МОДЕМ P660RT2

Двухдиапазонный модем ADSL2+ Annex A/B с портом Ethernet

Руководство пользователя

Версия 3.40
12/2006
Редакция 1

ZyXEL

www.zyxel.com

О данном Руководстве пользователя

Для кого предназначено данное Руководство

Данное руководство предназначено для тех, кто планирует производить настройку P660RT2 с помощью Web-конфигуратора. Для работы с Руководством необходимо обладать основными знаниями о топологии и принципах организации сетей TCP/IP.

Примечание: Зарегистрируйте ваше изделие ZyXEL через Интернет по адресу *zyxel.ru* для России, *ua.zyxel.com* – для Украины и *zyxel.kz* – для Казахстана. Регистрация изделия дает дополнительный год бесплатной гарантии, персональную техническую поддержку, уведомление по электронной почте об обновлениях, ряд других преимуществ и льгот.

Сопроводительная документация

- Краткое руководство

  Краткое руководство разработано для быстрого изучения и начала работы с устройством. В нем содержится информация о настройке сети и организации доступа в Интернет.
- Встроенная справка Web-конфигуратора

  Встроенная web-справка, содержащая описания отдельных окон и дополнительную информацию.

Рекомендуется выполнять настройку P660RT2 с помощью содержащейся на прилагаемом диске программы ZyXEL NetFriend.

- Справочный компакт-диск

  На входящем в комплект компакт-диске имеется программа быстрой настройки ZyXEL NetFriend, а также справочная документация.
- Web-сайт корпорации ZyXEL

  Сертификаты на изделие, а также дополнительную документацию см. на сайте www.zyxel.com.

Обратная связь с пользователями

Помогите нам помочь вам. Все комментарии, относящиеся к Руководству пользователя, вопросы и предложения по улучшению направляйте нам через Интерактивную систему консультаций в разделе «Поддержка» на сайте www.zyxel.ru. Спасибо

Обозначения, принятые в документе

Предупреждения и примечания

Предупреждения и примечания в данном Руководстве пользователя представлены следующем образом:

Значком "предупреждение" отмечены пункты, содержание которых предупреждает о возможном нанесении вреда пользователю или устройству.

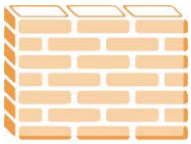
Значком "примечание" помечается важная информация (например, необходимость настройки других параметров или полезные подсказки), рекомендации, относящиеся к теме.

Условные обозначения

- Далее в данном Руководстве пользователя ZyXEL P660RT2 может именоваться как “P660RT2”, “устройство”, “система” или “изделие”.
- Надписи на изделии, имена окон, имена полей и пункты меню обозначаются **жирным** шрифтом.
- Название клавиш указаны прописными буквами в квадратных скобках, например, [ENTER] означает клавишу «ввод» или «возврат каретки» на клавиатуре.
- Указание «Введите...» означает, что следует набрать один или несколько символов и затем нажать клавишу [ENTER]. “Выберите” означает, что Вам следует использовать одну из предложенных опций.
- Правая угловая скобка (>) между названиями окон означает нажание кнопки мыши. Например, «Maintenance» (Сопровождение) > «Tools» (Средства) > «Configuration» (Конфигурация) означает, что для отображения этого окна сначала необходимо выбрать «Maintenance» (Сопровождение) в панели навигации, затем подменю «Tools» (Средства) и, далее, закладку «Configuration» (Конфигурация).
- Единицы измерения могут указывать как на “метрические”, так и на “научные” величины. Например, приставка «к» (кило) может означать как 1000, так и 1024, приставка «М» — 1000000 или 1048576 и т. д.

Используемые пиктограммы

В схемах данного Руководства используются следующие пиктограммы: Значок P660RT2 является схематичным изображением устройства.

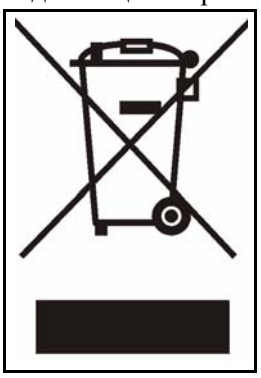
P660RT2	Компьютер	Ноутбук
Сервер	Концентратор DSLAM	Межсетевой экран 
Телефон	Коммутатор	Маршрутизатор

Техника безопасности

Для обеспечения безопасности необходимо ознакомиться и следовать следующим правилам.

- Не используйте изделие в непосредственной близости от воды, например, во влажных подвалах или рядом с бассейном.
- Не подвергайте устройство воздействию влаги, пыли или агрессивных жидкостей.
- Не кладите на устройство предметы.
- ЗАПРЕЩАЕТСЯ устанавливать, использовать и ремонтировать устройство во время грозы. Существует определенный риск получить удар электрическим током при разряде молнии.
- Подключайте к устройству ТОЛЬКО соответствующие комплектующие.
- Техническое обслуживание и разборка данного устройства должны выполняться только квалифицированным техническим персоналом.
- Убедитесь, что все кабели подключены к соответствующим портам.
- Прокладывайте соединительные кабели в местах, где никто не будет наступать на них или спотыкаться.
- Всегда отсоединяйте от устройства все кабели перед обслуживанием или разборкой.
- Используйте для устройства ТОЛЬКО соответсвующий адаптер или шнур питания. Подключайте кабель питания к сети электропитания с соответствующим напряжением (110 В переменного тока в Северной Америке или 230 В переменного тока в Европе).
- НЕ кладите на кабель или адаптер питания какие-либо предметы и не располагайте его в местах, где могут ходить люди.
- НЕ используйте устройство, если кабель или адаптер питания неисправен, так как это может привести к поражению электрическим током.
- Если кабель или адаптер питания поврежден, отключите его от розетки электропитания и от устройства.
- НЕ пытайтесь ремонтировать кабель или адаптер питания. Для заказа нового адаптера питания свяжитесь с местным поставщиком.
- Не заслоняйте вентиляционные отверстия устройства, так как недостаточный приток воздуха может стать причиной повреждения устройства.
- Используйте только телекоммуникационный кабель No. 26 AWG (American Wire Gauge - американская система калибровки проводов) или большего размера.
- При настенной установке устройства убедитесь, что при монтаже не будут повреждены электропроводка, газо- или водопроводы.

Материалы изделие пригодны для переработки. Утилизация должна производиться надлежащим образом.



Краткое содержание

Введение. Мастер подключения 23

Знакомство с P660RT2 25
Знакомство с Web-конфигуратором 29
Мастер настройки доступа в Интернет 41

Web-конфигуратор 51

Настройка глобальной сети 53
Настройка локальной сети 73
Окна NAT (Трансляция сетевых адресов) 87
Статический маршрут 101
Настройка динамической системы доменных имен (DYNDNS) 105
Настройка удаленного управления 109
Универсальная функция Plug and Play (UPnP) 121

Служебные программы и поиск/устранение неисправностей 133

Система 135
Программные средства 141
Диагностика 147
Поиск и устранение неисправностей 149

Приложения и алфавитный указатель 155

Содержание

О данном Руководстве пользователя 3

Обозначения, принятые в документе 4

Техника безопасности 6

Краткое содержание 9

Содержание 11

Список рисунков 17

Список таблиц 21

Часть I: Введение. Мастер подключения 23

Глава ... 1
Знакомство с P660RT2 25

1.1 Обзор 25
1.2 Способы управления устройством P660RT2 26
1.3 Полезные советы по управлению P660RT2 26
1.4 P660RT2 — Установка и подключение оборудования 27
1.5 Светодиоды 27

Глава ... 2
Знакомство с Web-конфигуратором 29

2.1 Знакомство с Web-конфигуратором 29
2.2 Доступ к Web-конфигуратору 29
2.3 Интерфейс Web-конфигуратора 32
2.3.1 Панель навигации 32
2.3.2 Окно «Status» (Состояние) 34
2.3.3 Состояние: Таблица IP-адресов 37
2.3.4 Состояние: Статистика пакетов 37
2.3.5 Изменение пароля 39

Глава ... 3
Мастер настройки доступа в Интернет 41

3.1 Введение 41
3.2 Мастер настройки доступа в Интернет 41

3.2.1 Автоматическое определение 43
3.2.2 Ручная настройка 44

Часть II: Web-конфигуратор 51

Глава ... 4
Настройка глобальной сети 53

4.1 Общая информация о глобальной сети 53
4.1.1 Инкапсуляция 53
4.1.2 Мультиплексирование 54
4.1.3 Сценарии инкапсуляции и мультиплексирования 55
4.1.4 VPI и VCI 55
4.1.5 Назначение IP-адреса 55
4.1.6 Полупостоянное соединение (PPP) 56
4.1.7 NAT 56
4.2 Метрика 56
4.3 Формирование трафика 57
4.3.1 Классы трафика ATM 58
4.4 Подключение к Интернету 59
4.4.1 Дополнительные параметры подключения к Интернет 62
4.5 Настройка других соединений 64
4.5.1 Редактирование других соединений 65
4.5.2 Настройка дополнительных параметров других соединений 67
4.6 Перенаправление трафика 69
4.7 Настройка резервного соединения с глобальной сетью 70

Глава ... 5
Настройка локальной сети 73

5.1 Описание локальных сетей 73
5.1.1 Локальные, глобальные сети и P660RT2 73
5.1.2 Настройка DHCP 74
5.2 Адреса серверов DNS 74
5.3 Настройка TCP/IP локальной сети 75
5.3.1 IP-адрес и маска подсети 75
5.3.2 Настройка RIP 76
5.3.3 Многоадресная рассылка 76
5.3.4 Any IP (Любой IP) 77
5.4 Настройка IP-адреса в локальной сети 79
5.4.1 Настройка дополнительных параметров локальной сети 80
5.5 Настройка DHCP 82
5.6 Список клиентов LAN 83

5.7 Псевдоним IP локальной сети 84

Глава ... 6
Окна NAT (Трансляция сетевых адресов) 87

6.1 Обзор NAT 87
6.1.1 Определения NAT 87
6.1.2 Назначение NAT 88
6.1.3 Как работает NAT 88
6.1.4 Применение NAT 89
6.1.5 Типы отображения NAT 89
6.2 SUA (Учетная запись одиночного пользователя) в сравнении с NAT 90
6.2.1 Шлюз SIP ALG 91
6.3 Настройка общих параметров NAT 91
6.4 Переадресация портов 92
6.4.1 IP-адрес сервера по умолчанию 93
6.4.2 Переадресация портов: Службы и номера портов 93
6.4.3 Пример настройки серверов, находящихся за преобразованием портов 93
6.5 Настройка переадресации портов 94
6.5.1 Изменение правила переадресации портов 95
6.6 Отображение адресов 97
6.6.1 Редактирование правил отображения адресов 99

Глава ... 7
Статический маршрут 101

7.1 Статический маршрут 101
7.2 Настройка статических маршрутов 101
7.2.1 Изменение статического маршрута 103

Глава ... 8
Настройка динамической системы доменных имен (DYNDNS) 105

8.1 Динамическая система доменных имен (DYNDNS) – общая информация 105
8.1.1 Маски DYNDNS 105
8.2 Настройка динамической DNS (DYNDNS) 106

Глава ... 9
Настройка удаленного управления 109

9.1 Удаленное управление – общая информация 109
9.1.1 Ограничения на удаленное управление 109
9.1.2 Удаленное управление и NAT 110
9.1.3 Время простоя системы 110
9.2 WWW 110
9.3 Управление с помощью Telnet 111
9.4 Настройка Telnet 111

9.5 Настройка FTP 113
9.6 Протокол SNMP 114
9.6.1 Поддерживаемые базы управляющей информации 115
9.6.2 Прерывания SNMP 115
9.6.3 Конфигурирование SNMP 116
9.7 Настройка DNS 117
9.8 Настройка ICMP 118

Глава . 10
Универсальная функция Plug and Play (UPnP) 121

10.1 Описание универсальной функции Plug and Play 121
10.1.1 Как узнать, используется ли UPnP? 121
10.1.2 NAT Transversal 121
10.1.3 Предупреждения по использованию UPnP 122
10.2 UPnP и ZyXEL 122
10.2.1 Настройка UPnP 122
10.3 Пример установки UPnP в Windows 123
10.3.1 Установка UPnP в Windows Me 123
10.3.2 Установка UPnP в Windows XP 125
10.4 Пример использования UPnP в Windows XP 126
10.4.1 Автоматическое обнаружение сетевого устройства UPnP 126
10.4.2 Простой доступ к Web-конфигуратору 129

Часть III: Служебные программы и поиск/устранение неисправностей 133

Глава . 11
Система.....135

11.1 Настройка общих параметров 135
11.1.1 Настройка общих параметров и ввод системного имени 135
11.1.2 Настройка общих параметров 135
11.2 Установка времени 138

Глава . 12
Программные средства 141

12.1 Обновление микропрограммы 141
12.2 Окно конфигурации 143
12.2.1 Резервное сохранение конфигурации 144
12.2.2 Восстановление конфигурации 144
12.2.3 Восстановление заводских настроек по умолчанию 145
12.3 Перезапуск 145

