

Широкополосный Интернет роутер

XRT-401D

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 Technology 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 для коммутатора WGSD-1020, 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

Ревизия

Руководство пользователя для широкополосного Интернет маршрутизатора XRT-401D:

Широкополосный Интернет Маршрутизатор

Модель: XRT-401D

Ревизия: 1.0 (Октябрь, 2003)

Перевод 1.04 (Декабрь 2006) Бекетов О.Э.

Part No. RM-XRT401DV1

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: supnopt@planet.com.ru

Оглавление

Раздел 1 Обзор	4
1.1 Возможности.....	4
1.2 Минимальные требования.....	4
1.3 Комплект поставки.....	4
1.4 Описание XRT-401D.....	5
1.5 Подключение.....	6
1.6 Начальная настройка.....	6
Раздел 2 Быстрая настройка	10
Шаг I. Временные зоны (Time Zone).....	10
Шаг II. Тип широкополосного подключения (Broadband Type).....	11
2.1 Кабельный Модем.....	11
2.2 Фиксированный IP Адрес (Fixed-IP xDSL).....	12
2.3 PPPoE.....	13
2.4 PPTP.....	14
Раздел 3 Основные Настройки	16
3.1 Меню System.....	16
3.1.1 Часовой Пояс (Time Zone).....	17
3.1.2 Изменение Пароля (Password Settings).....	17
3.1.3 Удаленное управление (Remote Management).....	18
3.2 WAN.....	19
3.2.1 Режим DHCP клиент (Dynamic IP).....	20
3.2.2 Статический IP Адрес (Static IP Address).....	20
3.2.3 PPPoE (PPP over Ethernet).....	20
3.2.4 PPTP.....	20
3.2.5 L2TP.....	20
3.2.6 Telstra Big Pond.....	21
3.2.7 Сервер Доменных Имен (DNS).....	22
3.2.8 Сервер Динамических Доменных Имен (DDNS).....	22
3.3 Локальная Сеть (LAN).....	23
3.4 Трансляция Сетевых Адресов (NAT).....	24
3.4.1 Перенаправление Портов (Port Forwarding).....	25
3.4.2 Виртуальный Сервер (Virtual Server).....	26
3.4.3 Специальные Приложения (Special Applications).....	27
3.4.4 Служба Уровня Приложения (ALG Settings).....	28
3.4.5 Универсальный PnP (UPnP).....	29
3.5 Межсетевой Экран.....	29
3.5.1 Контроль доступа (Access Control).....	30
3.5.2 Блокировка URL (URL Blocking).....	32
3.5.3 Отказ в Обслуживании (DoS).....	32
3.5.4 Демилитаризованная зона (DMZ).....	33
Раздел 4 Состояние устройства	34
4.1 Состояние (Status).....	34
4.2 Подключение к Интернет (Internet Connection).....	34
4.3 Состояние устройства (Device Status).....	35
4.4 Системный журнал (System Log).....	35
4.5 Журнал Защиты (Security Log).....	36
4.6 Таблица активных DHCP клиентов.....	36
4.7 Статистика.....	36
Раздел 5 Расширенное Администрирование	37
5.1 Инструмент Конфигурация (Configuration Tools).....	37
5.2 Обновление прошивки (Firmware Upgrade).....	38
5.3 Решение проблем с нестабильной работой.....	38
5.4 Аппаратная перезагрузка (Reset).....	39
Приложение А	40
Список терминов	41

Раздел 1 Обзор

Широкополосный Интернет роутер XRT-401D предназначен для защиты Вашей локальной сети и обеспечения совместного использования одного подключения к сети Интернет всеми пользователями локальной сети. Поддержка большого количества видов подключения (PPPoE/DHCP/fixed IP/PPTP) позволит использовать XRT401D в практически любом сетевом окружении.

Для простой интеграции и полной совместимости с существующими сетевыми инфраструктурами, Planet XRT-104D использует автоопределение типа (MDI/MDI-X) и скорости подключения на 4-х 10/100Mbps портах LAN и 10/100Base-TX WAN порту.

Обладая встроенной системой безопасности, доступа и журналом предупреждений, XRT-401D не только обеспечит скоростной доступ в Интернет, но и обеспечит безопасность соединения с высоким уровнем защищенности локальной сети. XRT-401D поддерживает заданные политики защиты и аутентификации пользователя, параметры предоставления доступа к ресурсам сети Интернет и систему управления роутером, что обеспечивает необходимую функциональность и гибкость работы

1.1 Возможности

- Высокая пропускная способность
- Совместный доступ к сети Интернет через одно подключение
- Поддержка до 253 пользователей
- Подключение к кабельному или xDSL модему
- Настраиваемый доступ к сервисам в Локальной сети из Интернет
- 4 порта LAN (10/100M) и один WAN порт (10/100M)
- Встроенный DHCP Сервер для LAN и поддержка режима DHCP клиент (для порта WAN)
- Поддерживает расширенные функции: Специальные приложения, DMZ (Демилитаризованная зона), Виртуальные Серверы, Контроль доступа, Межсетевой Экран.
- Возможность отключения NAT (режим Bridge)
- Поддерживает ведение логов для следующих событий: подключенные DHCP клиенты, Защита и Состояние устройства и подключения
- WEB интерфейс для управления и администрирования
- Режим удаленного управления позволяет настраивать, администрировать роутер, а также выполнить обновление программного обеспечения.

1.2 Минимальные требования

- Один внешний xDSL (ADSL) или кабельный модем (RJ-45) или прямое подключение
- Сетевые карты (NIC) установленные на всех персональных компьютерах (PC)
- WEB Браузер установленный на компьютере (Internet Explorer 4.0 или новее, или Netscape Navigator 4.7 или новее)

1.3 Комплект поставки

- XRT-401D
- Один экземпляр инструкции по быстрой установке и настройке (англ.)
- Компакт диск с Инструкцией по эксплуатации
- Адаптер питания

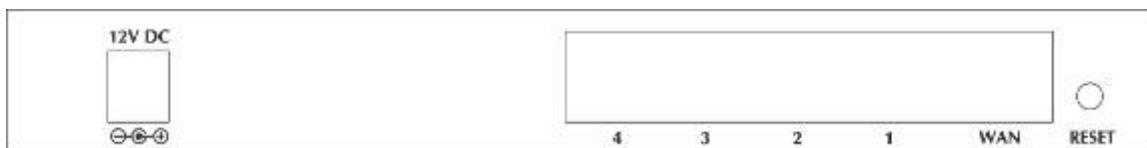
Внимание!

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

1.4 Описание XRT-401D

Задняя панель

На рисунке показана задняя панель XRT-401D. На ней расположены порты LAN (1,2,3,4), порт WAN, разъем питания и кнопка сброса (Reset).



1) Локальная Сеть (LAN)

Вы можете подключить к 4-х портовому коммутатору портов LAN ваши компьютеры, серверы печати и данных, коммутаторы 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 4-х 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 4-х секунд. Отпустите кнопку и дождитесь перезагрузки роутера. Все настройки будут сброшены (включая IP адрес, Имя пользователя и пароль) на значения по умолчанию.

