр копируется только в те порты, из которых поступали запросы на присоединение к многоадресной группе.

MTU (Maximum Transmission Unit - максимальный передаваемый модуль данных)

Максимально возможный модуль данных, который можно передать через данную физическую среду. Существуют ограничения, накладываемые на размер фрейма для Ethernet инкапсуляции и инкапсуляции 802.3. Ограничение накладывается на количество байтов данных в 1500 и 1492 соответственно. Эта характеристика канального уровня называется максимальный блок передачи (MTU - maximum transmission unit). Большинство типов сетей определяют верхний предел.

Если IP хочет отослать датаграмму, которая больше чем MTU канального уровня, осуществляется фрагментация (fragmentation), при этом датаграмма разбивается на меньшие части (фрагменты). Каждый фрагмент должен быть меньше чем MTU.

На рисунке приведен список некоторых типичных значений MTU, взятых из RFC 1191. Здесь приведены MTU для каналов точка-точка (таких как SLIP или PPP), однако они не являются физической характеристикой среды передачи. Это логическое ограничение, при соблюдении которого обеспечивается адекватное время отклика при диалоговом использовании.

Сеть	MTU (байт)
Hyperchannel	65535
16 Мбит/сек Token ring (IBM)	17914
4 Мбит/сек Token ring (IEEE 802.5)	4464
FDDI	4352
Ethernet	1500
IEEE 802.3/802.2	1492
X.25	576
Точка-точка (с маленькой задержкой)	296

N

NAT (Network Address Translation - трансляция сетевых адресов)

Технология преобразования множества внутренних IP-адресов сети в один или несколько внешних адресов, используемых для связи с Internet. Поддержка протокола позволяет решить проблему нехватки адресов IP и позволяет получать доступ в Internet из локальной сети, используя единственный внешний IP-адрес.

Network Administrator (Сетевой Администратор)

Сетевой администратор – это человек, который управляет локальной сетью в пределах организации. Работа администратора заключается в обеспечении гарантированной защиты сети, её модернизации и

конфигурировании, наблюдение за сетевой активностью пользователей, разрешении и предотвращении конфликтов в сетевом окружении, резервном копирование баз данных и другой информации, контроль за состоянием аппаратных средств и программного обеспечения на современном уровне и другие аспекты, зависящие от специфики обслуживаемой сети и задач.

NTP (Сетевой протокол службы времени)

Прикладной протокол (L7), позволяющий обратиться к иерархической сети серверов точного времени для синхронизации компьютерных часов с Координатором Универсального Времени (UTC). Говоря по другому, NTP позволяет добиться высокоточной синхронизации времени в сети синхронизирующихся серверов, каждый из которых получает показания из нескольких источников, обрабатывает их, и передаёт дальше. Для NTP, зарезервирован 123-й UDP-порт (см. также **SNTP**).

П

Packet (Пакет)

Группа битов, передаваемая целиком, включающая данные и дополнительные сведения, представленные в соответствующих форматах. Структура пакета зависит от используемого протокола. В общем случае пакет включает 3 основных элемента : управляющую информацию (адрес получателя и отправителя, длина пакета и т.п.), передаваемые данные, биты контроля и исправления ошибок. Блок информации помечается на уровне 3 (сетевой) модели OSI.

Packet filter (Фильтрация Пакетов)

Определение необходимости пересылки или отбрасывания пакетов на основе набора критериев (например, адрес отправителя или получателя, номер порта, длина пакета и т.п.). Фильтрация пакетов помогает управлять сетевым трафиком.

Ping (Packet internet groper)

Программа, используемая для проверки доступности адресата путем передачи ему специального сигнала (ICMP echo request - запрос отклика ICMP) и ожидания ответа.

Point-to-Point Connection (соединение "точка-точка ")

Соединение между парой конечных точек (узлов).