Глава . 13
Диагностика 147

13.1 Общая диагностика 147
13.2 Диагностика линии DSL 148

Глава . 14
Поиск и устранение неисправностей 149

14.1 Питание, подключение оборудования и светодиоды 149
14.2 Доступ и регистрация в P660RT2 150
14.3 Доступ в Интернет 152
14.4 Сброс настроек модема P660RT2 к заводским установкам 153
14.4.1 Использование кнопки сброса настроек 153

Часть IV: Приложения и алфавитный указатель 155

Приложение A Технические характеристики 157
Приложение B Инструкции по настенному монтажу 161
Приложение C Разделители частот и микрофильтры 163
Приложение D Настройка IP-адреса компьютера 167
Приложение E Всплывающие окна, сценарии и разрешения Java 183
Приложение F IP-адреса и организация подсетей 191
Приложение G Конфликты при назначении IP-адресов 201
Приложение H Службы Интернет 205
Приложение I Интерпретатор команд 209
Приложение J Правовая информация 215
Приложение K Сервисная служба 219
Алфавитный указатель 223

Список рисунков

Рис. 1 Использование P660RT2 для организации доступа в Интернет 25
Рис. 2 Использование P660RT2 для соединения локальных сетей 25
Рис. 3 Окно ввода пароля 30
Рис. 4 Изменение пароля при входе 31
Рис. 5 Выбор режима 31
Рис. 6 Web-конфигуратор: Главное окно 32
Рис. 7 Окно «Status» (Состояние) 35
Рис. 8 Состояние: Таблица IP-адресов 37
Рис. 9 Состояние: Статистика пакетов 38
Рис. 10 Общая информация о системе 40
Рис. 11 Выбор режима 42
Рис. 12 Мастер установки: Приветствие 42
Рис. 13 Автоопределение: Соединение DSL отсутствует 43
Рис. 14 Автоопределение: Отказ 43
Рис. 15 Автоопределение: PPPoE 44
Рис. 16 Мастер настройки доступа в Интернет: Параметры Интернет-провайдера 44
Рис. 17 Подключение к Интернету с использованием PPPoE 46
Рис. 18 Подключение к Интернету с использованием RFC 1483 46
Рис. 19 Подключение к Интернету с использованием ENET ENCAP (Протокол маршрутизации канального уровня с инкапсуляцией MAC) 47
Рис. 20 Подключение к Интернету с использованием PPPoA 48
Рис. 21 Неудачный тест подключения 1 49
Рис. 22 Неудачный тест подключения 2 49
Рис. 23 Завершение работы Мастера настройки доступа в Интернет 50
Рис. 24 Пример формирования трафика 58
Рис. 25 Подключение к Интернету (PPPoE) 59
Рис. 26 Дополнительные параметры подключения к Интернет 62
Рис. 27 Другие соединения 64
Рис. 28 Редактирование других соединений 65
Рис. 29 Настройка дополнительных параметров других соединений 68
Рис. 30 Пример перенаправления трафика 69
Рис. 31 Настройка локальной сети с перенаправлением трафика 70
Рис. 32 Настройка резервного подключения к глобальной сети 70
Рис. 33 Локальные и глобальные IP-адреса 73
Рис. 34 Пример: Любой IP 77
Рис. 35 IP-адрес в локальной сети 79
Рис. 36 Дополнительная настройка локальной сети 80
Рис. 37 Настройка DHCP 82

Рис. 38 Список клиентов LAN 83
Рис. 39 Физическая сеть и ее разделение на логические сети 85
Рис. 40 Псевдоним IP локальной сети 85
Рис. 41 Как работает NAT 88
Рис. 42 Применение NAT с использованием псевдонимов IP 89
Рис. 43 NAT: Общие параметры 91
Рис. 44 Пример: несколько серверов расположены за NAT 93
Рис. 45 Переадресация портов NAT 94
Рис. 46 Настройка правила переадресации портов 96
Рис. 47 Правила отображения адресов 97
Рис. 48 Редактирование правил отображения адресов 99
Рис. 49 Пример топологии статической маршрутизации 101
Рис. 50 Статический маршрут 102
Рис. 51 Изменение статического маршрута 103
Рис. 52 Динамическая система доменных имен (DYNDNS) 106
Рис. 53 Удаленное управление: WWW 110
Рис. 54 Настройка Telnet в сети TCP/IP 111
Рис. 55 Удаленное управление: Telnet 112
Рис. 56 Удаленное управление: FTP 113
Рис. 57 Модель управления SNMP 114
Рис. 58 Удаленное управление: SNMP 116
Рис. 59 Удаленное управление: DNS 118
Рис. 60 Удаленное управление: ICMP 119
Рис. 61 Настройка UPnP 122
Рис. 62 Установка и удаление программ: Установка Windows: Связь 124
Рис. 63 Установка и удаление программ: Установка Windows: Связь: Компоненты 124
Рис. 64 Сетевые подключения 125
Рис. 65 Мастер дополнительных компонентов Windows 125
Рис. 66 Сетевые службы 126
Рис. 67 Сетевые подключения 127
Рис. 68 Свойства подключения к Интернет 127
Рис. 69 Свойства подключения к Интернет: Дополнительные настройки 128
Рис. 70 Свойства подключения к Интернет: Дополнительные настройки: Добавить 128
Рис. 71 Значок в области уведомлений (на панели задач) 129
Рис. 72 Состояние подключения к Интернет 129
Рис. 73 Сетевые подключения 130
Рис. 74 Сетевые подключения: Сетевое окружение 131
Рис. 75 Пример – Сетевые подключения: Сетевое окружение: Свойства 131
Рис. 76 Общая настройка системы 136
Рис. 77 Установка системного времени 138
Рис. 78 Обновление микропрограммы 141
Рис. 79 Выполняется загрузка микропрограммы 142
Рис. 80 Временное отключение сети 143

Рис. 81 Сообщение об ошибке 143
Рис. 82 Configuration (Конфигурация) 143
Рис. 83 Конфигурация успешно восстановлена 144
Рис. 84 Временное отключение сети 145
Рис. 85 Ошибка восстановления конфигурации 145
Рис. 86 Окно перезапуска 146
Рис. 87 Диагностика: Общая информация 147
Рис. 88 Диагностика: Линия DSL 148
Рис. 89 Пример настенного монтажа 162
Рис. 90 Подключение телефонного сплиттера 163
Рис. 91 Подключение микрофильтра 164
Рис. 92 Подключение микрофильтра и Y-образного разъема 165
Рис. 93 Установка P660RT2 для работы по ISDN 165
Рис. 94 WIndows 95/98/Me: Сеть: Конфигурация 168
Рис. 95 Windows 95/98/Me: Свойства протокола TCP/IP: IP-адрес 169
Рис. 96 Windows 95/98/Me: Свойства протокола TCP/IP: Конфигурация DNS 170
Рис. 97 Windows XP: Меню Пуск 171
Рис. 98 Windows XP: Control Panel (Windows XP: Панель управления 171
Рис. 99 Windows XP: Панель управления: Сетевые подключения: Свойства 172
Рис. 100 Windows XP: Подключение по локальной сети: Свойства 172
Рис. 101 Windows XP: Свойства: Протокол Интернета (TCP/IP) 173
Рис. 102 Windows XP: Дополнительные свойства TCP/IP 174
Рис. 103 Windows XP: Свойства: Протокол Интернета (TCP/IP) 175
Рис. 104 Macintosh OS 8/9: Меню Apple 176
Рис. 105 Macintosh OS 8/9: TCP/IP 176
Рис. 106 Macintosh OS X: Меню Apple 177
Рис. 107 Macintosh OS X: Сеть 178
Рис. 108 Red Hat 9.0: KDE: Конфигурация сети: Устройства 179
Рис. 109 Red Hat 9.0: KDE: Устройство Ethernet: Общие 180
Рис. 110 Red Hat 9.0: KDE: Конфигурация сети: DNS 180
Рис. 111 Red Hat 9.0: KDE: Конфигурация сети: Включить 181
Рис. 112 Red Hat 9.0: Настройка динамического IP-адреса в файле «ifconfig-eth0» 181
Рис. 113 Red Hat 9.0: Настройка статического IP-адреса в файле «ifconfig-eth0» 181
Рис. 114 Red Hat 9.0: Установка параметров DNS в файле «resolv.conf» 182
Рис. 115 Red Hat 9.0: Перезапуск карты Ethernet 182
Рис. 116 Red Hat 9.0: Проверка свойств протокола TCP/IP 182
Рис. 117 Блокирование всплывающих окон 184
Рис. 118 Свойства обозревателя: Конфиденциальность 184
Рис. 119 Свойства обозревателя: Конфиденциальность 185
Рис. 120 Параметры блокирования всплывающих окон 186
Рис. 121 Свойства обозревателя : Безопасность 187
Рис. 122 Параметры безопасности – Выполнение сценариев приложений Java 187
Рис. 123 Параметры безопасности – Java 188

Рис. 124 Java (Sun) 189
Рис. 125 Номер сети и идентификатор узла 192
Рис. 126 Пример организации подсетей: до разделения на подсети 195
Рис. 127 Пример организации подсетей: после разделения на подсети 195
Рис. 128 Конфликт IP-адресов: Случай A 201
Рис. 129 Конфликт IP-адресов: Случай B 202
Рис. 130 Конфликт IP-адресов: Случай C 202
Рис. 131 Конфликт IP-адресов: Случай D 203
Рис. 132 Пример команды "routing" 210
Рис. 133 Backup Gateway (Резервный шлюз) 212
Рис. 134 Пример команды "routing" 213

Список таблиц

Табл. 1 Стандарты ADSL 26
Табл. 2 Описание светодиодов 27
Табл. 3 Сводная таблица окон Web-конфигуратора 32
Табл. 4 Окно «Status» (Состояние) 35
Табл. 5 Состояние: Таблица IP-адресов 37
Табл. 6 Состояние: Статистика пакетов 38
Табл. 7 Мастер настройки доступа в Интернет: Параметры Интернет-провайдера 45
Табл. 8 Подключение к Интернету с использованием PPPoE 46
Табл. 9 Подключение к Интернету с использованием RFC 1483 47
Табл. 10 Подключение к Интернету с использованием ENET ENCAP 47
Табл. 11 Подключение к Интернету с использованием PPPoA 48
Табл. 12 Подключение к Интернету 60
Табл. 13 Дополнительные параметры подключения к Интернет 62
Табл. 14 Другие соединения 64
Табл. 15 Редактирование других соединений 65
Табл. 16 Настройка дополнительных параметров других соединений 68
Табл. 17 Настройка резервного подключения к глобальной сети 71
Табл. 18 IP-адрес в локальной сети 79
Табл. 19 Дополнительная настройка локальной сети 80
Табл. 20 Настройка DHCP 82
Табл. 21 Список клиентов LAN 84
Табл. 22 Псевдоним IP локальной сети 85
Табл. 23 Определения NAT 87
Табл. 24 Типы отображения NAT 90
Табл. 25 NAT: Общие параметры 91
Табл. 26 Переадресация портов NAT 94
Табл. 27 Настройка правила переадресации портов 96
Табл. 28 Правила отображения адресов 97
Табл. 29 Edit Address Mapping Rule (Редактирование правил отображения адресов) 99
Табл. 30 Статический маршрут 102
Табл. 31 Изменение статического маршрута 103
Табл. 32 Динамическая система доменных имен (DYNDNS) 106
Табл. 33 Удаленное управление: WWW 110
Табл. 34 Удаленное управление: Telnet 112
Табл. 35 Удаленное управление: FTP 113
Табл. 36 Прерывания SNMP 115
Табл. 37 Удаленное управление: SNMP 116
Табл. 38 Удаленное управление: DNS 118

Табл. 39 Удаленное управление: ICMP 119
Табл. 40 Настройка UPnP 123
Табл. 41 Общая настройка системы 136
Табл. 42 Установка системного времени 138
Табл. 43 Обновление микропрограммы 142
Табл. 44 Сопровождение: Восстановление конфигурации 144
Табл. 45 Диагностика: Общая информация 147
Табл. 46 Диагностика: Линия DSL 148
Табл. 47 Устройство 157
Табл. 48 Встроенное программное обеспечение 158
Табл. 49 Характеристики встроенного программного обеспечения 159
Табл. 50 Пример номера сети и идентификатора узла в IP-адресе 192
Табл. 51 Маска подсети 193
Табл. 52 Максимальное число узлов 193
Табл. 53 Альтернативные варианты записи маски подсети 194
Табл. 54 Подсеть 1 196
Табл. 55 Подсеть 2 196
Табл. 56 Подсеть 3 197
Табл. 57 Подсеть 4 197
Табл. 58 Восемь подсетей 197
Табл. 59 Проектирование подсетей в сети с 24-битным номером сети 198
Табл. 60 Проектирование подсетей в сети с 16-битным номером сети 198
Табл. 61 Наиболее часто используемые службы 205

Часть I
Введение. Мастер подключения

Знакомство с P660RT2(25)
Знакомство с Web-конфигуратором(29)
Мастер настройки доступа в Интернет(41)

1

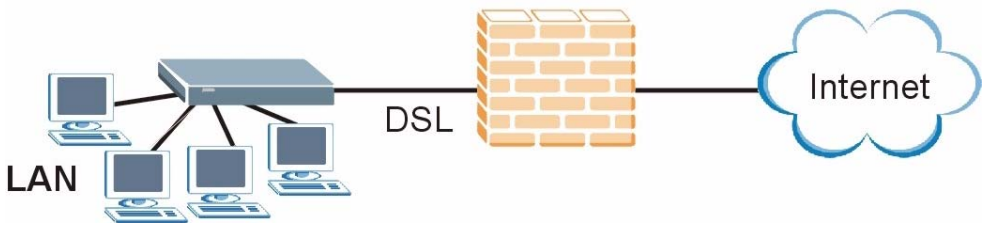
Знакомство с P660RT2

В этой главе рассказывается об основных функциях и сферах применения P660RT2, а также о способах управления устройством P660RT2.