Настройки роутера по умолчанию:

LAN IP: 192.168.0.1

Имя пользователя: admin

Пароль: 1234

Передняя Панель

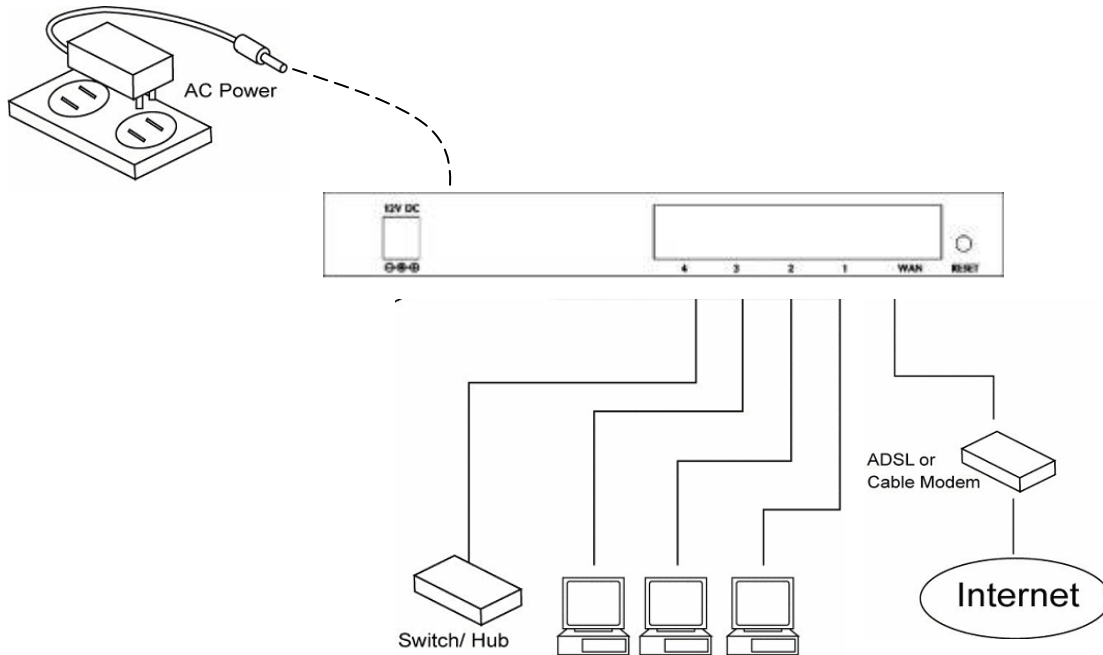
На передней панели расположены индикаторы, отображающие состояние интерфейсов роутера.



Индикация	Состояние	Описание
PWR	горит	Питание включено
WAN 10/100M	горит	WAN порт подключен на скорости 100Mbps
	не горит	WAN порт подключен на скорости 10Mbps
WAN LNK/ACT	горит	WAN подключен
	не горит	нет подключения WAN
	мигает	порт активен (ACT), идет передача данных
LAN 10/100M (Порты 1-4)	горит	LAN порт подключен на скорости 100Mbps
	не горит	LAN порт подключен на скорости 10Mbps
LAN LNK/ACT (Порты 1-4)	горит	LAN подключен
	не горит	нет подключения LAN
	мигает	порт активен (ACT), идет передача данных

1.5 Подключение

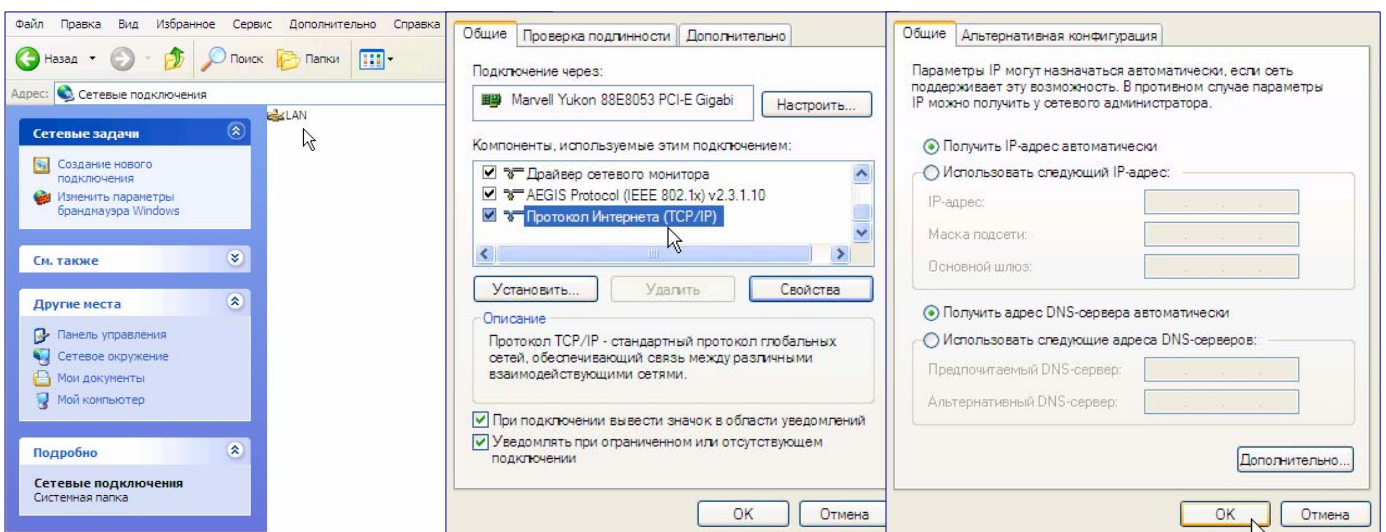
На рисунке показано общее схемотехническое подключения устройств и интерфейсов роутера.



1.6 Начальная настройка

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

- Шаг I.** Включите роутер, подключив адаптер питания идущий в комплекте 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 hosts (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!

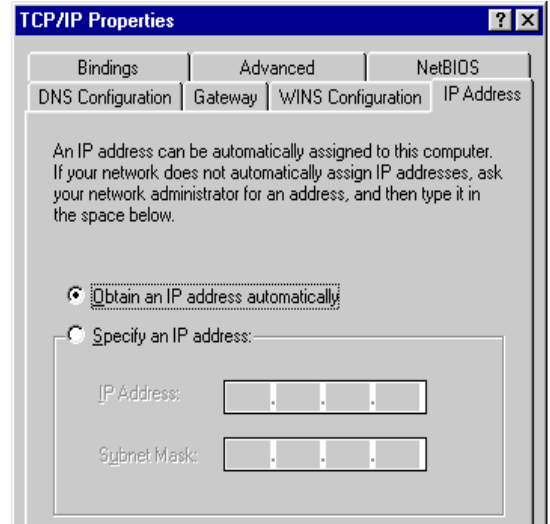
По умолчанию роутер использует для Локальной сети IP адреса из подсети класса C (192.168.0.0/24). Если Вам необходимо использовать другой диапазон адресов, то впоследствии, при настройке роутера вы можете изменить этот параметр.

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 настройка 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 (Настройка)**, 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.



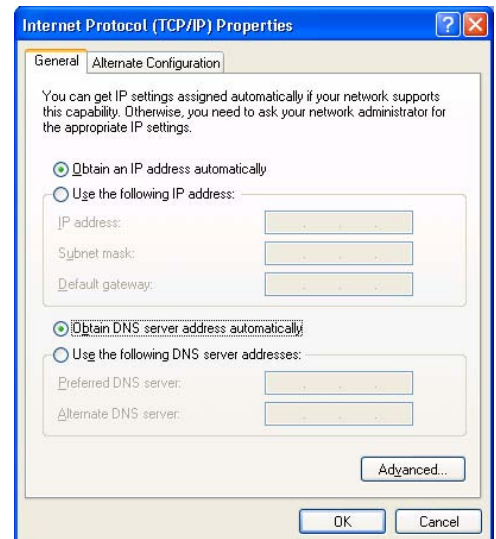
Обязательно убедитесь, что DHCP сервер роутера является единственным DHCP сервером в вашей локальной сети! Если в локальной сети используется ещё один DHCP сервер, то его следует временно отключить и в дальнейшем решить, какой из DHCP серверов Вы будете использовать (встроенный в роутер или другой).

Внимание!

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 (Настройка)**, 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 роутера является единственным DHCP сервером в вашей локальной сети!

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 (Настройка)**, 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. Откроеся 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 ОК на соответствующих открытых вкладках, чтобы сохранить изменения.
7. После сохранения изменений компьютер сможет автоматически получить IP адрес от DHCP сервера роутера.

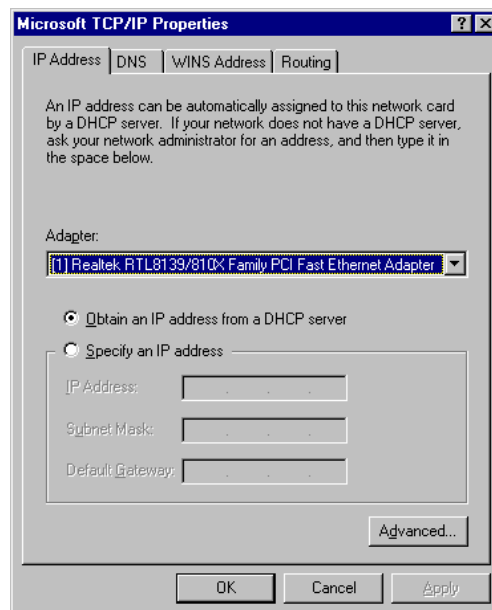
Внимание!