Port (Порт)

Абстракция, используемая транспортными протоколами Internet для обозначения многочисленных одновременных соединений с единственным хостом-адресатом. Сетевые клиенты (хосты LAN) используют номера портов для организации доступа по тому или иному протоколу, что позволяет отличить одно сетевое приложение / протокол от другого.

Port Number (Номер Порта)

Протоколы TCP и UDP идентифицируют приложения с использованием 16-битных номеров порта. Обычно серверы знают свои заранее известные (well-known) номера портов. Например, каждая реализация TCP/IP, предоставляющая FTP сервер, знает, что сервисный порт TCP номер 21 зарезервирован для FTP сервиса. Каждый Telnet сервер имеет порт номер 23. Каждая реализация TFTP (Trivial File Transfer Protocol) использует UDP порт 69. Подобные сервисы, предоставляемые в любой реализации TCP/IP, имеют заранее известные номера портов в диапазоне от 1 до 1023. Заранее известные порты обслуживаются Internet Assigned Numbers Authority (IANA).

Клиент обычно не заботится о том, какой порт используется с его стороны. Все что ему необходимо, это быть уверенным, что данный номер порта уникален на его компьютере. Номер порта клиента называется динамически назначаемым портом (ephemeral port), то есть портом с коротким временем жизни. Это объясняется тем, что клиент обычно существует ровно столько времени, сколько пользователь нуждается в клиентском сервисе, тогда как сервера функционируют все время, пока запущен компьютер.

Ниже приведен краткий список основных сервисов, используемый протокол и номера портов:

Сервис	Протокол	Номер Порта
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162

Сервис	Протокол	Номер Порта
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632
SIP Reg	TCP/UDP	5060

PPP (Point-to-Point Protocol, Протокол Точка-Точка)

Протокол связи между терминалом и маршрутизатором. Обеспечивает доступ по коммутируемым линиям в сеть Интернет. PPP инкапсулирует пакеты протоколов сетевого уровня в специальные пакеты управления сетью (NCP). Примером такой инкапсуляции может служить IPCP (IP over PPP) and IPXCP (IPX over PPP). Будучи наследником SLIP, PPP обеспечивает соединения маршрутизатор-маршрутизатор и хост-сеть как для синхронных, так и для асинхронных устройств. Протокол PPP определен в RFC 1661.

PPPoE

Спецификация для подключения пользователей сети стандарта Ethernet к Интернету через широкополосное соединение, такое как линия DSL, беспроводное устройство или кабельный модем. С помощью PPPoE и широкополосного модема пользователи локальной сети могут получать доступ с индивидуальной проверкой подлинности к высокоскоростным сетям данных. Объединяя Ethernet и протокол PPP (Point-to-Point Protocol), протокол PPPoE обеспечивает эффективный способ создания отдельных соединений с удаленным сервером для каждого пользователя.

PPTP

Сетевая технология, поддерживающая многопротокольную виртуальную частную сеть (VPN); предоставляет удаленным пользователям защищенный доступ к корпоративным сетям через Интернет (или другие сети) либо через поставщика услуг Интернета, либо с помощью непосредственного подключения к Интернету. Протокол PPTP туннелирует (или инкапсулирует) трафик IP, IPX или NetBEUI в IP-пакетах. Это позволяет пользователям удаленно запускать приложения, зависящие из отдельных сетевых протоколов.

Preamble (Заголовок, Преамбула)

В беспроводном оборудовании термин относится к длине блока CRC (Cyclic Redundancy Check), который контролирует состояние подключения между перемещающимися активными беспроводными устройствами и точками доступа.

Protocol (Протокол)

Формат описания передаваемых сообщений и правила, по которым происходит обмен информацией между двумя или несколькими системами. Формальный набор правил и форматов (семантика и синтаксис), разработанный для форматирования, тактирования и управления сетевыми коммуникациями. Обычно протокол реализуется как группа услуг на одном или двух уровнях модели OSI. Протокол может описывать детали взаимодействия оборудования на нижних уровнях или обмена информацией между программами на верхних уровнях.