1.1 Обзор

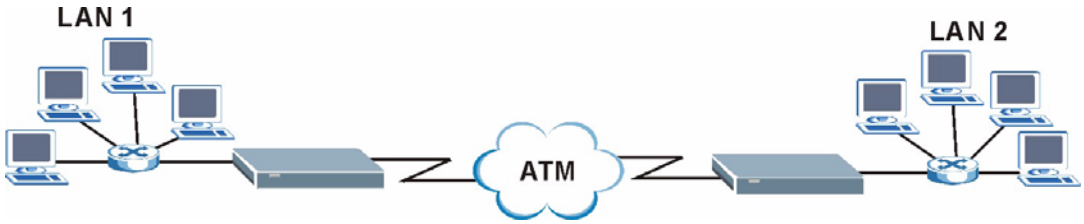
Устройство P660RT2 предназначено для организации высокоскоростного доступа в Интернет в домашних условиях. Типичный пример организации доступа в Интернет приводится ниже. Подробные характеристики устройства см. в Прил. А на с. 157.

Рис. 1 Использование P660RT2 для организации доступа в Интернет



P660RT2 можно использовать для соединения с помощью линии ADSL двух географически разделенных сетей. Далее представлен типичный пример организации соединения локальных сетей с помощью P660RT2.

Рис. 2 Использование P660RT2 для соединения локальных сетей



P660RT2 является маршрутизатором ADSL, совместимым со стандартами ADSL/ADSL2/ADSL2+. Устройство обеспечивает высокоскоростной доступ в Интернет по аналоговым (POTS) или цифровым (ISDN) телефонным линиям. В следующей таблице представлены максимально достижимые скорости передачи для каждого стандарта.

Табл. 1 Стандарты ADSL

СТАНДАРТ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ	ПЕРЕДАЧА ДАННЫХ	ПРИЕМ ДАННЫХ
ADSL	832 кбит/с	8 Мбит/с
ADSL2	3.5 Мбит/с	12 Мбит/с
ADSL2+	3.5 Мбит/с	24 Мбит/с

Стандарт, используемый вашим Интернет-провайдером, определяет максимальную скорость исходящего и входящего потока данных. Фактические скорости будут зависеть от расстояния до вашего Интернет-провайдера, качества линии и т. д.

1.2 Способы управления устройством P660RT2

Для управления устройством P660RT2 используются следующие средства:

- Программа ZyXEL NetFriend, поставляемая на диске. Рекомендуется для первоначальной настройки доступа в Интернет. Инструкция по его использованию содержится в кратком руководстве.
- Web-конфигуратор. Рекомендуется для повседневного управления устройством P660RT2 с использованием рекомендуемого Web-браузера. См. Глава 2 на с. 29.
- Интерфейс командной строки. Управление с помощью команд главным образом используется сервисными инженерами при поиске и устранении неисправностей. См. Глава 9 на с. 109.
- FTP. Протокол FTP (File Transfer Protocol – протокол передачи файлов) используется для обновления микропрограммы и резервного сохранения/восстановления конфигурации. См. Глава 9 на с. 109.
- SNMP. Мониторинг и управление устройством можно выполнять с помощью управляющей станции SNMP. См. Глава 9 на с. 109.

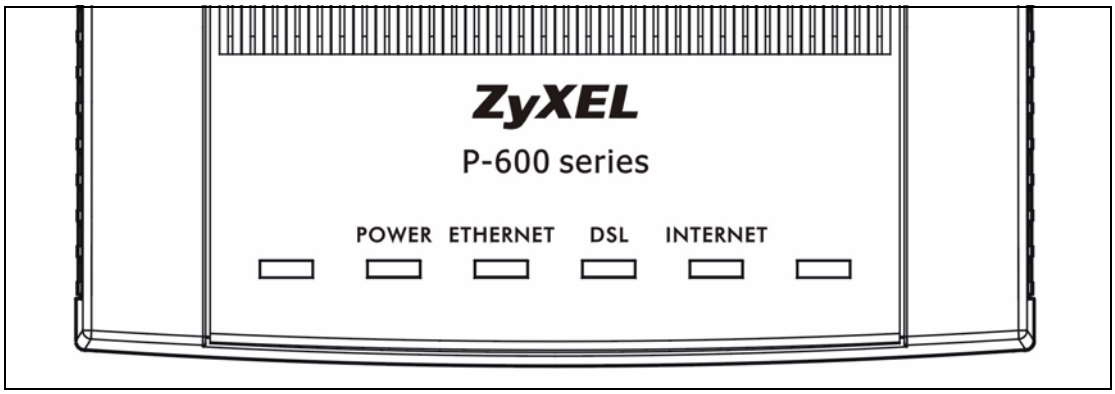
1.3 Полезные советы по управлению P660RT2

Для обеспечения безопасной и более эффективной работы P660RT2 рекомендуется регулярное и правильное выполнение описанных далее процедур.

1.4 P660RT2 — Установка и подключение оборудования

Рекомендации по установке и подключению оборудования см. в Кратком руководстве.

1.5 Светодиоды



В следующей таблице представлено описание светодиодов P660RT2.

Табл. 2 Описание светодиодов

СВЕТОДИОД	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
POWER (Питание)	Зеленый	Горит	Питание подается и P660RT2 работает нормально.
		Мигает	P660RT2 перезагружается.
	Красный	Горит	На P660RT2 подается недостаточное питание.
		Выключен	Устройство P660RT2 не готово или неисправно.
Ethernet (Локальная сеть)	Зеленый	Горит	Модем P660RT2 успешно установил соединение с Ethernet.
		Мигает	Модем P660RT2 успешно установил соединение с Ethernet и производит прием или передачу данных.
		Выключен	Соединение P660RT2 с Ethernet не установлено.
DSL	Зеленый	Горит	Модеммодем P660RT2 успешно установил связь с концентратором DSLAM.
		Мигает (медленно)	P660RT2 инициализирует линию DSL.
		Мигает (быстро)	Модем P660RT2 передает или принимает данные.
		Выключен	P660RT2 Отсутствует канал DSL.
INTERNET (Интернет)	Зеленый	Горит	Модем P660RT2 установил соединение по протоколу PPP (PPPoA или PPPoE).
		Мигает	Модем P660RT2 передает или принимает трафик PPPoA или PPPoE.
		Выключен	Соединение по протоколу PPP (PPPoA или PPPoE) не установлено.

2

Знакомство с Web-конфигуратором

В этой главе описаны способы получения доступа к Web-конфигуратору и методы работы с его интерфейсом.

2.1 Знакомство с Web-конфигуратором

Web-конфигуратор – это интерфейс управления на основе технологии HTML, который позволяет выполнять настройку и управление модемом P660RT2 с помощью браузера Интернет. Следует использовать Internet Explorer версии 6.0 и выше либо Netscape Navigator версии 7.0 и выше. Рекомендуемое разрешение экрана: 1024 на 768 пикселей.

Чтобы воспользоваться web-конфигуратором, необходимо активировать следующие опции:

- Инициированные модемом всплывающие окна в Интернет-браузере. Блокировка всплывающих окон активирована по умолчанию в Windows XP SP2.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (по умолчанию активированы).

Информацию о том, как проверить, действительно ли эти функции включены в браузере Internet Explorer, см. в главе «Поиск и устранение неисправностей».

2.2 Доступ к Web-конфигуратору

1. Убедитесь, что P660RT2 подключен правильно (см. Краткое руководство).
2. Подготовьте компьютер/компьютерную сеть для подключения к модему P660RT2 (см. Краткое руководство).
3. Запустите Web-браузер.
4. В адресной строке введите "192.168.1.1".
5. Появится следующий экран. Введите пароль администратора по умолчанию «1234» для выполнения настройки с помощью мастера установки, а также настройки расширенных функций устройства, или введите пароль пользователя по умолчанию «user» для просмотра статуса. Нажмите кнопку «Login» (Регистрация), чтобы перейти в окно изменения пароля или «Cancel» (Отмена), чтобы сохранить пароль по умолчанию.

Рис. 3 Окно ввода пароля

6 Если вы ввели пароль пользователя, пропустите следующие два действия и обратитесь к Разд. 2.3.2 на с. 34 за более подробной информацией об экране «Status» (Состояние).

Если вы ввели пароль администратора, настоятельно рекомендуется изменить пароль администратора по умолчанию! Введите новый пароль длиной от 1 до 30 символов, введите его еще раз для подтверждения и нажмите кнопку «Apply» (Применить); в противном случае нажмите кнопку «Ignore» (Пропустить) для перехода в главное меню, если в настоящее время вы не хотите менять пароль.

Если вы не изменили пароль, то каждый раз при регистрации с паролем администратора будет появляться следующее окно.

Рис. 4 Изменение пароля при входе

7 Выберите «Go to Wizard setup» (Мастер установки) и нажмите кнопку «Apply» (Применить) для отображения главного окна Мастера установки. В противном

случае, выберите «Go to Advanced setup» (Дополнительная настройка) и щелкните «Apply» (Применить) для отображения окна «Status» (Статус).

Рис. 5 Выбор режима

Сеанс управления будет автоматически завершен по истечении периода времени, установленного в поле «Administrator Inactivity Timer» (Время простоя в режиме администрирования),по умолчанию — 5 минут. В этом случае следует снова выполнить процедуру регистрации.

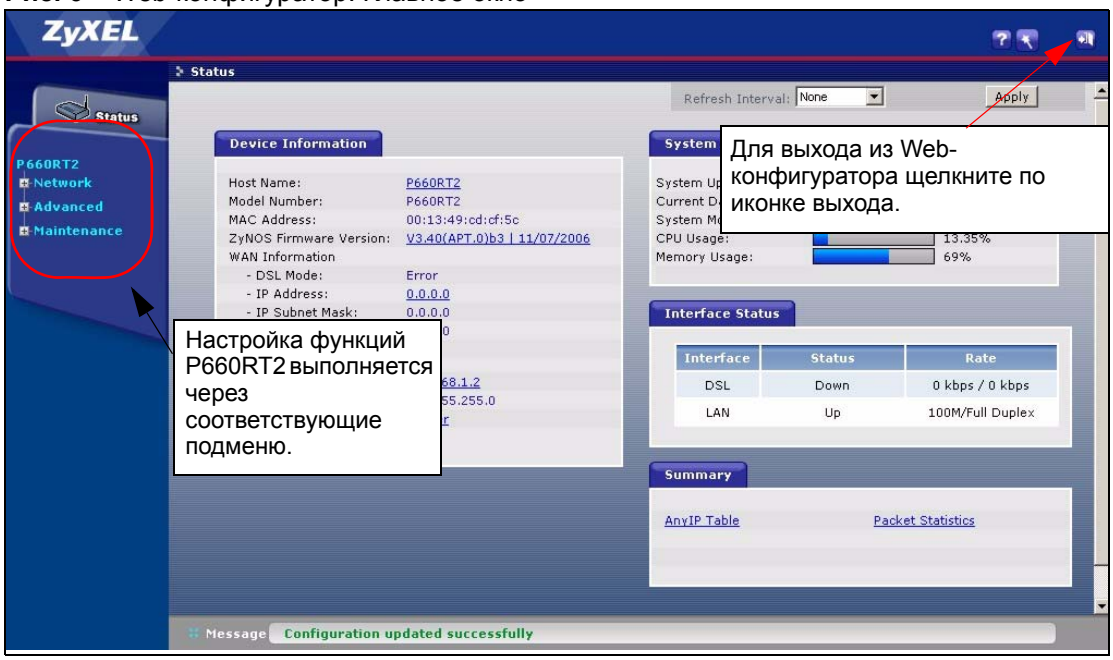
2.3 Интерфейс Web-конфигуратора

В качестве примера в данном руководстве используются окна, соответствующие модели P660. Вид окон может незначительно отличаться для различных моделей P660RT2.

2.3.1 Панель навигации

После ввода пароля администратора отображается главное меню. Для настройки функций P660RT2 используются соответствующие подменю в панели навигации. Описание подменю представлено в следующей таблице.

Рис. 6 Web-конфигуратор: Главное окно



Для просмотра встроенной справки щелкните по иконке (расположена в верхнем правом углу большинства окон).