Обязательно убедитесь, что DHCP сервер 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**.

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 "1234". 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 2)	Этот раздел меню поможет выполнить начальную настройку роутера
General Setup – Основные Настройки (Раздел 3)	Т 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 4)	В этом разделе можно посмотреть информацию о статистике и состоянии подключений.
Tools – Расширенное Администрирование (Раздел 5)	Этот раздел предназначен для сохранения или восстановления конфигурации роутера, а также для обновления прошивки оборудования.

Шаг IX. Нажмите **Quick Setup Wizard** (см. Раздел 2) 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 2 Быстрая настройка

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

Шаг I. Временные зоны (Time Zone)

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

1. Time Zone

Set the time zone of the Broadband router. This information is used for log entries and firewall settings.

Set Time Zone :	(GMT+03:00)Moscow, St. Petersburg, Volgograd
Time Server Address :	192.43.244.18
Daylight Savings :	<input checked="" type="checkbox"/> Enable Function Times From January 1 To January 1

Next

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

Шаг II. Тип широкополосного подключения (Broadband Type)

В этом разделе меню Вам необходимо выбрать правильный тип подключения к Интернет провайдеру порта WAN роутера. Для этого необходимо обратиться к настройкам, выданным Вам Интернет провайдером.



Внимание!

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

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

Также роутер может выполнять подключение по протоколам L2TP и Telstra Big Point, но они не будут рассматриваться в этом мануале, так как Российские провайдеры 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.

2.1 Кабельный Модем

В режиме **Cable Modem** роутер 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 \(раздел 3.2.7\)](#) IP адреса первичного и вторичного DNS сервера.

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. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.

2.2 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**. Для дополнительной информации смотрите приложение А.

Fixed-IP xDSL
Enter the IP Address, Subnet Mask, Gateway IP Address and DNS IP Address provided to you by your ISP in the appropriate fields.

IP address assigned by your Service Provider :	172.145.2.202
Subnet Mask :	255.255.0.0
DNS Address :	193.158.25.2
Service Provider Gateway Address :	172.145.2.1
TTL :	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
MAC Address :	004063ca979d <input type="button" value="Clone Mac"/>

Параметр	Описание
IP	Статический IP адрес, выданный Вам Интернет провайдером.
Gateway IP	Шлюз по умолчанию (Интернет провайдера)
DNS	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 **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. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.



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 \(раздел 3.2.7\)](#) IP адреса первичного и вторичного DNS сервера.

2.3 PPPoE

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).

The screenshot shows the configuration interface for a Planet Internet Broadband Router. The page title is "Internet Broadband Router" and the breadcrumb is "HOME | General Setup | STATUS | Tool". The main heading is "3. IP Address Info" with a sub-heading "PPPoE". Below the heading, there is a text instruction: "Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a 'Service Name' enter it in the Service Name field, otherwise, leave it blank." The configuration form includes fields for "User Name", "Password", and "Service Name". There is also an "MTU" field with a value of 1492 and a note "(512<=MTU Value<=1492)". The "Connection Type" is set to "Continuous" with "Connect" and "Disconnect" buttons. The "Idle Time" is set to 0 with a note "(1-1000 minutes)". At the bottom of the form are "Back" and "OK" buttons.

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)	<p>Если выбрать Continuous: Ваш роутер будет постоянно подключен к сети Интернет. При разрыве подключения он автоматически переподключится к PPPoE Серверу провайдера.</p> <p>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.</p> <p>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.</p>
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 **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. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.

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.

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.

The screenshot shows the configuration interface for a Planet Internet Broadband Router. The page title is "Internet Broadband Router" and the breadcrumb is "HOME | General Setup | PPTP/ISRAEL | cool". The left sidebar shows a navigation menu with three items: "1. Time Zone", "2. Broadband Type", and "3. IP Address Info". The main content area is titled "PPTP" and includes a description: "Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections." Below this, there are two main sections: "WAN Interface Settings" and "PPTP Settings".

WAN Interface Settings:

- Obtain an IP address automatically :
- Use the following IP address :

IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0

PPTP Settings:

User ID :
Password :
PPTP Gateway : 0.0.0.0
Connection ID : (Optional)
BEZEQ-ISRAEL : Enable (for BEZEQ network in ISRAEL use only)
Connection Type : Continuous [Connect] [Disconnect]
Idle Time Out : 10 (-1-100 minutes)

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

Параметр	Описание
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.
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 **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. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.

Раздел 3 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
3.1 System	В этом меню можно настроить Параметры Сервера Времени (Time Zone), Изменить пароль (Password Settings) и настроить удаленное управление и администрирование (Remote Management).
3.2 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
3.3 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.
3.4 NAT	Здесь можно настроить Проброс портов (Port Forwarding), 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.
3.5 Firewall	Меню Межсетевое 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

3.1 Меню System

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

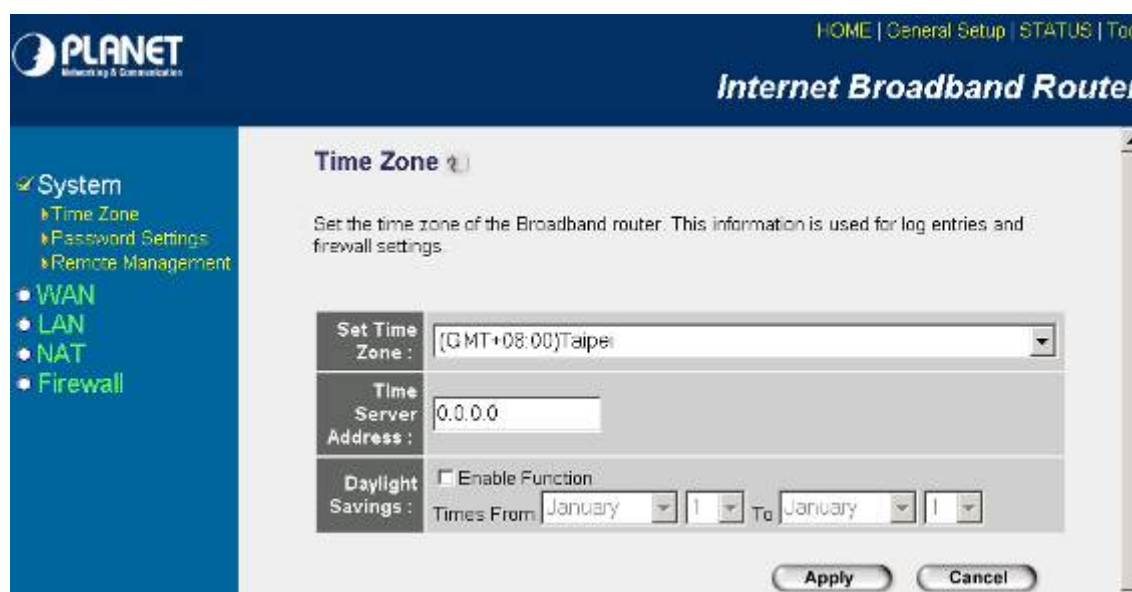


Раздел меню	Описание
3.1.1 Time Zone (временная зона)	В этом меню необходимо выбрать и настроить временную зону в соответствии с вашим часовым поясом. Например, для Москвы это +3.
3.1.2 Password Settings (Изменение пароля)	Этот раздел меню позволяет изменить пароль, используемый в роутере по умолчанию 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

3.1.1 Часовой Пояс (Time Zone)

В этом меню можно 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	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. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.

3.1.2 Изменение Пароля (Password Settings)

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 зависит от регистра, то при вводе обратите внимание на клавишу Caps Lock.



Параметр	Описание
Current Password	Введите старый пароль
Внимание!: Пароль по умолчанию 1234	
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 4-х 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. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.

3.1.3 Удаленное управление (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.