QoS (Quality of Service - гарантированное качество услуг)

в применении к данной модели маршрутизатора термин обозначает, что данные, для которых назначен класс обслуживания, будут передаваться максимально быстро и стабильно в соответствии с выделенной для них максимальной или гарантированной полосой пропускной способности. Эта функция позволяет зарезервировать для определенных видов входящего и исходящего трафика заданную полосу пропускания с привязкой к диапазонам IP адресов и видам трафика. При настройке следует учитывать максимальную пропускную способность Вашего канала и очерёдность выставления правил (максимальный приоритет имеет первое правило).

RIP (Routing Information Protocol)

RIP - это протокол Маршрутизации, который интегрирован в протокол TCP/IP. В сетях IP, протокол RIP, работающий на основе векторов расстояния, является внутренним протоколом маршрутизации, используемым для обмена информацией между сетями. RIP находит маршрут, основанный на наименьшем числе интервалов (Hops) на пути перемещения сообщения между источником пакета и его получателем.

RTS (Request To Send - готовность к передаче)

Управляющий сигнал, передаваемый модему от DTE, который говорит что DTE имеет данные для передачи.

Router (Маршрутизатор)

этот термин в зависимости от конкретного применения может иметь два значения:

1. Система, отвечающая за принятие решений о выборе одного из нескольких путей передачи сетевого трафика. Для выполнения этой задачи используются маршрутизируемые протоколы, содержащие информацию о сети и алгоритмы выбора наилучшего пути на основе нескольких критериев, называемых метрикой маршрутизации ("routing metrics"). В терминах OSI маршрутизатор является промежуточной системой Сетевого уровня.
2. Зависящий от протокола компонент межсетевого взаимодействия, настроенный так, чтобы знать какие сегменты ЛВС взаимодействуют с ним и отвечающий за передачу пакетов между сегментами по наилучшему пути. Маршрутизатор должен распознавать различные протоколы сетевого уровня, которые могут использоваться для объединения сетей. Многопротокольные маршрутизаторы могут работать с различными протоколами.

Roaming (Роуминг)

Перемещение устройства конечного пользователя между узлами доступа с прозрачной сменой подключения (незаметной для пользователя и не приводящей к перерывам и сбоям в работе устройства пользователя), обеспечивающее непрерывную работу конечного устройства. Примером могут служить мобильные устройства (например, телефоны или компьютеры) в сотовой сети, которые могут передавать и принимать данные (GPRS трафик, телефонный разговор и т.п.) непрерывно перемещаясь по городу или старне без потери связи (при условии наличия покрытия у данного мобильного оператора на всем пути следования пользователя).

Server (Сервер)

Компьютер, специализированное устройство или процесс, обеспечивающее доступ и управление доступом к разделяемым сетевым ресурсам (диски, принтеры, данные). См. также **Client**.

SLIP

Протокол Интернет, используемый для реализации IP при соединении двух систем последовательными линиями (телефонными или RS-232). В настоящее время вместо SLIP в основном используется протокол PPP.

SMTP (Simple Mail Transfer Protocol - простой протокол передачи почтовых сообщений)

Протокол передачи электронной почты в сети Internet. Определен в RFC 821, а форматы сообщений описаны в RFC 822.

SNTP (Simple Network Time Protocol)

В отличие от NTP протокол SNTP образует не сеть синхронизирующихся серверов, а пары «клиент-сервер». Любой NTP-сервер является одновременно SNTP-сервером, однако бывают и только SNTP-сервера. Клиент, который не передаёт полученное время дальше, может работать как NTP или SNTP клиент, в зависимости от условий. Для SNTP, как и для NTP, зарезервирован 123-й UDP-порт (см. также **NTP**).