Табл. 3 Сводная таблица окон Web-конфигуратора

ССЫЛКА/ ИКОНКА	ПОДМЕНЮ	ФУНКЦИЯ
Wizard (Мастер установки)	INTERNET SETUP (Настройка доступа в Интернет)	Эти окна используются для первоначальной настройки, включая настройку общих параметров, параметров Интернет-провайдера для доступа в Интернет и назначения IP-адреса в глобальной сети, сервера DNS, MAC-адреса.
Logout (Выход)		Для выхода из Web-конфигуратора щелкните по этой иконке.
Status (Состояние)		В этом окне отображается общая информация о состоянии устройства, системы и интерфейсов P660RT2. Это окно открывает доступ к таблицам, содержащим сводную статистику системы.
Network (Сеть)		

Табл. 3 Сводная таблица окон Web-конфигуратора (продолжение)

ССЫЛКА/ ИКОНКА	ПОДМЕНЮ	ФУНКЦИЯ
WAN (Глобальная сеть)	Internet Connection (Подключение к Интернету)	Это окно позволяет назначить IP-адрес устройства в глобальной сети, установить параметры Интернет-провайдера, определить серверы DNS и настроить другие свойства.
	More Connections (Другие соединения)	Это окно используется для просмотра и настройки других соединений для выполнения вызовов на другой удаленный шлюз.
	WAN Backup Setup (Настройка резервного доступа к WAN)	Используйте этот экран для конфигурирования свойств переадресации трафика и настроек резервного доступа к ГВС.
LAN (ЛВС)	IP	Это окно используется для настойки протокола TCP/IP в локальной сети, включения функции «Any IP» (Любой IP) и других свойств.
	DHCP Setup (Настройка DHCP)	Это окно используется для настройки протокола DHCP в локальной сети.
	Client List (Список клиентов)	Это окно используется для просмотра параметров конкретного клиента DHCP и назначения IP-адреса по MAC-адресу (и имени узла).
	IP Alias (Псевдоним IP)	Это окно позволяет разделить локальную сеть на подсети.
NAT	General (Общие)	Это окно используется для включения функции NAT.
	Port Forwarding (Переадресация портов)	Это окно используется для настройки маршрутизации связанных с приложением служб на соответствующие компьютеры локальной сети.
	Address Mapping (Отображение адресов)	Это окно используется для настройки серверов, находящихся за P660RT2.
Advanced (Дополнительные настройки)		
Static Route (Статический маршрут)		Здесь выполняется настройка статических маршрутов IP.
Dynamic DNS (Динамическая DNS)		Это окно используется для настройки динамической службы DNS.

Табл. 3 Сводная таблица окон Web-конфигуратора (продолжение)

ССЫЛКА/ ИКОНКА	ПОДМЕНЮ	ФУНКЦИЯ
Remote MGMT (Удаленное управление)	WWW	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление P660RT2 по протоколу HTTPS или HTTP.
	Telnet	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление P660RT2 по протоколу Telnet.
	FTP	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается доступ к P660RT2 по протоколу FTP.
	SNMP	В этом окне производятся настройки для управления P660RT2 по протоколу SMNP (простой протокол управления сетью).
	DNS	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователи могут посылать запросы DNS к P660RT2.
	ICMP	Это окно используется для изменения настроек блокирования эхо-тестирования.
UPnP		Это окно используется для включения в P660RT2 функции UPnP (универсальная функция Plug and Play).
Maintenance (Сопровождение)		
System (Система)	General (Общие)	Это окно служит для отображения административной и общесистемной информации, а также позволяет изменить пароль.
	Time Setting (Установка времени)	Это окно используется для изменения даты и времени в P660RT2.
Tools (Инструменты)	Firmware (Встроенное программное обеспечение)	Это окно используется для загрузки микропрограммы в P660RT2.
	Configuration (Конфигурация)	Это окно позволяет выполнить резервное сохранение и восстанавление конфигурации или сброс настроек P660RT2 к заводским установкам.
	Restart (Перезапуск)	Это окно позволяет выполнить перезагрузку P660RT2 без выключения электропитания.
Diagnostic (Диагностика)	General (Общие)	Информация, отображаемая в этих окнах, помогает определить неисправности, связанные с подключением P660RT2.
	DSL Line (Линия DSL)	В этих окнах отображается информация, помогающая идентифицировать проблемы, связанные с линией DSL.

2.3.2 Окно «Status» (Состояние)

В этом разделе рассказывается, как работать с Web-конфигуратором из окна «Status» (Состояние). Если в окне ввода пароля вы зарегистрировались с правами пользователя, некоторые поля и ссылки будут недоступны (см. Рис. 3 на с. 30). В некоторых моделях устройства не все поля являются доступными.

Рис. 7 Окно «Status» (Состояние)

В следующей таблице представлено описание элементов окна «Status» (Состояние).

Табл. 4 Окно «Status» (Состояние)

ПОЛЕ	ОПИСАНИЕ
Refresh Interval (Интервал обновления)	Из выпадающего списка выберите количество секунд для автоматического обновления статистики в окнах по истечении заданного временного интервала или значение «None» (Нет), чтобы статистика не обновлялась.
Apply (Применить)	Щелкните по этой кнопке для обновления статистики в окне состояния и сохранения значения в поле «Refresh Interval» (Интервал обновления).
Device Information (Информация об устройстве)	
Host Name (Имя узла)	Здесь отображается «System Name» (Системное имя), которое вводится в окне «Maintenance» (Сопровождение) > «System» (Система) > «General» (Общие настройки). Оно служит для идентификации устройства.
Model Number (Номер модели)	Здесь отображается наименование модели P660RT2.
MAC Address (MAC-адрес)	Это уникальный MAC-адрес (Media Access Control – управление доступом к среде) или адрес Ethernet P660RT2.
ZyNOS Firmware Version (Версия встроенного программного обеспечения ZyNOS)	Здесь отображается версия и дата создания микропрограммы ZyNOS. ZyNOS – это сетевая операционная система, собственная разработка ZyXEL.
WAN Information (Параметры глобальной сети)	
DSL Mode (Режим DSL)	Это стандарт, по которому работает P660RT2.
IP Address (IP-адрес)	Это IP-адрес порта DSL.
IP Subnet Mask (Маска IP подсети)	Здесь отображается маска IP подсети для порта DSL.

Табл. 4 Окно «Status» (Состояние)

ПОЛЕ	ОПИСАНИЕ
Default Gateway (Шлюз по умолчанию)	Здесь отображается IP-адрес шлюза по умолчанию, если он применяется.
VPI/VCI	Это идентификатор виртуального пути и идентификатор виртуального канала, настраиваемые с помощью Мастера установки или в окне «WAN» (Глобальная сеть).
LAN Information (Параметры локальной сети)	
IP Address (IP-адрес)	Здесь отображается IP-адрес порта ETHERNET.
IP Subnet Mask (Маска IP подсети)	Здесь отображается маска IP подсети для порта ETHERNET.
DHCP	Здесь отображается DHCP роль порта ETHERNET – «Server» (Сервер), «Relay» (Ретранслятор) или «None» (Отключить).
System Status (Статус системы)	
System Uptime (Время работы системы)	Здесь отображается время, истекшее с момента запуска P660RT2.
Current Date/ Time (Текущая дата/время)	В этом поле отображается текущая дата и время P660RT2 .
System Mode (Режим системы)	В этом поле отображается режим работы P660RT2: маршрутизатор или мост.
CPU Usage (Загрузка центрального процессора)	Здесь отображается использование динамической памяти P660RT2 в килобайтах. Операционная система ZyNOS (ZyXEL Network Operating System) не использует динамическую память, т. о., она может использоваться для работы таких функций как NAT, VPN и межсетевой экран. Индикатор показывает процент использования динамической памяти P660RT2. Индикатор меняет свой цвет с зеленого на красный, когда память полностью занята.
Memory Usage (Использование памяти)	Здесь отображается использование всей памяти P660RT2 в килобайтах. Индикатор показывает процент использования динамической памяти P660RT2. Индикатор меняет свой цвет с зеленого на красный, когда память используется полностью.
Interface Status (Статус портов)	
Interface (Порт)	В этом поле отображаются типы портов P660RT2.
Status (Состояние)	В этом поле отображается «Down» (Нет) (соединение отсутствует), «Up» (Работает) (соединение установлено и активно), если установлена инкапсуляция Ethernet, или «Down» (Нет) (соединение отсутствует), «Up» (Работает) (соединение установлено и активно), «Idle» (Ожидание) (соединение (ppp) в режиме ожидания), «Dial» (Вызов) (запуск процедуры вызова) и «Drop» (Сброс) (сброс соединения), если установлена инкапсуляция PPPoE.
Rate (Скорость передачи)	Для портов LAN здесь отображается скорость порта и режим передачи. Для порта DSL здесь отображается скорость приема и передачи данных.
Summary (Общая информация)	

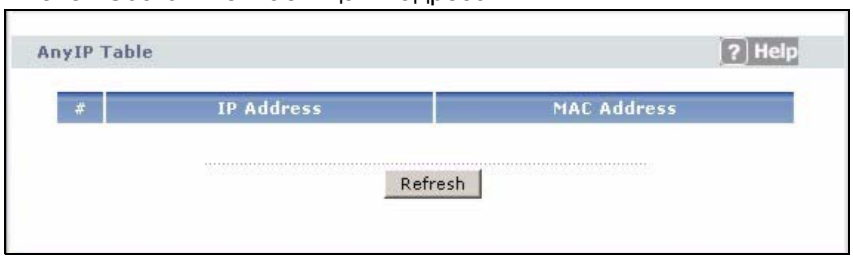
Табл. 4 Окно «Status» (Состояние)

ПОЛЕ	ОПИСАНИЕ
Any IP Table (Таблица IP-адресов)	В этом окне отображается список IP-адресов и MAC-адресов компьютеров, которые находятся в подсети, отличной от подсети P660RT2.
Packet Statistics (Статистика пакетов)	В этом окне отображается статус портов и статистика пакетов.

2.3.3 Состояние: Таблица IP-адресов

Щелкните по гиперссылке «Any IP Table» (Таблица IP-адресов) в окне «Status» (Состояние). В таблице IP-адресов отображаются текущие данные в режиме только для чтения (в том числе IP-адрес и MAC-адрес) для всех сетевых устройств, которые используют функцию «Any IP» (Любой IP) для подключения к P660RT2.

Рис. 8 Состояние: Таблица IP-адресов



В следующей таблице даны описания полей этого окна.

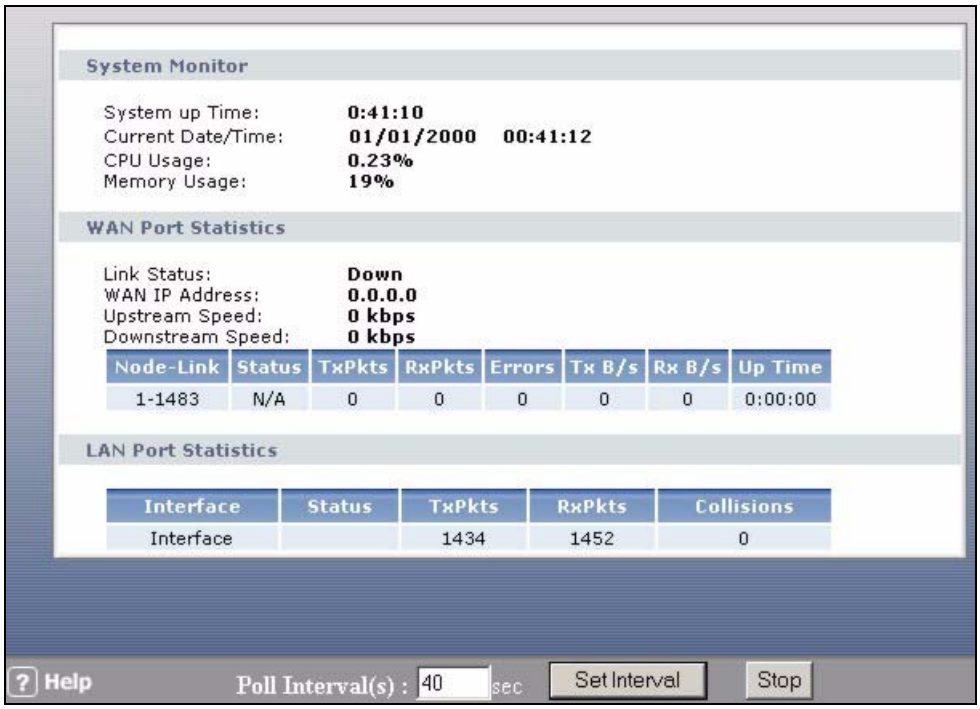
Табл. 5 Состояние: Таблица IP-адресов

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер узла.
IP Address (IP-адрес)	В этом поле отображается IP-адрес сетевого устройства.
MAC Address (MAC-адрес)	В этом поле отображается MAC-адрес (Media Access Control — Управление доступом к среде) компьютера с данным IP-адресом. Каждое устройство Ethernet имеет уникальный MAC-адрес. MAC-адрес присваивается изготовителем и состоит из шести пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02.
Refresh (обновить)	Щелкните «Refresh» (Обновить) для обновления информации в этом окне.

2.3.4 Состояние: Статистика пакетов

Щелкните по гиперссылке «Packet Statistics» (Статистика пакетов) в окне «Status» (Состояние). Здесь отображается информация о состоянии портов и статистика пакетов в режиме только для чтения. Также здесь отображается время работы системы и интервалы опроса системы. В поле «Poll Interval(s)» (Интервал(ы) опроса) можно изменять значение. В некоторых моделях устройства не все поля являются доступными.

Рис. 9 Состояние: Статистика пакетов



В следующей таблице даны описания полей этого окна.