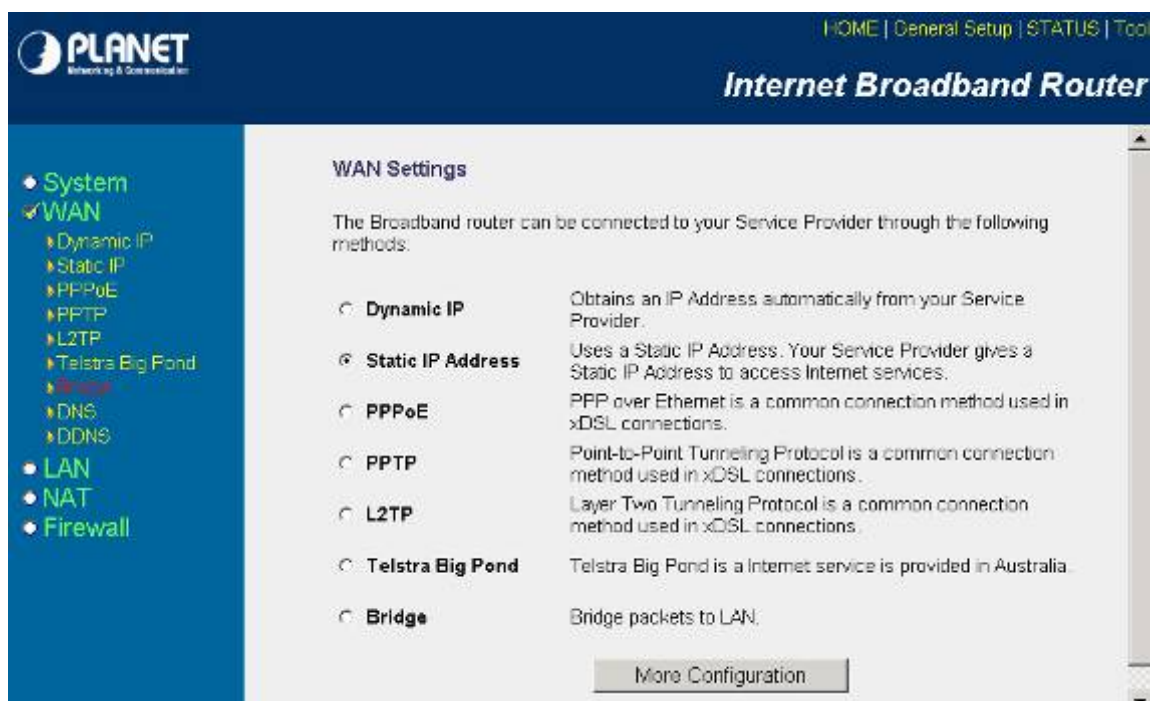


Параметр	Описание
Enabled	Поставьте галочку в окошке Enabled , чтобы активизировать функцию удаленного администрирования.
Host Address	Определённый IP адрес, с которого будет разрешено удаленное администрирование и управление маршрутизатором. То есть подключиться к WEB интерфейсу роутера удаленно можно 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. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.

3.2 WAN

В этом разделе меню вы можете настроить тип подключения к Интернет провайдеру порта WAN роутера. 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
3.2.1 Dynamic IP	Интернет провайдер автоматически назначает IP адрес (режим DHCP клиент)
3.2.2 Static IP address	Интернет провайдер выдал Вам статический IP адрес
3.2.3 PPPoE	Интернет провайдер осуществляет подключение по протоколу Point-to-Point Protocol over Ethernet (PPPoE).
3.2.4 PPTP	Интернет провайдер осуществляет подключение по протоколу Point-to-Point Tunneling Protocol (PPTP).
3.2.5 L2TP	Интернет провайдер осуществляет подключение по протоколу L2TP
3.2.6 Telstra Big Pond	Интернет провайдер осуществляет подключение по протоколу Telstra Big Pond
3.2.7 DNS	Меню дополнительной настройки Сервера Доменных Имен (DNS)
3.2.8 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**.

3.2.1 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 2.1 “Кабельный Модем”](#) для более детальной информации.

3.2.2 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 ОК.

Смотрите [Раздел 2.2 “Фиксированный IP Адрес”](#) для более детальной информации.

3.2.3 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 2.3 “PPPoE”](#) для более детальной информации.

3.2.4 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 2.4 “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.

3.2.5 L2TP

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

The screenshot shows the configuration interface for a PLANET Internet Broadband Router. The page title is "Internet Broadband Router" and the breadcrumb navigation is "HOME | General | Setup | STATUS | Tool". The left sidebar contains a menu with "System" selected and "WAN" expanded, showing options like Dynamic IP, Static IP, PPPoE, PPTP, L2TP, Telstra Big Pond, and others. The main content area is titled "L2TP" and includes a description: "Layer Two Tunneling Protocol is a common connection method used in xDSL connections." Under "WAN Interface Settings", there are two radio buttons: "Obtain an IP address automatically:" (selected) and "Use the following IP address:". Below these are input fields for IP Address, Subnet Mask, and Default Gateway, all set to 0.0.0.0. The "L2TP Settings" section includes fields for User ID, Password, L2TP Gateway (0.0.0.0), Connection Type (set to Continuous), and Idle Time Out (0 minutes). There are "Connect" and "Disconnect" buttons next to the Connection Type dropdown. At the bottom right, there are "Apply" and "Cancel" buttons.

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.
	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 **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. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.

3.2.6 Telstra Big Pond

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

Параметр	Описание
User Name	Enter the User Name provided by your ISP for the Telstra Big Pond connection
Password	Enter the Password provided by your ISP for the Telstra Big Pond connection
User decide login server manually	Select if you want to assign the IP of Telstra Big Pond's login server manually
Login Server	The IP of the Login Server.

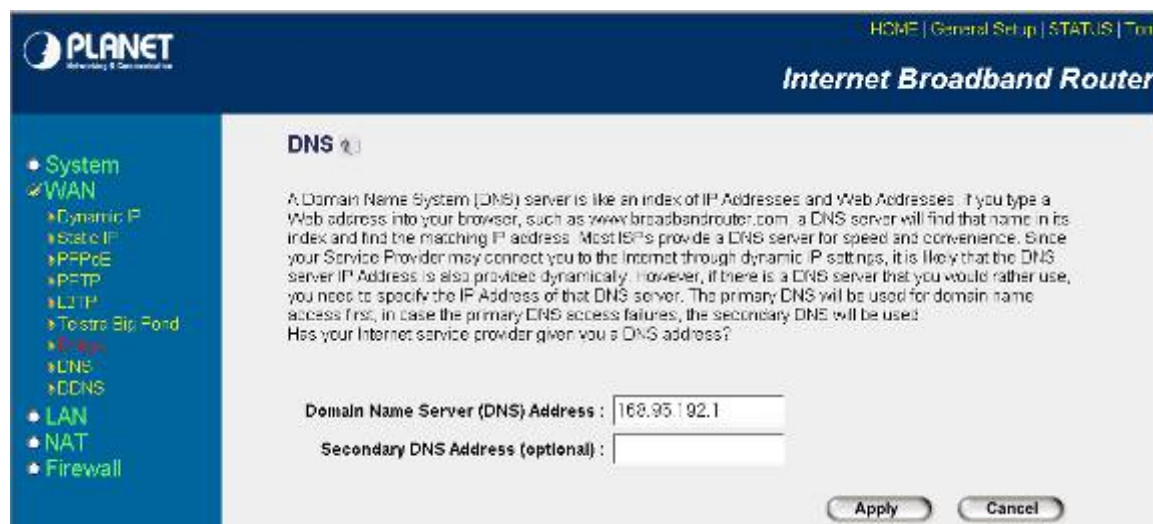
Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**. Если все настройки сделаны правильно, то после их сохранения можно использовать Ваш роутер для подключения к Интернет. Для тонкой настройки роутера обратитесь к разделам 3, 4, 5.

3.2.7 Сервер Доменных Имен (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 .com. 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**.