SNMP (Simple Network Management Protocol - простой протокол сетевого управления)

Протокол сетевого администрирования SNMP очень широко используется в настоящее время. Управление сетью входит в стек протоколов TCP/IP. Протокол SNMP определен в RFC 1157.

SSID и SSID Broadcast

Каждая сеть во внешнем мире имеет свой уникальный логический адрес - network name (сетевое имя). В стандарте 802.11 в качестве такого имени служит SSID (Service Set Identifier). Оборудование работающее в одной беспроводной сети должно иметь одинаковый SSID. В практическом применении SSID используется для того, чтобы указать беспроводной станции адрес сети для подсоединения. Прежде чем связаться с определенной беспроводной сетью, станция должна получить тот же SSID, что и AP (если включен режим **SSID Broadcast**) или его необходимо прописать вручную. Если включен режим **SSID Broadcast**, то точка доступа включает SSID в широковещательный маркерный пакет, что позволяет станции автоматически сконфигурировать беспроводную сетевую карту, установив корректный SSID. Клиент 802.11 вправе ожидать, что он может установить связь с любой AP, объявляющей данный SSID и не использующей шифрование.

Subnet (подсеть)

Физически или логически независимая часть сети, задаваемая номером (внутренний адрес)

Subnet address (адрес подсети)

Связанная с подсетью часть IP-адреса. В сети с подсетями номер хоста (host portion) делится на две части - подсеть и хост, причем последняя использует маску подсети (subnet mask).

Subnet Mask (маска подсети)

Шаблон или фильтр, используемый по отношению к адресу Internet для идентификации узлов отдельной подсети. Биты, имеющие значение "1" в маске подсети показывают значимые биты в адресе подсети, а биты, имеющие значение "0", указывают на биты адреса, которые игнорируются. См. также **IP Address and Network (Subnet) Mask.**

SysLog Server (Сервер протоколирования событий)

SysLog сервер отслеживает события, декодирует полученные сообщения и регистрирует их в жулнале

T

TCP (Transmission Control Protocol, протокол управления передачей)

Основной транспортный протокол в наборе протоколов Internet, обеспечивающий надежные, ориентированные на соединения, полнодуплексные потоки. Протокол TCP является одним из транспортных протоколов уровня 4 в модели OSI. Для доставки данных используется протокол IP.

Telnet

Протокол виртуального терминала в стеке протоколов Internet, описанный в RFC 854. Позволяет пользователям одного хоста подключаться к другому удаленному хосту и работать с ним как через обычный терминал

TKIP (Temporal Key Integrity Protocol)

В отличие от протокола WEP, где для обеспечения целостности передаваемых данных применялся механизм CRC-32, протокол TKIP использует MIC (Message Integrity Code), обеспечивающий криптографическую контрольную сумму от полей “адрес источника”, “адрес назначения” и поля данных. В качестве номера пакета в TKIP используется вектор инициализации IV - TSC (TKIP Sequence Counter) длиной 48 бит (в WEP использовался 24 битный).

V

Virtual Servers (Виртуальный Сервер)

используются для присвоения одному компьютеру нескольких доменных имен. Например, microsoft.com, www.microsoft.com, ftp.microsoft.com - это виртуальные адреса одного и того же компьютера. Обычно реальный WEB-сервер поддерживает несколько разных виртуальных серверов.

VCI (Virtual Channel Identifier – Идентификатор виртуального канала)

Адрес или метка, содержащаяся в заголовке ячейки ATM для обозначения виртуального канала в виртуальном пути на физическом соединении ATM.

VPI (virtual path identifier - Идентификатор виртуального пути)

Поле в заголовке ячейки ATM, указывающее на определенный виртуальный путь

VPN (virtual private network - виртуальная частная сеть)

Распределенная коммуникационная сеть, организованная на базе каналов и сервиса общего пользования, с обеспечением возможностей, функциональности и безопасности сетей на базе выделенных каналов.