Табл. 6 Состояние: Статистика пакетов

ПОЛЕ	ОПИСАНИЕ
System Monitor (Системный мониторинг)	
System up Time (Время работы системы)	Здесь отображается время, истекшее с момента запуска системы.
Current Date/Time (Текущая дата/ время)	В этом поле отображается текущая дата и время P660RT2 .
CPU Usage (Загрузка центрального процессора)	В этом поле отображается процент использования ресурсов CPU.
Memory Usage (Использование памяти)	В этом поле отображается использование памяти в процентах.
LAN or WAN Port Statistics (Статистика порта LAN или WAN)	Здесь отображается статистика порта глобальной или локальной сети.
Link Status (Состояние канала связи)	Здесь отображается статус подключения к глобальной сети.
Upstream Speed (Скорость исходящего трафика)	В этом поле отображается скорость исходящего трафика P660RT2

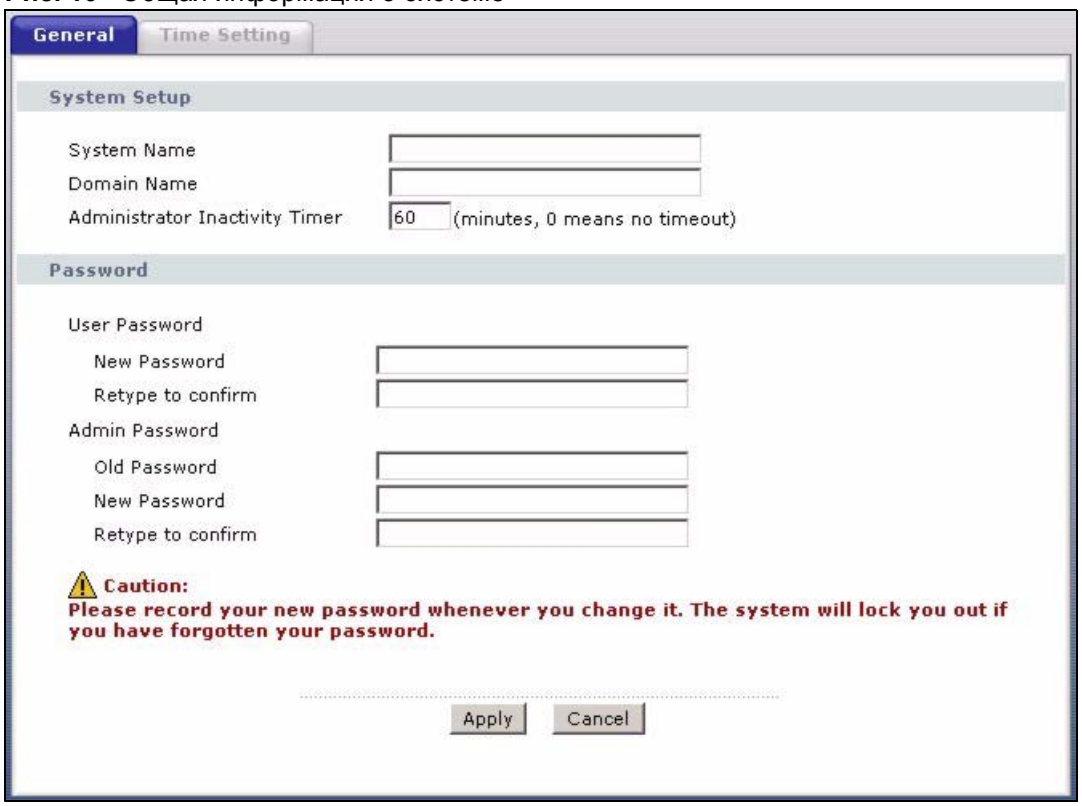
Табл. 6 Состояние: Статистика пакетов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Downstream Speed (Скорость входящего трафика)	В этом поле отображается скорость входящего трафика P660RT2
Node-Link (Номер — вид соединения)	В этом поле отображается порядковый номер удаленного узла и вид соединения. Виды соединения: PPPoA, ENET, RFC 1483 и PPPoE.
Interface (Порт)	В данном поле отображается тип порта.
Status (Состояние)	В этом поле отображается «Down» (Нет) (соединение отсутствует), «Up» (Работает) (соединение установлено и активно), если установлена инкапсуляция Ethernet, или «Down» (Нет) (соединение отсутствует), «Up» (Работает) (соединение установлено и активно), «Idle» (Ожидание) (соединение (ppp) в режиме ожидания), «Dial» (Вызов) (запуск процедуры вызова) и «Drop» (Сброс) (сброс соединения), если установлена инкапсуляция PPPoE.
TxPkts (Передано пакетов)	В этом поле отображается количество пакетов, переданных через этот порт.
RxPkts (Принято пакетов)	В этом поле отображается количество пакетов, принятых через этот порт.
Errors (Ошибки)	В этом поле отображается количество пакетов с ошибками, принятых через этот порт.
Tx B/s (Передача, байт/с)	В этом поле отображается количество байтов, переданных в последнюю секунду.
Rx B/s (Прием, байт/с)	В этом поле отображается количество байтов, принятых в последнюю секунду.
Up Time (Время соединения)	В этом поле отображается время, истекшее с момента установления соединения через этот порт.
Collisions (Конфликты)	Здесь отображается количество конфликтов при передаче через данный порт.
Help (Справка)	Нажмите эту кнопку для вывода окна справки.
Poll Interval(s) / Интервал(ы) опроса	Введите интервал времени, через который браузер будет обновлять информацию о системе.
Set Interval (Задать интервал)	Нажмите эту кнопку, чтобы применить новый интервал опроса, заданный в поле «Poll Interval» (Интервал опроса).
Stop (Остановить)	Нажмите эту кнопку, чтобы прекратить обновление информации о системе.

2.3.5 Изменение пароля

Настоятельно рекомендуется периодически менять пароль доступа к P660RT2. Если после регистрации вы не изменили пароль по умолчанию или хотите еще раз изменить пароль, щелкните «Maintenance» (Сопровождение) > «System» (Система) для отображения следующего окна. Подробное описание полей окна см. в Табл. 41 на с. 136.

Рис. 10 Общая информация о системе



Мастер настройки доступа в Интернет

В этой главе описываются окна Web-конфигуратора «Wizard Setup» (Мастер настройки), используемые для настройки доступа в Интернет.

3.1 Введение

Окна Мастера используются для настройки системы для доступа в Интернет с помощью ввода параметров, предоставленных Интернет-провайдером.

Более подробная информация об этих полях приведена в главах, посвященных отдельным меню.

3.2 Мастер настройки доступа в Интернет

1 После ввода пароля администратора и получения доступа к Web-конфигуратору, выберите «Go to Wizard setup» (Запуск мастера установки) и щелкните «Apply» (Применить). Также для отображения главного окна Мастера установки можно щелкнуть по иконке Мастера установки ( ) в верхнем правом углу Web-конфигуратора.

Рис. 11 Выбор режима

2 Щелкните «INTERNET SETUP» (Настройка доступа в Интернет), чтобы настроить доступ в Интернет.

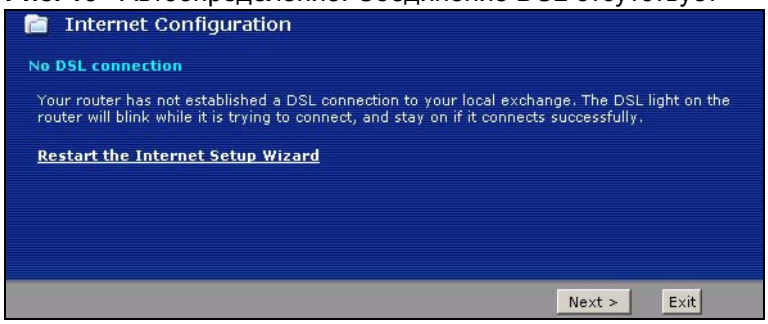
Рис. 12 Мастер установки: Приветствие

3 Мастер попытается определить, какой тип подключения к глобальной сети используется.

Если Мастер определяет тип соединения, и ваш Интернет-провайдер использует протокол PPPoE или PPPoA, перейдите к Разд. 3.2.1 на с. 43. Вид окна меняется в зависимости от типа соединения.

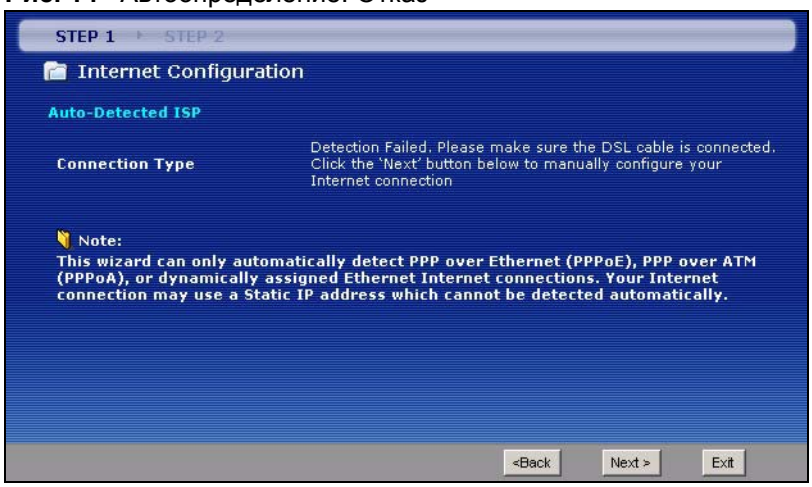
Если Мастер не может определить тип соединения, и появляется следующее окно (см. Рис. 13 на с. 43), проверьте правильность подключения оборудования и нажмите «Restart the Internet Setup Wizard» (Повторный запуск Мастера настройки доступа в Интернет), чтобы P660RT2 попытался еще раз определить тип соединения.

Рис. 13 Автоопределение: Соединение DSL отсутствует



Если Мастер установки снова не может определить тип соединения, и появляется следующее окно (см. Рис. 14 на с. 43), нажмите кнопку «Next» (Далее) и обратитесь к Разд. 3.2.2 на с. 44, где даются сведения о настройке подключения P660RT2 к Интернету вручную.

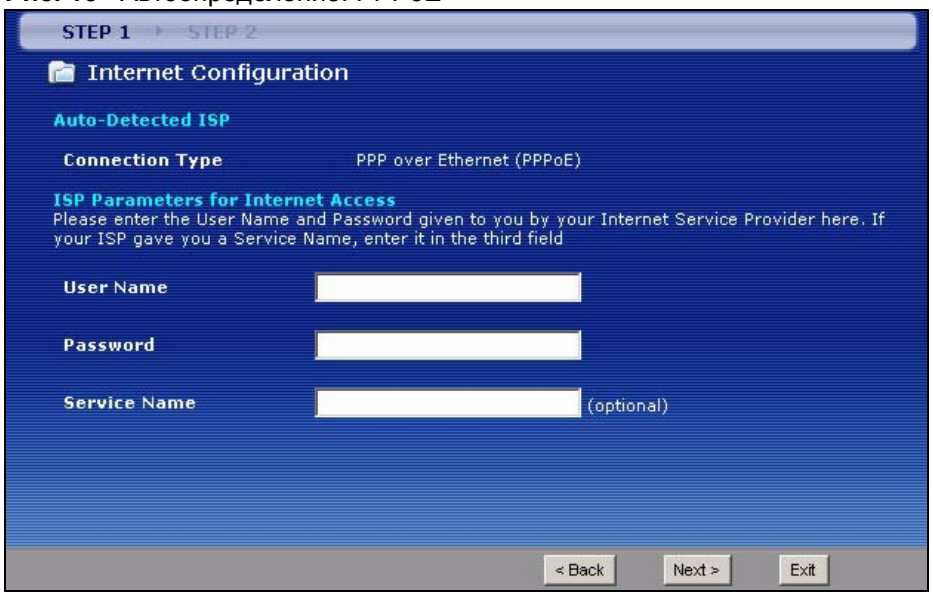
Рис. 14 Автоопределение: Отказ



3.2.1 Автоматическое определение

1. При подключении PPPoE или PPPoA появится окно с запросом на ввод данных учетной записи Интернет. Введите имя пользователя, пароль и/или имя услуги в соответствии с предоставленной провайдером информацией.
2. Щелкните «Next» (Далее) для подтверждения настроек и тестирования соединения.