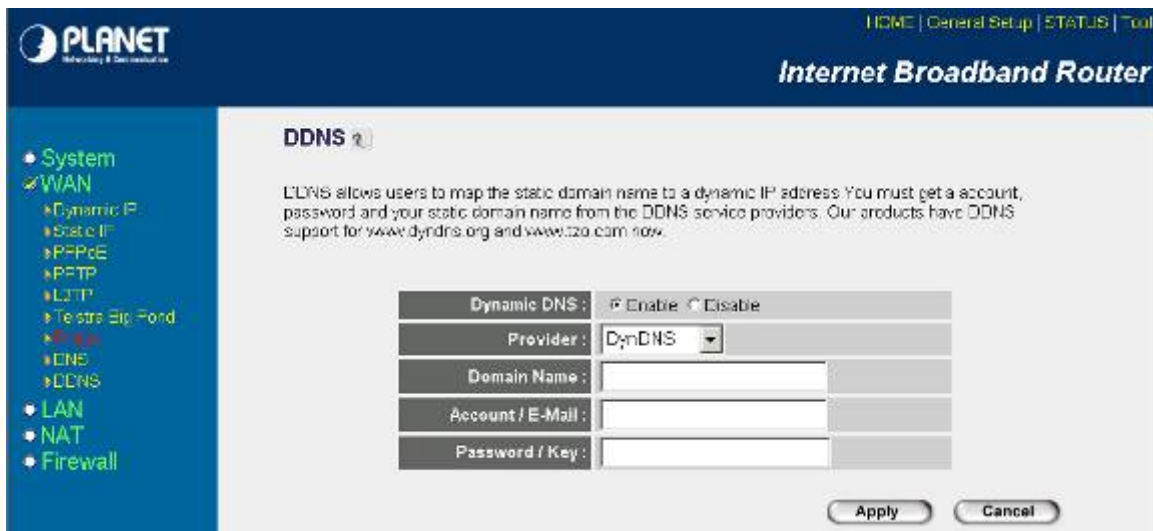


Параметр	Описание
Domain Name Server (DNS) Server	IP адрес Сервера Доменных Имен (DNS server) выданный Вам Интернет Провайдером или специфический IP адрес Вашего DNS сервера.
Secondary DNS Address (optional)	IP адрес резервного Сервера Доменных Имен (DNS server) выданный Вам Интернет Провайдером или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

3.2.8 Сервер Динамических Доменных Имен (DDNS)

Сервер Динамических Доменных Имен (DDNS) (требует регистрации на одном из сайтов поддерживаемых маршрутизатором 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 выделит 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

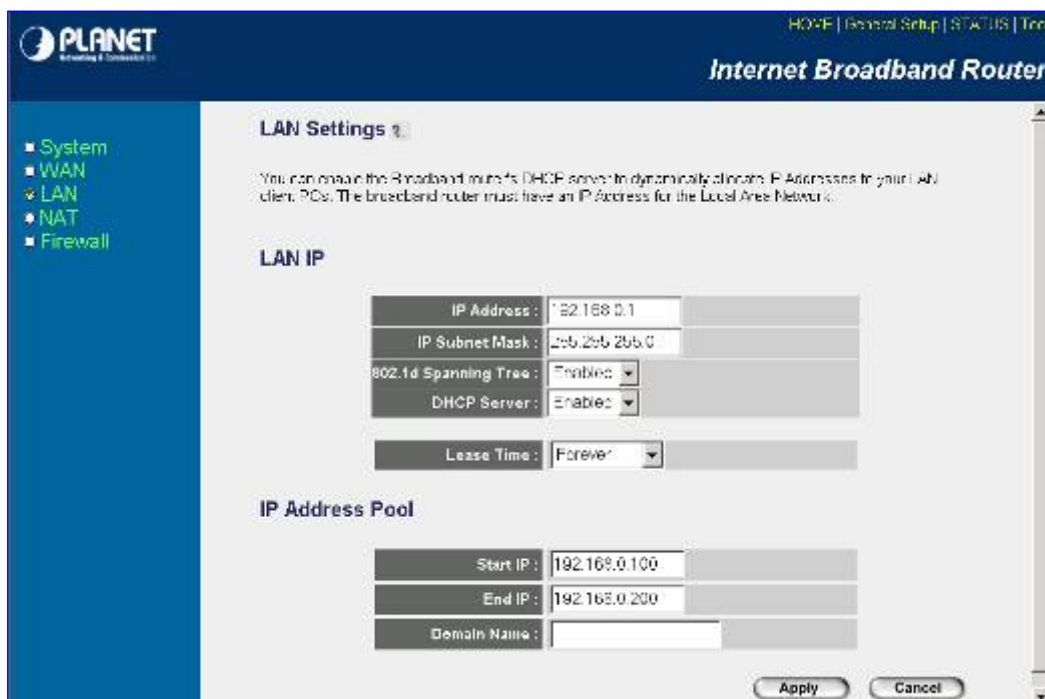
Нажмите кнопку **Apply**, после завершения настройки. Роутер сохранит изменения и выдаст сообщение: **Change Setting Successfully**. Нажмите кнопку **OK**.

Как использовать dynamic DNS:

XRT-401D поддерживает несколько поставщиков данного сервиса, у которых Вы можете зарегистрироваться, чтобы использовать эту функцию. Для получения подробных инструкций по настройке смотрите информацию на сайте выбранного поставщика службы DDNS.

3.3 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 vfhienbpfnjhf (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 apply . End IP – конечный IP адрес выдаваемый DHCP сервером в аренду Domain Name – Имя домена. В большинстве случаев это поле можно оставить пустым.
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 оставить пустым.	
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

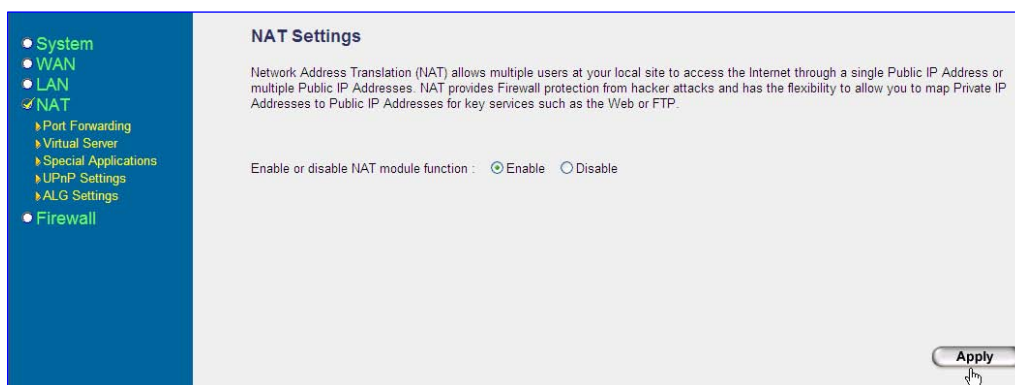
При настройке интерфейсов LAN и WAN обязательно убедитесь, что диапазон IP адресов в локальной сети маршрутизатора (порты LAN) и диапазоны IP адресов локальной сети провайдера (со стороны порта WAN) не пересекаются. При необходимости измените настройки LAN интерфейса, выбрав из таблицы диапазон IP адресов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

3.4 Трансляция Сетевых Адресов (NAT)

В режиме NAT все пользователи используют локальные IP адреса и при обращении к сети Интернет они скрыты извне 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 дополнительные

сервисы позволяющие осуществить проброс портов и обеспечить работу специальных приложений и протоколов, расположенных на хостах в локальной сети.

Вы можете отключить NAT. В этом случае XRT-401D 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.

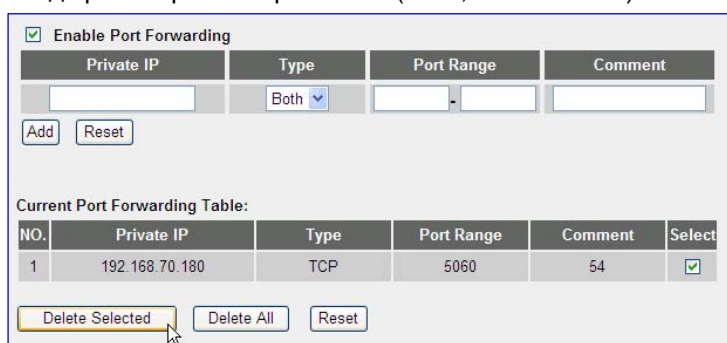


Параметр	Описание
3.4.1 Port Forwarding	Вы можете использовать различные службы (например, электронная почта, FTP, Web и т.д.) расположенные за NAT на разных хостах в вашей локальной сети и использующих различные сервисы к которым нужно разрешить доступ из Внешней сети (Интернет или Интранет). Перенаправление 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).
3.4.2 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 отличие от Перенаправления портов в этом меню нельзя указать диапазон портов, зато можно указать различные порты для внешнего и внутреннего интерфейса маршрутизатора.
3.4.3 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.
3.4.4 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".
3.4.5 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" сетевое образование, 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.