Ω

WAN (Wide-Area Network - распределенная сеть, глобальная сеть)

сеть, обеспечивающая передачу информации на значительные расстояния с использованием коммутируемых и выделенных линий или специальных каналов связи. WAN-сети обычно состоят из локальных сетей, соединенных публичными или арендованными каналами. См. также **LAN**.

WEP (Wireless Encryption Protocol или Протокол Беспроводного Шифрования)

протокол шифрования в беспроводной связи. Базируется на поточно симметричном алгоритме шифрования RC4. Используются статические ключи с длинной от 64 до 256 бит. Требует заранее прописанных, одинаковых ключей шифрования на беспроводном оборудовании, которое подключается к друг другу. Из всех протоколов шифрования является наименее защищенным. Слабые места: несовершенный механизм обмена ключами, а точнее, практически полное его отсутствие, малая длина ключа и вектора инициализации, механизм проверки целостности передаваемых данных, сам способ аутентификации и алгоритм шифрования RC4.

Web-based management Graphical User Interface (GUI)

графический пользовательский интерфейс доступ к которому возможен с помощью обычного WEB браузера. Это метод взаимодействия между пользователем и интерфейсом активного сетевого оборудования (хоста), при котором пользователь может вызывать различные функции, указывая на графические элементы (кнопки) вместо ввода команд с клавиатуры.

Wireless LAN (Беспроводной интерфейс)

Беспроводной интерфейс (беспроводная локальная сеть, сетевой адаптер), широко распространенный на мобильных устройствах (ноутбук, КПК и т.п.). Применяется для построения локальных компьютерных сетей без использования проводов, как в одноранговых, так и с использованием беспроводных коммутаторов. В настоящее время используется несколько стандартов для беспроводных компьютерных сетей. См**. IEEE 802.11.a/b/g**

Wireless LAN (WLAN Беспроводная локальная сеть)

Это стандартизированная технология с помощью которой несколько устройств могут соединяться между собой с помощью беспроводного соединения. Семейство протоколов 802.11 работает полностью прозрачно, относительно других протоколов передачи данных. Все устройства , поддерживающие протоколы семейства 802.11, выполняют роль преобразователей среды передачи данных, которые не вносят изменений в пакеты данных, используемых другими протоколами. На практике это значит, что пакет данных, переданный одним устройством, может быть точно распакован другим устройством. Вследствие чего, сети Wi-Fi поддерживают все возможные протоколы передачи данных.

WPA (Wi-Fi Protected Access или Защищенный Беспроводной Доступ)

это шифрование обеспечивающее значительно более высокий уровень защиты для Вашей беспроводной сети и данных. Этот протокол содержит несколько инструментов, повышающих защищённость беспроводных сетей: динамические ключи, изменённый механизм генерации ключей, более надёжный механизм проверки целостности сообщений, увеличенный по длине вектор инициализации, нумерацию пакетов. В отличие от WEP использующего статические ключи шифрования, этот стандарт использует пароль владельца, от которого система производит постоянно изменяющиеся ключи (динамически), используя протокол TKIP. Ключи никогда не используются повторно, что значительно снижает риск того, что хакер сможет их перехватить и воспользоваться ими. WPA также включает в себя поддержку стандарта 802.1x, который позволяет системе проверять, кто подключается к сети используя центральную базу данных известных пользователей (RADIUS).

WPA-PSK (Pre-shared Key)

позволяет настроить подключение беспроводных клиентов без использования RADIUS сервера, на основе пароля с последующей динамической сменой ключа шифрования. Используется для организации небольших беспроводных сетей. Устойчивость к взлому выше, чем у WEP, но имеются существенные недостатки, влияющие на устойчивость к взлому. Первым недостатком WPA-PSK является то, что используется статическая парольная фраза, которая не меняется с течением времени, следовательно, её можно подобрать за какое-то конечное время. Второй недостаток это то, что контрольная фраза должна быть одинаковой у всех клиентов беспроводной сети.