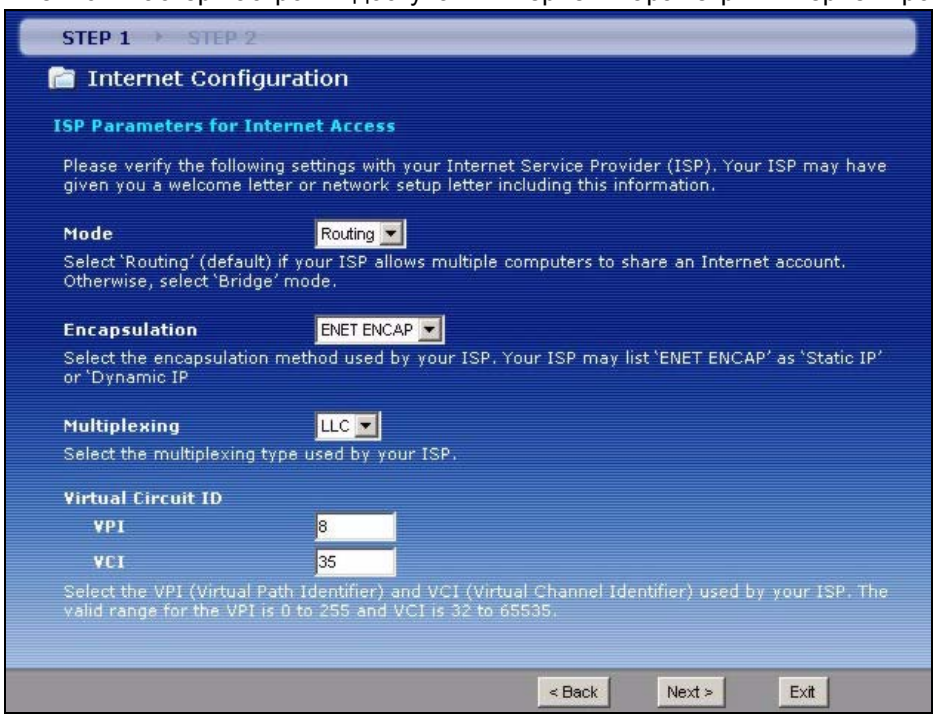
Рис. 15 Автоопределение: PPPoE



3.2.2 Ручная настройка

1 Если P660RT2 не удалось определить тип соединения DSL, введите в окне Мастера информацию для доступа в Интернет, предоставленную вашим Интернет-провайдером. Если информация отсутствует, оставьте значения полей по умолчанию.

Рис. 16 Мастер настройки доступа в Интернет: Параметры Интернет-провайдера



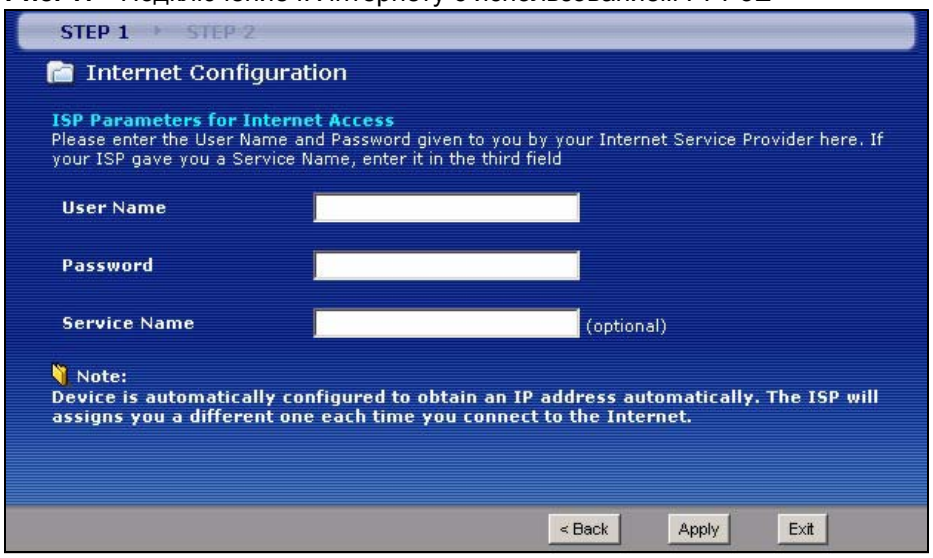
В следующей таблице даны описания полей этого окна.

Табл. 7 Мастер настройки доступа в Интернет: Параметры Интернет-провайдера

ПОЛЕ	ОПИСАНИЕ
Mode (Режим)	Если ваш провайдер разрешает множественный доступ компьютеров по одной учетной записи Интернет, выберите из выпадающего списка поля «Mode» (Режим) параметр «Routing» (Маршрутизация) (этот режим установлен по умолчанию). В другом случае выберите режим «Bridge» (Мост).
Encapsulation (Инкапсуляция)	Выберите тип инкапсуляции, который использует ваш Интернет-провайдер, из выпадающего списка поля «Encapsulation» (Инкапсуляция). Варианты в списке изменяются в зависимости от того, какой режим установлен в поле «Mode» (Режим). Если в поле «Mode» (Режим) установлено «Bridge» (Мост), выберите «PPPoA» или «RFC 1483». Если в поле «Mode» (Режим) установлено «Routing» (Маршрутизация), выберите «PPPoA», «RFC 1483», «ENET ENCAP» или «PPPoE».
Multiplexing (Мультиплексирование)	Из выпадающего списка поля «Multiplex» (Мультиплексирование) выберите используемый Интернет-провайдером метод мультиплексирования: на базе VC или LLC.
Virtual Circuit ID (Идентификатор виртуального канала)	VPI (Идентификатор виртуального пути) и VCI (Идентификатор виртуального канала) определяют виртуальный канал. Более подробную информацию см. в приложении.
VPI (Идентификатор виртуального пути)	Введите назначенный идентификатор виртуального пути. Это поле может быть уже заполнено.
VCI (Идентификатор виртуального канала)	Введите назначенный идентификатор виртуального канала. Это поле может быть уже заполнено.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку «Back» (Назад).
Next (Далее)	Для перехода к следующему окну Мастера нажмите кнопку «Next» (Далее). Вид следующего окна Мастера настройки зависит от того, какой протокол был выбран до этого.
Exit (Выход)	Щелкните по кнопке «Exit» (Выход), чтобы закрыть окно Мастера без сохранения изменений.

2 Вид следующего окна Мастера установки зависит от выбранного режима и используемого типа инкапсуляции. Во всех представленных экранных окнах используется режим маршрутизации. Заполните поля и щелкните «Next» (Далее) для продолжения.

Рис. 17 Подключение к Интернету с использованием PPPoE

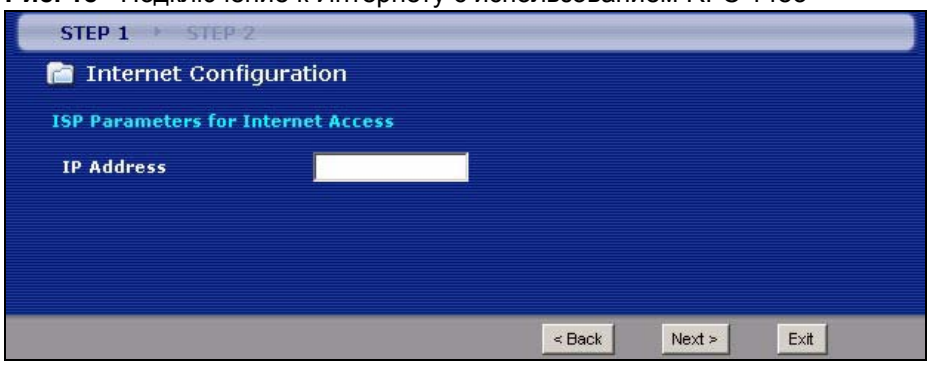


В следующей таблице даны описания полей этого окна.

Табл. 8 Подключение к Интернету с использованием PPPoE

ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите имя пользователя, предоставленное Интернет-провайдером. Если имя назначается в формате user@domain, где domain означает имя услуги, то введите оба элемента имени в полном соответствии с данными от провайдера.
Password (Пароль)	Введите пароль для данного имени пользователя.
Service Name (Название услуги)	Введите имя провайдера услуг PPPoE.
Back (Назад)	Нажмите кнопку «Back» (Назад) для возвращения к предыдущему окну Мастера.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Exit (Выход)	Щелкните по кнопке «Exit» (Выход), чтобы закрыть окно Мастера без сохранения изменений.

Рис. 18 Подключение к Интернету с использованием RFC 1483

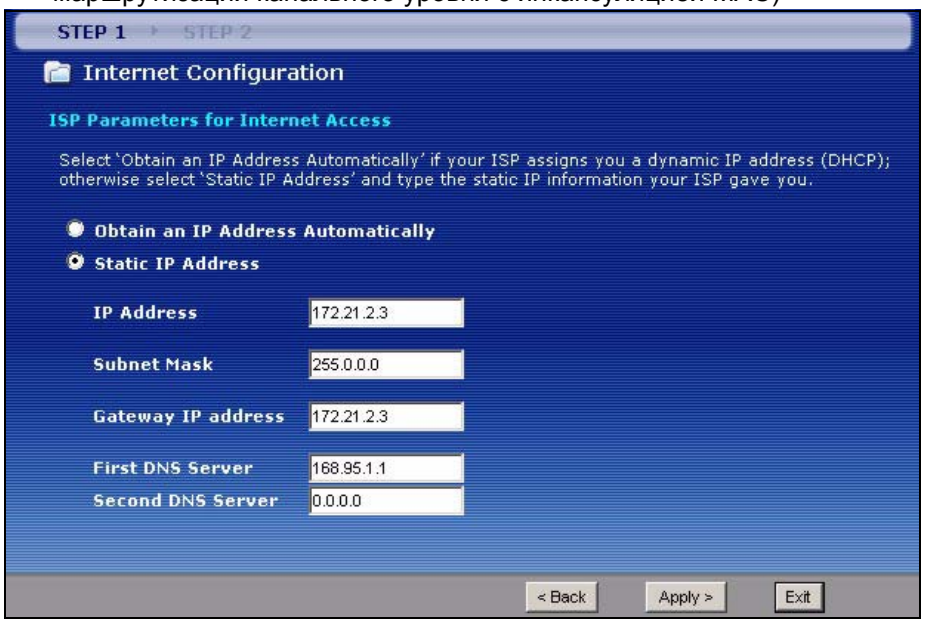


В следующей таблице даны описания полей этого окна.

Табл. 9 Подключение к Интернету с использованием RFC 1483

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Это поле доступно, если в поле «Mode» (Режим) выбран режим «Routing» (Маршрутизация). Введите в это поле IP-адрес, предоставленный Интернет-провайдером.
Back (Назад)	Щелкните «Back» (Назад) для возвращения к предыдущему окну Мастера установки.
Next (Далее)	Для перехода к следующему окну Мастера нажмите кнопку «Next» (Далее).
Exit (Выход)	Щелкните по кнопке «Exit» (Выход), чтобы закрыть окно Мастера без сохранения изменений.

Рис. 19 Подключение к Интернету с использованием ENET ENCAP (Протокол маршрутизации канального уровня с инкапсуляцией MAC)



В следующей таблице даны описания полей этого окна.

Табл. 10 Подключение к Интернету с использованием ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
Obtain an IP Address Automatically (Получать IP-адрес автоматически)	Статический IP-адрес — это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является фиксированным; Интернет-провайдер назначает вам новый адрес каждый раз, когда вы подключаетесь к Интернету. Если у вас динамический IP-адрес, выберите «Obtain an IP Address Automatically» (Получать IP-адрес автоматически).
Static IP Address (Статический IP-адрес)	Если Интернет-провайдер назначил вам фиксированный IP-адрес, выберите «Static IP Address» (Статический IP-адрес).
IP Address (IP-адрес)	Введите IP-адрес, назначенный вашим Интернет-провайдером.

Табл. 10 Подключение к Интернету с использованием ENET ENCAP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Subnet Mask (Маска подсети)	Введите маску подсети в десятичном виде с разделительными точками. Информацию о расчете маски подсети при создании подсетей см. в приложениях.
Gateway IP Address (IP-адрес шлюза)	Необходимо указать IP-адрес шлюза (предоставленный вашим Интернет-провайдером), если в предыдущем окне в поле «Encapsulation» (Инкапсуляция) установлен тип инкапсуляции «ENET ENCAP».
First DNS Server (Первый сервер DNS)	Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Second DNS Server (Второй сервер DNS)	Аналогично предыдущей записи.
Back (Назад)	Щелкните «Back» (Назад) для возвращения к предыдущему окну Мастера установки.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Exit (Выход)	Щелкните по кнопке «Exit» (Выход), чтобы закрыть окно Мастера без сохранения изменений.

Рис. 20 Подключение к Интернету с использованием PPPoA

В следующей таблице даны описания полей этого окна.

Табл. 11 Подключение к Интернету с использованием PPPoA

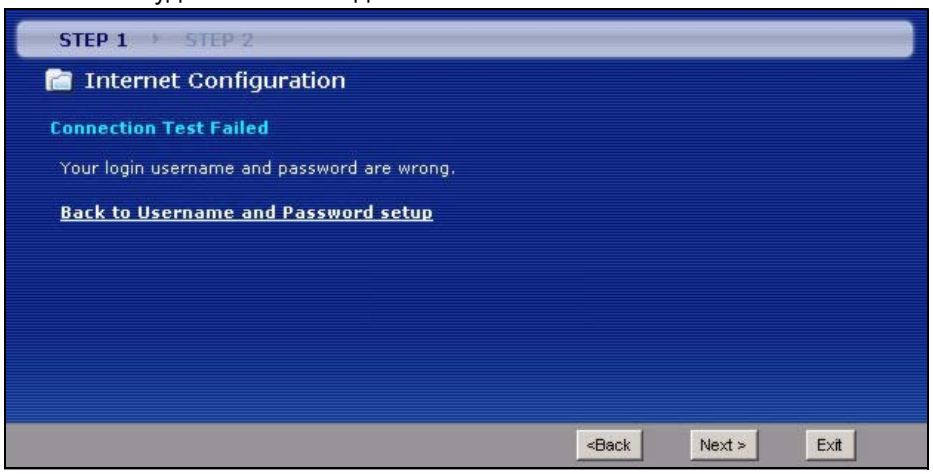
ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите регистрационное имя, предоставленное Интернет-провайдером.
Password (Пароль)	Введите пароль для данного имени пользователя.
Back (Назад)	Щелкните «Back» (Назад) для возвращения к предыдущему окну Мастера установки.