3.4.1 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)

3.4.2 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)

Enable Virtual Server

Private IP	Private Port	Type	Public Port	Comment
<input type="text"/>	<input type="text"/>	Both	<input type="text"/>	<input type="text"/>

Add Reset

Current Virtual Server Table:

NO.	Private IP	Private Port	Type	Public Port	Comment	Select
1	192.168.70.180	80	TCP	8082	ICA-106	<input checked="" type="checkbox"/>

Delete Selected Delete All Reset

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.

Параметр	Описание
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)

3.4.3 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.
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: Специальные Применения

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.

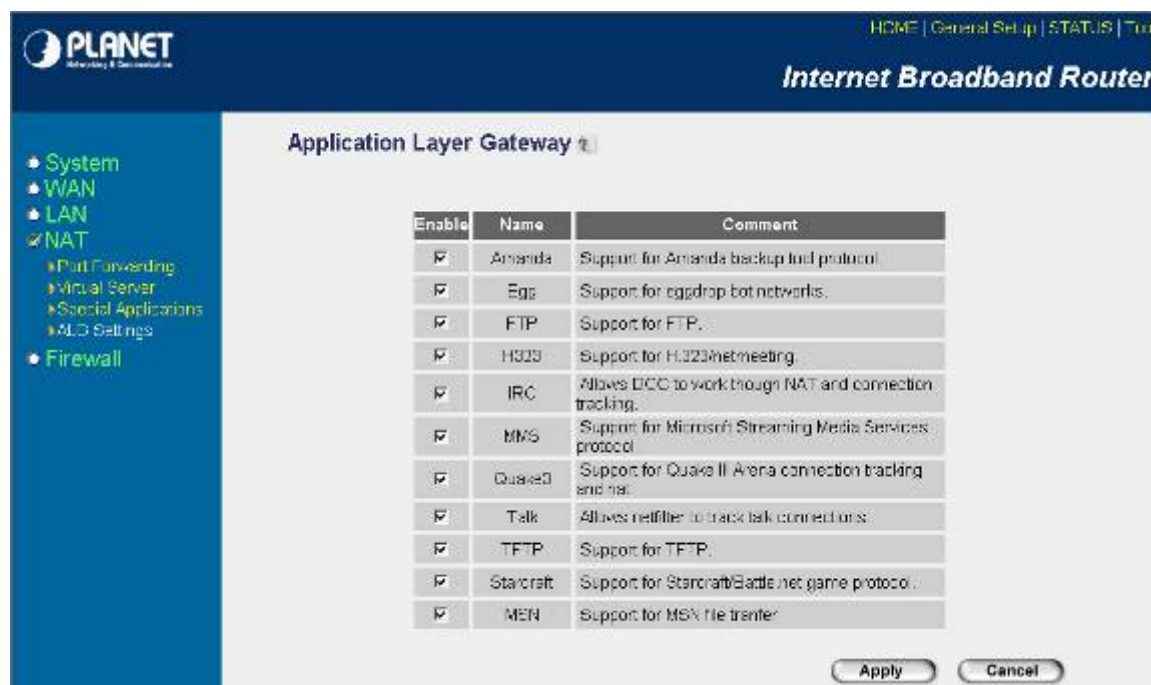
Пример:

ID	Trigger Port	Trigger Type	Public Порт	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 триггерный 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

3.4.4 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".

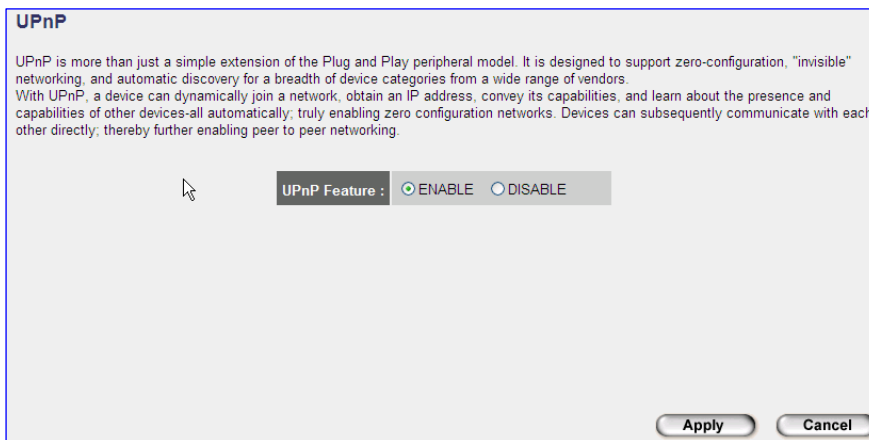


Параметр	Описание
Enable	Поставьте галочку напротив нужных приложений, чтобы обеспечить их правильную работу за NAT. По умолчанию: выбраны все приложения

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

3.4.5 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" сетевое образование, 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**.

3.5 Межсетевой Экран

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
2.5.1 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.
2.5.2 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.
2.5.3 DoS	Выбор видов атак, которые будет обрабатывать межсетевой экран роутера.
2.5.4 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

3.5.1 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	<p>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".</p> <p>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.</p> <p>Вы можете создать до 20 правил фильтрации по MAC адресам.</p> <p>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.</p>
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	<p>Нажмите кнопку Add PC – откроется новое окно добавления правила фильтрации по IP. Смотрите подробное описание ниже.</p> <p>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.</p> <p>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.</p>
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, Скаре и многие другие сервисы будут работать без проблем). Если это действительно Босс, то сисадмина видимо скоро попросят написать заявление на увольнение...

Client PC Description :	<input type="text" value="Boss"/>	
Client PC IP Address :	<input type="text" value="192.168.70.100"/>	
Client PC Service :		
Service Name	Detail Description	Select
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	<input checked="" type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input checked="" type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input checked="" type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 389,522,1503,1720,1731	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>
User Define Service		
Protocol :	<input type="text" value="Both"/>	
Port Range :	<input type="text"/>	
<input type="button" value="Add"/> <input type="button" value="Reset"/>		

3.5.2 Блокировка URL (URL Blocking)

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

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.

3.5.3 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

Измените необходимые настройки и нажмите Apply для сохранения изменений.

3.5.4 Демилитаризованная зона (DMZ)

Демилитаризованная зона – это зона, в которой не действуют правила и политики межсетевое 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 VM-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 4 Состояние устройства

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.

Параметр	Описание
4.1 Status	Общая информация о роутере (модель роутера, версия загрузчика, версия ПО, аппаратная версия, время непрерывной работы)
4.2 Internet Connection	Информация о типе используемого подключения для порта WAN и его текущие настройки
4.3 Device Status	Информация о настройках порта LAN
4.4 System Log	Информация системного журнала
4.5 Security Log	Информация о попытках любых зафиксированных атак на маршрутизатор
4.6 DHCP Client Table	Информация об активных DHCP клиентах
4.7 Statistics	Статистика принятых и отправленных пакетов

Выберите нужный пункт меню и перейдите к его подробному описанию

4.1 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)

Status and Information

You can use the Status page to monitor the connection status for the Broadband router's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.