Аппаратная версия Устройства

Производитель периодически может вносить изменения в конструкцию изделия. Это может быть связано как с усовершенствованием интерфейсов, так и с частичной заменой элементной базы. Оборудование с новой ревизией печатной платы маркируется на шильдике (как правило расположен на дне корпуса) индексом **“v.”** и номером версии после наименования модели. Например, VRT-401**v.2**. На это следует обратить особое внимание при обновлении прошивки в таком оборудовании. Как правило, прошивки предназначенные для других аппаратных версий не подходят для оборудования первой аппаратной версии (без индекса **“v.”**) и загрузка прошивки от оборудования другой аппаратной версии приведет к неработоспособности устройства.

Уровни и протоколы межсетевого взаимодействия

Сетевые протоколы разрабатываются по уровням, причем каждый уровень отвечает за собственную фазу коммуникаций. Семейства протоколов, такие как TCP/IP, это комбинации различных протоколов на различных уровнях. TCP/IP состоит из четырех уровней

1. **Канальный уровень** (link layer). Еще его называют уровнем сетевого интерфейса. Обычно включает в себя драйвер устройства в операционной системе и соответствующую сетевую интерфейсную плату в компьютере. Вместе они обеспечивают аппаратную поддержку физического соединения с сетью (с кабелем или с другой используемой средой передачи).
2. **Сетевой уровень** (network layer), иногда называемый уровнем межсетевого взаимодействия, отвечает за передачу пакетов по сети. Маршрутизация пакетов осуществляется именно на этом уровне. IP (Internet Protocol - протокол Internet), ICMP (Internet Control Message Protocol - протокол управления сообщениями Internet) и IGMP (Internet Group Management Protocol - протокол управления группами Internet) обеспечивают сетевой уровень в семействе протоколов TCP/IP.
3. **Транспортный уровень** (transport layer) отвечает за передачу потока данных между двумя компьютерами и обеспечивает работу прикладного уровня, который находится выше. В семействе протоколов TCP/IP существует два транспортных протокола: **TCP** (Transmission Control Protocol) и **UDP** (User Datagram Protocol).
   TCP осуществляет надежную передачу данных между двумя компьютерами. Он обеспечивает деление данных, передающихся от одного приложения к другому, на пакеты подходящего для сетевого уровня размера, подтверждение принятых пакетов, установку тайм-аутов, в течение которых должно прийти подтверждение на пакет, и так далее. Так как надежность передачи данных гарантируется на транспортном уровне, на прикладном уровне эти детали игнорируются.
   UDP предоставляет более простой сервис для прикладного уровня. Он просто отсылает пакеты, которые называются датаграммами (datagram) от одного компьютера к другому. При этом нет никакой гарантии, что датаграмма дойдет до пункта назначения. За надежность передачи данных, при использовании датаграмм отвечает прикладной уровень. Для каждого транспортного протокола существуют различные приложения, которые их используют.
4. **Прикладной уровень** (application layer) определяет детали каждого конкретного приложения. Существует несколько распространенных приложений TCP/IP, которые присутствуют практически в каждой реализации:
   - Telnet - удаленный терминал
   - FTP, File Transfer Protocol - протокол передачи файлов
   - SMTP, Simple Mail Transfer Protocol - простой протокол передачи электронной почты
   - SNMP, Simple Network Management Protocol - простой протокол управления сетью.

802.1x

обеспечивает аутентификацию удаленных клиентов и выдачу им временных ключей для шифрования данных. Ключи (в зашифрованном виде) высылаются клиенту на незначительный промежуток времени, после которого генерируется и высылается новый ключ. Алгоритм шифрования не изменился – тот же RC4, но постоянная смена ключей очень сильно затрудняет вероятность взлома. Поддержка этого протокола есть только в операционных системах (от Microsoft) Windows XP. Этот протокол требует обязательного наличия RADIUS-сервера.