Табл. 11 Подключение к Интернету с использованием PPPoA (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Exit (Выход)	Щелкните по кнопке «Exit» (Выход), чтобы закрыть окно Мастера без сохранения изменений.

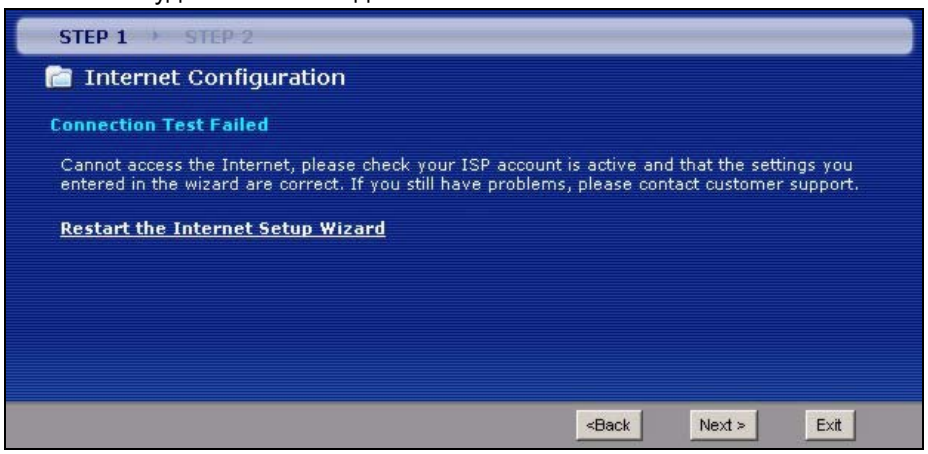
- Если вы неправильно ввели имя пользователя и/или пароль для соединения PPPoE или PPPoA, появится окно, показанное ниже. Щелкните «Back to Username and Password setup» (Назад к установке имени пользователя и пароля), чтобы вернуться назад к окну, где можно внести изменения.

Рис. 21 Неудачный тест подключения 1



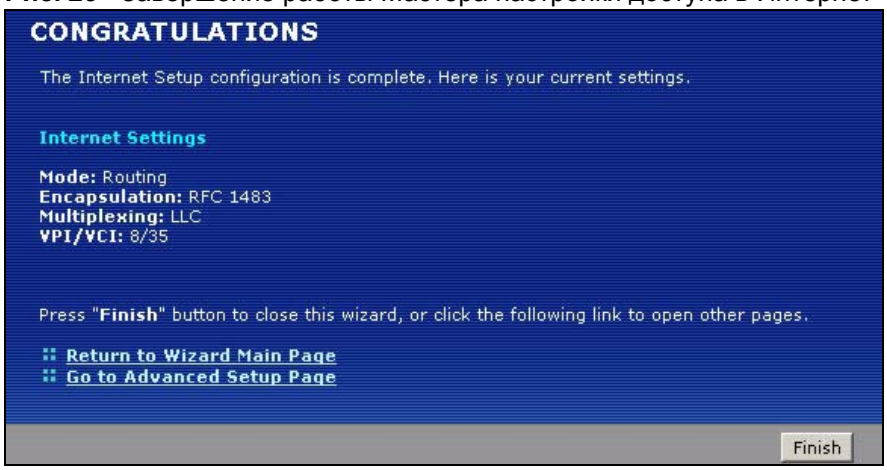
- Если появляется следующее окно, проверьте, активирована ли ваша учетная запись или нажмите «Restart the Internet/Wireless Setup Wizard» (Повторный запуск Мастера установки Интернета / беспроводной сети), чтобы проверить параметры доступа в Интернет.

Рис. 22 Неудачный тест подключения 2



После завершения работы Мастера установки появится следующее окно, содержащее информацию о конфигурации. Щелкните «Finish» (Готово), чтобы закрыть Мастер установки.

Рис. 23 Завершение работы Мастера настройки доступа в Интернет



Часть II
Web-конфигуратор

Настройка глобальной сети(53)
Настройка локальной сети(73)
Окна NAT (Трансляция сетевых адресов)(87)
Статический маршрут(101)
Настройка динамической системы доменных имен (DYNDNS)(105)
Настройка удаленного управления(109)
Универсальная функция Plug and Play (UPnP)(121)

4

Настройка глобальной сети

В этой главе описывается настройка глобальной сети.

4.1 Общая информация о глобальной сети

WAN (Wide Area Network – Глобальная вычислительная сеть) формируется при наличии подключения к другой сети или к сети Интернет.

4.1.1 Инкапсуляция

Убедитесь, что используется метод инкапсуляции, предписываемый Интернет-провайдером. Ниже перечислены методы инкапсуляции, поддерживаемые P660RT2.

4.1.1.1 Инкапсуляция ENET ENCAP

ENET ENCAP (MAC Encapsulated Routing Link Protocol – Протокол маршрутизации канального уровня с инкапсуляцией MAC) может быть реализован только с сетевым протоколом IP. IP-пакеты маршрутизируются между портом Ethernet и портом WAN, а затем форматируются таким образом, чтобы межсетевые устройства могли их распознавать. Например, протокол инкапсулирует маршрутизируемые кадры Ethernet в передаваемые ячейки ATM. Для ENET ENCAP необходимо указать IP-адрес шлюза в поле «ENET ENCAP Gateway» (Шлюз ENET ENCAP) во втором окне Мастера установки. Эту информацию можно получить у Интернет-провайдера.

4.1.1.2 Протокол "точка-точка" поверх Ethernet (PPPoE)

PPPoE (Point-to-Point Protocol over Ethernet – протокол "точка-точка" поверх Ethernet) обеспечивает контроль доступа и учет соединений аналогично услугам коммутируемых линий связи, использующим PPP. PPPoE – это стандарт IETF (RFC 2516), определяющий, каким образом персональный компьютер (PC) взаимодействует с широкополосным модемным соединением (DSL, кабель, беспроводной канал и т. д.).

Для провайдера услуг протокол PPPoE обеспечивает метод доступа и аутентификации, который работает с существующими системами управления доступом (например, RADIUS).

Одним из преимуществ PPPoE является возможность доступа пользователей к нескольким сетевым службам, т. е. функция, называемая динамическим выбором служб. Это позволяет провайдеру услуг легко создавать и предоставлять конкретным пользователям новые услуги IP.

С точки зрения функциональности PPPoE значительно экономит усилия пользователей и Интернет-провайдеров или операторов связи, так как не требует специальной настройки широкополосного модема на стороне пользователя.

Так как PPPoE реализован непосредственно в P660RT2 (а не на отдельных компьютерах), установка программного обеспечения PPPoE на компьютерах локальной сети не требуется, поскольку эта процедура полностью выполняется модемом P660RT2. Кроме того, при включении функции NAT доступ будут иметь все компьютеры локальной сети.

4.1.1.3 Протокол "точка-точка" поверх ATM (PPPoA)

PPPoA означает Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) (Протокол "точка-точка" поверх адаптации ATM, уровень 5). Соединение PPPoA работает аналогично коммутируемому соединению Интернет. P660RT2 инкапсулирует сеанс связи PPP на базе RFC1483 и передает его через постоянный виртуальный канал ATM (Permanent Virtual Circuit) на концентратор DSLAM (цифровой мультиплексор доступа) Интернет-провайдера. Для получения дополнительной информации по PPPoA см. комментарий RFC 2364. Более подробно о PPP см. в RFC1661.

4.1.1.4 RFC 1483

RFC 1483 описывает два способа многопротокольной инкапсуляции на уровне 5 адаптации ATM (AAL5). Первый метод позволяет передачу с мультиплексированием нескольких протоколов по одному виртуальному каналу ATM (мультиплексирование на базе LLC), а второй метод предполагает передачу каждого протокола по отдельному виртуальному каналу ATM (мультиплексирование на базе VC). Для получения более подробной информации см. комментарии RFC.

4.1.2 Мультиплексирование

Определить, какие протоколы используются для передачи по виртуальному каналу (VC), можно двумя способами. Убедитесь, что вы используете метод мультиплексирования, который поддерживает ваш Интернет-провайдер.

4.1.2.1 Мультиплексирование на базе VC

По предварительному взаимному соглашению, за каждым протоколом закрепляется конкретный виртуальный канал, напр., VC1 передает IP, VC2 передает IPX и т.д. Мультиплексирование на базе VC может быть основным методом в средах, где динамическое создание большого количества виртуальных каналов ATM происходит быстро и экономично.

4.1.2.2 Мультиплексирование на базе LLC

В этом случае один виртуальный канал передает несколько протоколов, снабженных идентифицирующей информацией, которая содержится в заголовке каждого пакета. Несмотря на использование дополнительной пропускной способности и обработку служебной информации, этот метод может оказаться предпочтительным там, где иметь отдельный виртуальный канал для каждого передаваемого протокола нерационально, например, если оплата во многом зависит от количества одновременно задействованных виртуальных каналов.

4.1.3 Сценарии инкапсуляции и мультиплексирования

Для обеспечения доступа в Интернет должны использоваться методы инкапсуляции и мультиплексирования, предписанные Интернет-провайдером. Проконсультируйтесь с вашей телефонной компанией относительно методов инкапсуляции и мультиплексирования для соединения между локальными сетями, например, между филиалом и головным офисом. Необходимо иметь предварительное соглашение по использованию методов инкапсуляции и мультиплексирования, так как они не могут быть определены автоматически. Выбор методов инкапсуляции и мультиплексирования также зависит от количества имеющихся виртуальных каналов и количества необходимых сетевых протоколов. Инкапсуляция ENET ENCAP требует передачи дополнительной служебной информации, что делает этот метод нерациональным для соединения локальных сетей. Далее приводится несколько примеров комбинирования методов, наиболее подходящих для такого применения.

4.1.3.1 Сценарий 1: Один виртуальный канал, множество протоколов

Инкапсуляция **PPPoA** (RFC-2364) с мультиплексированием **на базе VC** является наиболее оптимальным сочетанием, так как отсутствует необходимость в дополнительных заголовках для идентификации протокола. Протокол **PPP** уже содержит эту информацию.

4.1.3.2 Сценарий 2: Один виртуальный канал, один протокол (IP)

Инкапсуляция **RFC-1483** с мультиплексированием **на базе VC** требует минимального количества служебной информации (0 байт). Однако если в дальнейшем возникнет необходимость в поддержке нескольких протоколов, то разумно выбрать инкапсуляцию **PPPoA**, а не **RFC-1483**, так как в этом случае не придется заново настраивать компьютеры.

4.1.3.3 Сценарий 3: Несколько виртуальных каналов

Если количество имеющихся виртуальных каналов совпадает (или превышает) с количеством протоколов, следует выбрать инкапсуляцию **RFC-1483** и мультиплексирование **на базе VC**.

4.1.4 VPI и VCI

Убедитесь, что вы используете верные номера VPI (Virtual Path Identifier – Идентификатор виртуального пути) и VCI (Virtual Channel Identifier – Идентификатор виртуального канала), которые вам назначены. Допустимый диапазон для VPI - от 0 до 255, а для VCI - от 32 до 65535 (0 - 31 зарезервированы для локального управления трафиком ATM). Более подробную информацию см. в приложении.

4.1.5 Назначение IP-адреса

Статический IP представляет собой фиксированный IP, предоставленный Интернет-провайдером. Динамический IP-адрес не фиксирован. Интернет-провайдер каждый раз назначает новый IP-адрес. Функция учетной записи одиночного пользователя (SUA) может быть включена или отключена, как для динамического, так и для статического IP-адреса. Тем не менее, на выбор IP-адреса и шлюза ENET ENCAP влияет назначенный способ инкапсуляции.

4.1.5.1 Назначение IP при инкапсуляции PPPoA или PPPoE

Если используется динамический IP-адрес, то поля «IP Address» (IP-адрес) и «ENET ENCAP Gateway» (Шлюз ENET ENCAP) являются недоступными (N/A). Если используется статический IP, необходимо заполнить *только* поле «IP Address» (IP-адрес), и *не заполнять* поле «ENET ENCAP Gateway» (Шлюз ENET ENCAP).

4.1.5.2 Назначение IP с инкапсуляцией RFC 1483

В этом случае *следует* назначать статический IP-адрес при тех же требованиях к заполнению полей «IP Address» (IP-адрес) и «ENET ENCAP Gateway» (Шлюз ENET ENCAP), как указано выше.

4.1.5.3 Назначение IP с инкапсуляцией ENET ENCAP

В этом случае может назначаться как статический, так и динамический IP. Для статического IP-адреса необходимо заполнить оба поля «IP Address» (IP-адрес) и «ENET ENCAP Gateway» (Шлюз ENET ENCAP) в соответствии с параметрами, предоставленными вашим Интернет-провайдером. Однако при назначении динамического IP-адреса P660RT2 функционирует как клиент DHCP через WAN-порт и, следовательно, поля «IP Address» (IP-адрес) и «ENET ENCAP Gateway» (Шлюз ENET ENCAP) являются недоступными (N/A), так как эти параметры для P660RT2 назначает сервер DHCP.