System

Model	Broadband Router
Uptime	0day:19h:6m:42s
Hardware Version	Rev. A
Boot Code Version	1.0
Runtime Code Version	3.22

Current Time
1/12/2007 14:17:17

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

4.2 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

4.3 Состояние устройства (Device Status)

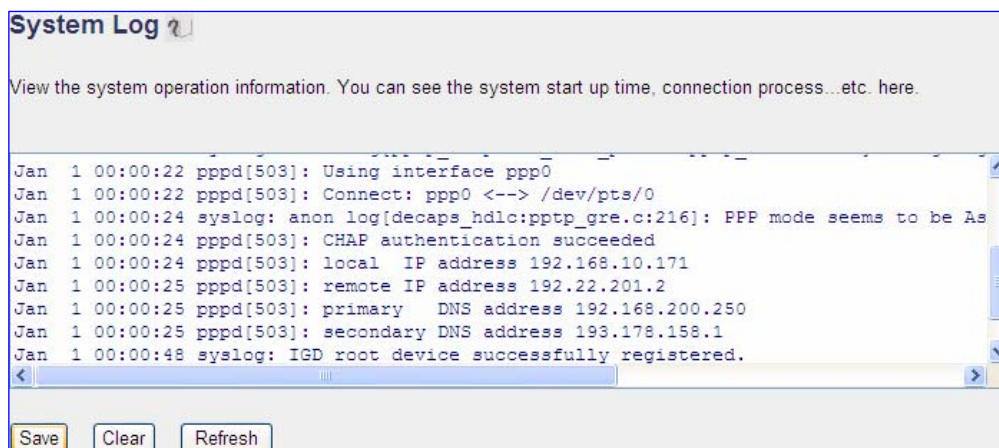
Информация о настройках порта LAN, которые были сделаны в меню [LAN](#).

LAN Configuration	
IP Address	192.168.70.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:30:4f:2f:0c:bd

Параметр	Описание
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

4.4 Системный журнал (System Log)

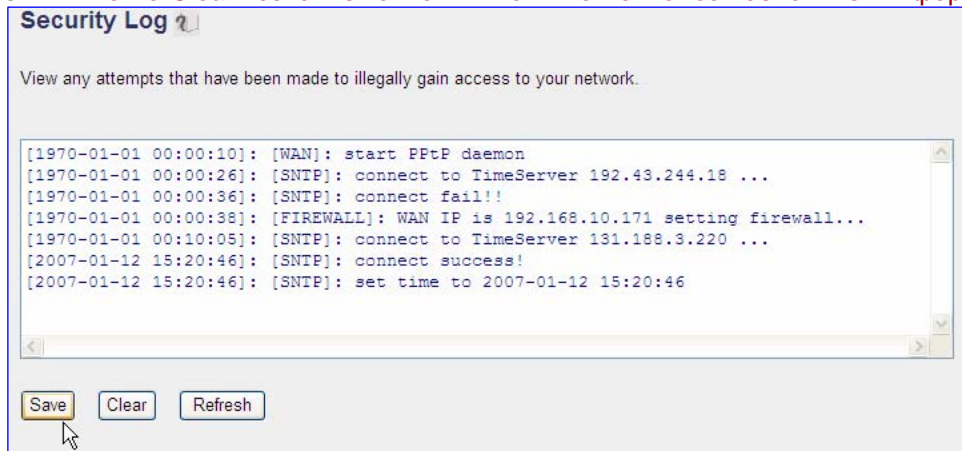
В этом журнале фиксируются все системные события. Вы можете сохранить эту информацию на жестком диске компьютера, нажав кнопку Save и указав директорию и Имя файла для сохранения. Кнопка Clear позволяет очистить лог. Кнопка Refresh обновляет информацию лога.



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

4.5 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.



4.6 Таблица активных DHCP клиентов

Информация об активных DHCP клиентах

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

Refresh

На этой странице показывается информация о всех клиентах DHCP Сервера – хостах в локальной сети получающие параметры сетевого окружения от DHCP сервера маршрутизатора и подключенных в настоящее время. Таблица Активных DHCP Клиентов выводит на экран монитора **IP** и **MAC Адрес** подключенного хоста и **Время** до окончания срока аренды адреса для каждого из клиентов в локальной сети. Кнопка **Refresh** позволяет обновить информацию в таблице.

4.7 Статистика

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

The screenshot shows a window titled "Statistics" with a help icon. Below the title is the text "This page shows the packet counters for transmission and reception regarding to networks." A table displays the following data:

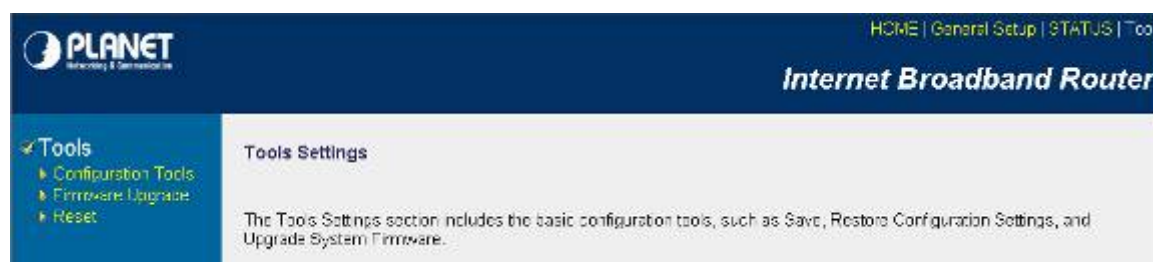
Ethernet LAN	Sent Packets	9793
	Received Packets	11428
Ethernet WAN	Sent Packets	2879
	Received Packets	5161

At the bottom of the window is a "Refresh" button with a mouse cursor pointing at it.

Раздел 5 Расширенное Администрирование

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
5.1 Configuration Tools	В этом разделе меню можно выполнить сохранение и восстановление конфигурации, а также выполнить сброс всех настроек роутера на значения по умолчанию.
5.2 Firmware Upgrade	Этот раздел меню предназначен для обновления программного обеспечения роутера
5.3 Reset	Этот раздел меню предназначен для принудительной перезагрузки роутера.

Выберите нужный пункт меню и перейдите к его подробному описанию

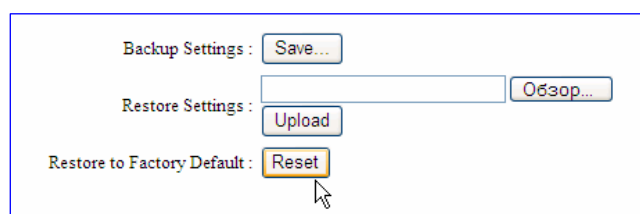
5.1 Инструмент Конфигурация (Configuration Tools)

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 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.

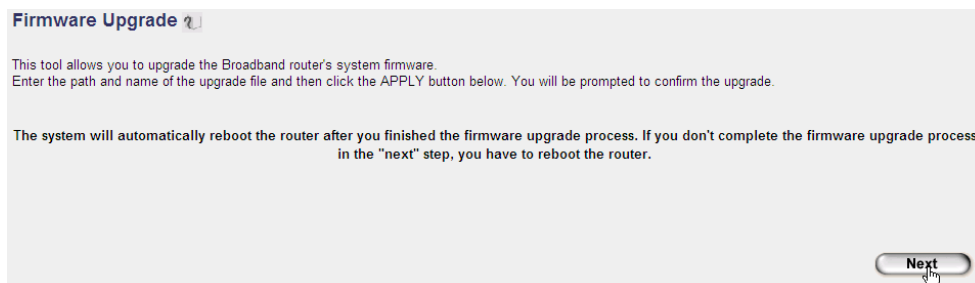
Внимание!: Во время восстановления конфигурации и сброса настроек нельзя выключать питание маршрутизатора и выполнять отключение и подключение интерфейсных кабелей! Дождитесь окончания процедуры восстановления конфигурации или сброса настроек.



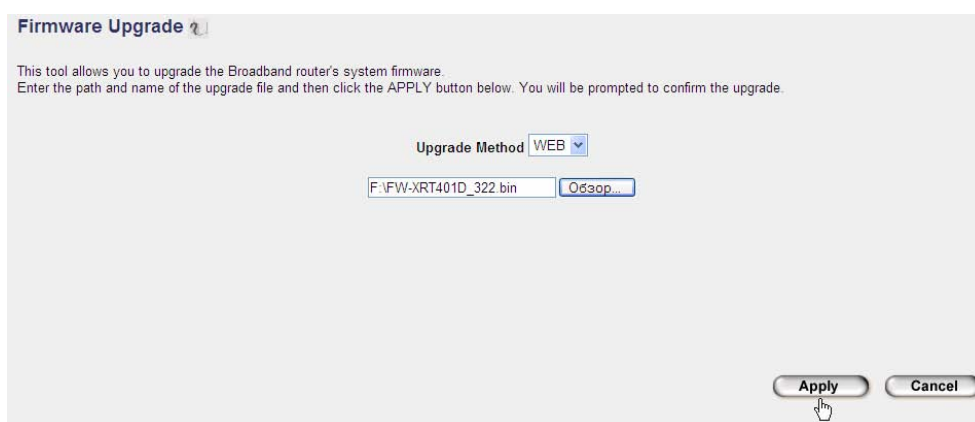
5.2 Обновление прошивки (Firmware Upgrade)

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. Впоследствии загрузите сохраненную конфигурацию.
 - ☞ Нельзя обновлять прошивку оборудования, если маршрутизатор работает нестабильно (периодически зависает). За дополнительной информацией обратитесь к [разделу 5.3](#)
- Соблюдение этих правил позволит избежать проблем при обновлении программного обеспечения роутера.

5.3 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 блокирует подключение к Интернет. Описание термина флуд смотрите в [Глоссарии сетевых терминов](#).
- Убедитесь в исправности сетевых адаптеров, кабелей, разъёмов, соединителей и их правильном и надёжном 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.

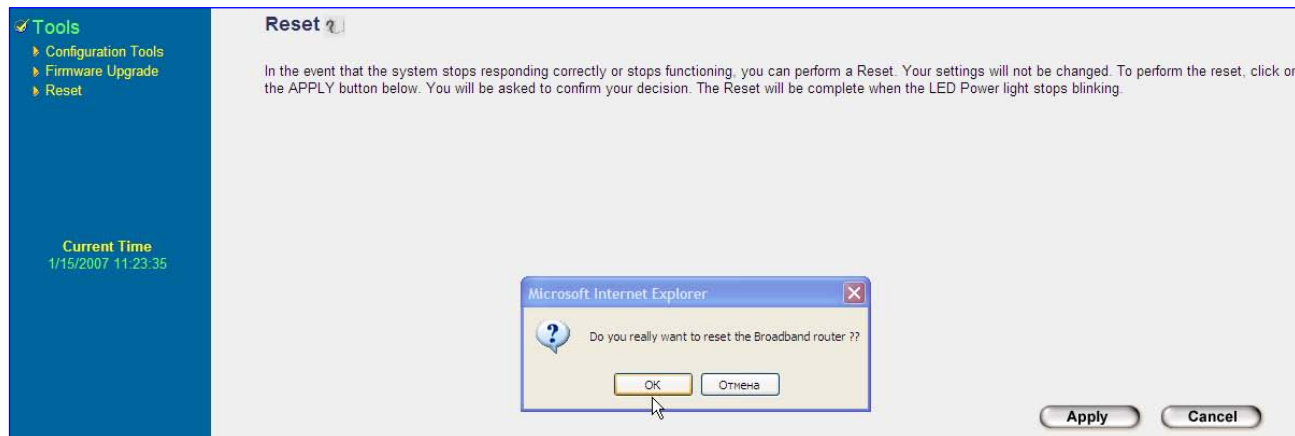
Если ни одно из вышеописанных действий не помогло, то рекомендуется обратиться в сервисный центр.

Внимание!:

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

5.4 Аппаратная перезагрузка (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.

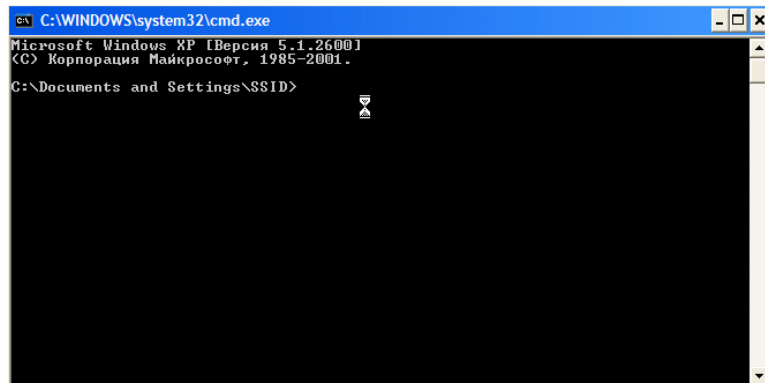
Внимание!:

- ☞ 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 А

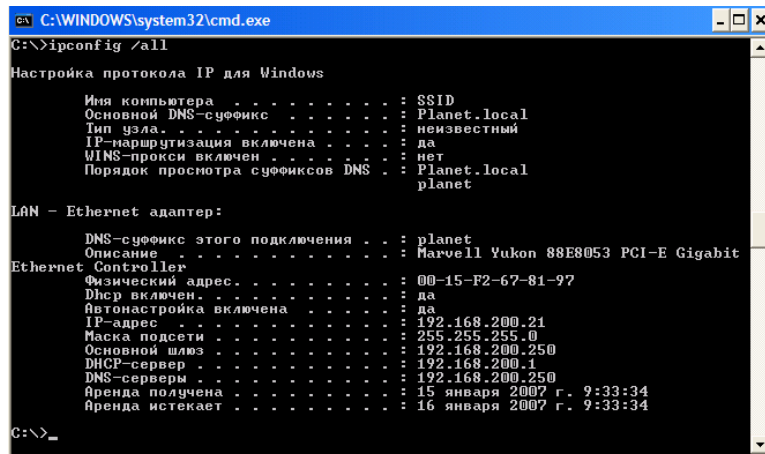
Как посмотреть в Windows MAC и IP адрес сетевого подключения Вашего компьютера и другие параметры сетевого подключения?

- 1) Откройте окно командной строки (Пуск ⇒ Выполнить... ⇒ cmd ⇒ нажмите Enter)



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.
C:\Documents and Settings\SSID>
```

- 2) наберите `ipconfig /all` и нажмите Enter



```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : SSID
Основной DNS-суффикс . . . . . : Planet.local
Тип узла . . . . . : неизвестный
IP-маршрутизация включена . . . . . : да
WINS-прокси включен . . . . . : нет
Порядок просмотра суффиксов DNS . . . . . : Planet.local
planet

LAN - Ethernet адаптер:

DNS-суффикс этого подключения . . . . . : planet
Описание . . . . . : Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Controller
Физический адрес . . . . . : 00-15-F2-67-81-97
Dhcp включен . . . . . : да
Автонастройка включена . . . . . : да
IP-адрес . . . . . : 192.168.200.21
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 192.168.200.250
DNS-сервер . . . . . : 192.168.200.1
DNS-серверы . . . . . : 192.168.200.250
Аренда получена . . . . . : 15 января 2007 г. 9:33:34
Аренда истекает . . . . . : 16 января 2007 г. 9:33:34

C:\>_
```

- 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)

Список терминов

Bridge (Мост): интеллектуальное устройство, соединяющее две локальные сети или удаленные сегменты в одну сеть. Функционирует на подуровне MAC канального уровня и прозрачен для протоколов более 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.

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.

Default Gateway (Router, Маршрутизатор): 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.

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.

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.

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

Idle Timeout: Этот параметр задает максимальный период непрерывного бездействия, по истечении которого пользовательский сеанс прерывается. Атрибут доступен для передачи от сервера к клиентам в пакетах Access-Асcept 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.

Firewall (Брандмауэр или Межсетевой экран) можно перевести как 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.

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.

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).

IP Address and Network (Subnet) Mask: IP-адрес) 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 чисел, отделенных символом точки: уууууууу. уууууууу. уууууууу. уууууууу, где каждый "у" 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-битовое 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 В. В верхнем примере происходит разделение на хосте, где идентификатор подсети и идентификатор хоста занимают 8 бит. В нижнем примере показано разделение адреса класса В, при этом идентификатор подсети занимает 10 бит, а идентификатор хоста - 6 бит.



Рисунок 3.7 Пример масок подсетей для двух различных подсетей класса В.

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: А, В или С (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 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).

ISP (Провайдер Сервиса Интернет): Провайдер предоставляющий услуги доступа в Интернет для частных пользователей или организаций.

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.

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.

Network	MTU (байты)
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

Рисунок 2.5 Типичные значения максимальных блоков передачи (MTU).

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.

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
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.

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.

Router (Маршрутизатор) - данный 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.

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.

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**.

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**.

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.

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 отправляет 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.