4.1.6 Полупостоянное соединение (PPP)

Полупостоянное соединение - это коммутируемая линия, по которой соединение всегда установлено, независимо от трафика. При выборе полупостоянного соединения модем P660RT2 выполняет следующее: во-первых, отключается время простоя; во-вторых, P660RT2 пытается восстановить соединение при включении питания, а также при разрыве соединения. Полупостоянное соединение является дорогостоящим по очевидным причинам.

Стоит устанавливать полупостоянное соединение только в случае, если ваша телефонная компания предоставляет услуги связи без ограничения времени, или если требуется постоянная связь и ее стоимость не имеет значения.

4.1.7 NAT

NAT (Network Address Translation — Трансляция сетевых адресов, RFC 1631) является преобразованием IP-адреса узла в пакете, например, адреса источника исходящего пакета, используемого внутри одной сети в другой IP-адрес, известный в другой сети.

4.2 Метрика

Метрика представляет собой «стоимость передачи данных». Маршрутизатор определяет наилучший маршрут для передачи, выбирая путь с самой низкой «стоимостью». При маршрутизации RIP для измерения стоимости используется счетчик переходов по сети, с минимальным значением, равным "1" для стоимости прямого соединения между сетями. Число должно находиться в интервале от 1 до 15; число больше 15 означает разрыв соединения. Чем меньше число, тем меньше "стоимость".

Метрика устанавливает приоритет для маршрутов трафика P660RT2 в Интернете. Если два маршрута по умолчанию имеют одинаковую метрику, P660RT2 использует следующие заданные приоритеты:

- Стандартный маршрут: назначается Интернет-провайдером (см. в Разд. 4.4 на с. 59)
- Маршрут перенаправления трафика (см. Разд. 4.6 на с. 69)
- Резервный маршрут WAN, называемый также резервное коммутируемое подключение (см. Разд. 4.7 на с. 70)

Например, если стандартный маршрут имеет метрику "1", маршрут перенаправления трафика имеет метрику "2", а резервный маршрут имеет метрику "3", то стандартный маршрут используется как основной маршрут по умолчанию. Если по стандартному маршруту не удается подключиться к Интернету, P660RT2 пытается использовать маршрут перенаправления трафика. Аналогично, P660RT2 использует резервный маршрут, если маршрут переадресации трафика тоже не работает.

Если вы хотите, чтобы резервный маршрут имел приоритет над маршрутом перенаправления трафика или даже над стандартным маршрутом, то необходимо для резервного маршрута установить метрику "1", а другим маршрутам - "2" (или выше).

Политика маршрутизации IP замещает схему маршрутизации по умолчанию и имеет приоритет над всеми маршрутами, описанными выше.

4.3 Формирование трафика

Функция формирования трафика представляет собой соглашение между владельцем сети и абонентом, предназначенное для регулировки средней скорости и колебаний скорости передачи данных через сеть ATM. Такое соглашение помогает устранить перегрузку сети, что важно для передачи данных в реальном времени, таких как аудио- и видеоданные.

PCR (Peak Cell Rate – Пиковая скорость ячеек) – это максимальная скорость, с которой отправитель может передавать ячейки. Данный параметр может быть ниже (но не выше), чем максимальная скорость передачи в линии. Размер одной ячейки ATM составляет 53 байта (424 бита), таким образом при максимальной скорости передачи данных в 832 кбит/с максимальная скорость передачи ячеек PCR будет 1962 ячеек/с. Однако эта скорость не гарантирована, потому что она зависит от скорости передачи линии.

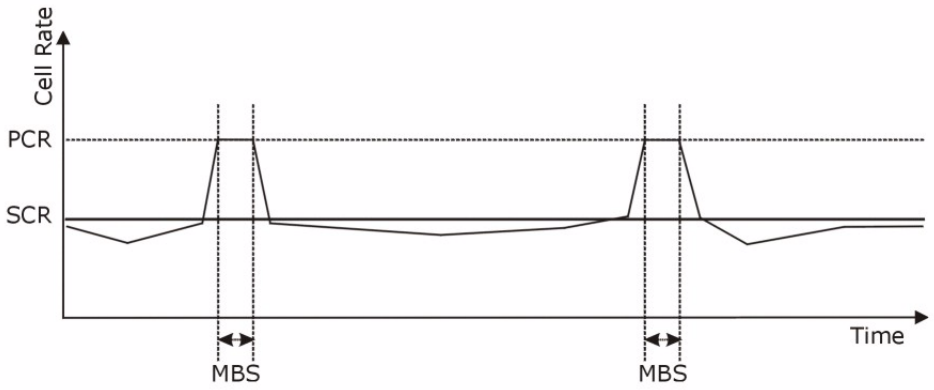
SCR (Sustained Cell Rate – Поддерживаемая скорость передачи ячеек) представляет собой среднюю скорость передачи ячеек от каждого источника пульсирующего трафика. Она определяет максимальную среднюю скорость, с которой ячейки могут передаваться по виртуальному соединению. Значение SCR не может быть больше, чем PCR.

MBS (Maximum Burst Size – Максимальный размер пакета) – это максимальное количество ячеек, которые можно передать со скоростью PCR. При достижении MBS скорость ячеек падает ниже значения SCR и держится на этом уровне до тех пор, пока средняя скорость ячеек не вернется к значению SCR. В течение этого времени также можно будет передавать большее количество ячеек (до MBS) на скорости PCR.

Если значение PCR, SCR или MBS по умолчанию установлено на "0", то система будет назначать максимальное значение в соответствии со скоростью передачи линии.

На следующем рисунке показано соотношение между PCR, SCR и MBS.

Рис. 24 Пример формирования трафика



4.3.1 Классы трафика ATM

Существуют основные классы трафика ATM, определяемые в «Спецификации управления трафиком 4.0» в составе Форума ATM.

4.3.1.1 Постоянная скорость передачи (CBR)

Тип трафика CBR (постоянная скорость передачи) обеспечивает фиксированную пропускную способность, которая всегда доступна, даже если не производится передача данных. Как правило, трафик CBR является чувствительным ко времени (задержка не допускается). CBR используется в соединениях, где постоянно требуется определенная величина пропускной способности. Скорость PCR является заданной, и если скорость трафика превышает эту скорость, ячейки могут отбрасываться. Примерами соединений CBR являются передача речи и видеосигнала с высоким разрешением.

4.3.1.2 Переменная скорость передачи (VBR)

Тип трафика VBR ATM (Variable Bit Rate – Переменная скорость передачи) используется в соединениях с пульсирующим трафиком. Соединения, где используется трафик VBR, могут группироваться в соединения реального времени VBR-RT (real time VBR) или соединения вне реального времени VBR-nRT (non-real time VBR).

Тип трафика VBR-RT (real-time Variable Bit Rate – Переменная скорость передачи в реальном времени) используется для передачи пульсирующего трафика, который требует тщательного контроля задержки и изменений задержки. Здесь также обеспечивается фиксированная пропускная способность (скорость PCR является заданной), но она доступна, только когда производится передача данных. Примером соединения VBR-RT является проведение видеоконференций. Для организации видеоконференций требуется передача данных в реальном времени и предоставление полосы пропускания, меняющейся в зависимости от динамики изменения видеоизображений.

Тип трафика VBR-nRT (non real-time Variable Bit Rate – Переменная скорость передачи вне реального времени) используется для передачи пульсирующего трафика, который не требует тщательного контроля задержки и изменений задержки. Такой тип трафика используется для пульсирующего трафика, типичного для локальных сетей. Скорость PCR и максимальный размер пакета MBS определяют размеры блоков пакетов, SCR определяет минимальный размер блока. Примером соединения VBR-nRT является передача файлов данных, которая не чувствительна к задержкам.

4.3.1.3 Неопределенная скорость передачи (UBR)

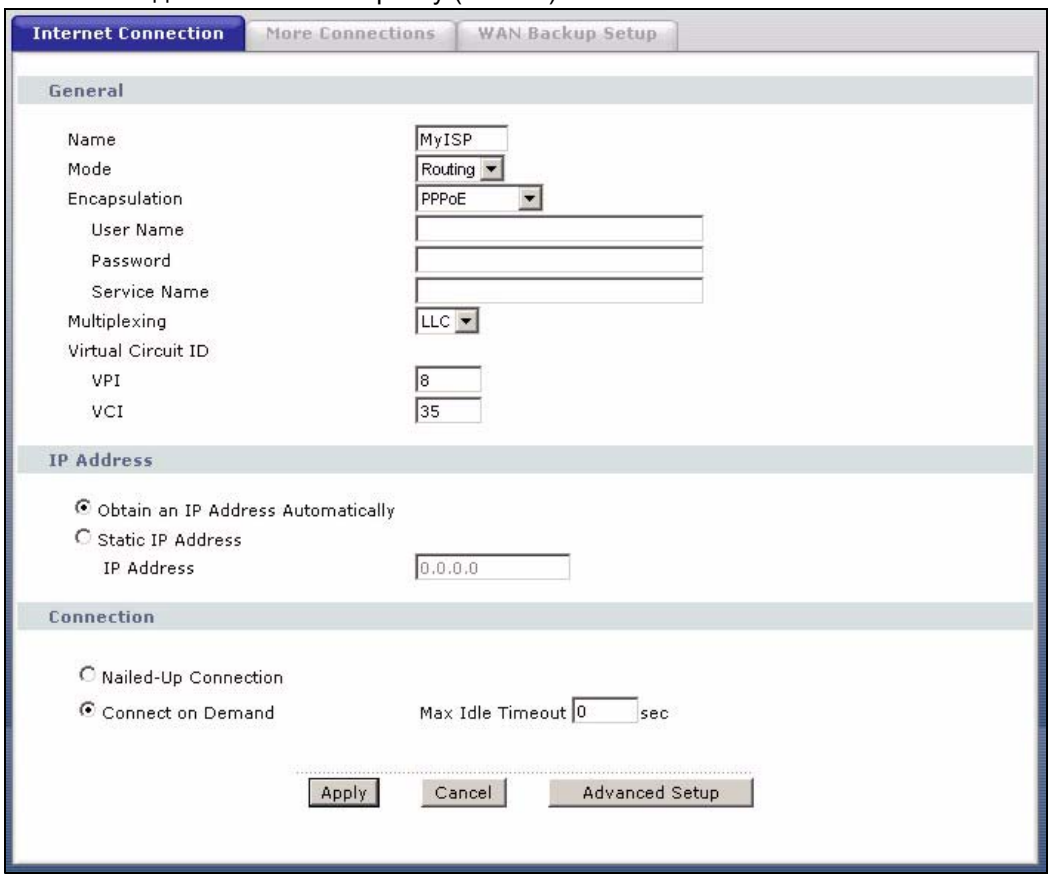
Тип трафика UBR ATM (Unspecified Bit Rate – Неопределенная скорость передачи) используется для пакетной передачи данных. Но при использовании UBR не гарантируется величина пропускной способности, и трафик передается, только когда сеть имеет ресурсы. Примером применения UBR является фоновая передача файлов.

4.4 Подключение к Интернету

Для изменения параметров доступа в Интернет порта WAN модема P660RT2 щелкните «Network» (Сеть) > «WAN». Окно «Internet Connection» (Подключение к Интернет) может иметь различный вид в зависимости от выбранной инкапсуляции.

Более подробную информацию см. в Разд. 4.1 на с. 53.

Рис. 25 Подключение к Интернету (PPPoE)



В следующей таблице даны описания полей этого окна.

Табл. 12 Подключение к Интернету

ПОЛЕ	ОПИСАНИЕ
Line (линия)	
Modulation (Модуляция)	Выберите модуляцию, используемую вашим провайдером или установите “multimode” для автоматического определения.
Annex (Аннекс)	В подавляющем большинстве случаев в России используется Annex A, т.е. ADSL поверх стандартной телефонной линии. Annex B обычно используется либо на линии ISDN либо на линии с установленной охранно-пожарной сигнализацией. В любом случае эта настройка должна соответствовать типу оборудования, установленного у вашего провайдера.
General (Общие)	
Name (Имя)	Введите имя Интернет-провайдера, например MyISP. Эта информация используется только в целях идентификации.
Mode (Режим)	Из раскрывающегося списка поля «Mode» (Режим) выберите «Routing» (Маршрутизация) (установлено по умолчанию), если ваш Интернет-провайдер позволяет нескольким компьютерам использовать одну учетную запись для подключения к Интернету. В другом случае выберите Bridge (Мост).
Encapsulation (Инкапсуляция)	Из выпадающего списка выберите метод инкапсуляции, используемый Интернет-провайдером. Варианты в списке зависят от режима, установленного в поле «Mode» (Режим). Если в поле «Mode» (Режим) установлено «Bridge» (Мост), выберите «PPPoA» или «RFC 1483». Если в поле «Mode» (Режим) установлено «Routing» (Маршрутизация), выберите «PPPoA», «RFC 1483», «ENET ENCAP» или «PPPoE».
User Name (Имя пользователя)	Введите имя пользователя, назначенное вашим Интернет-провайдером (только для инкапсуляции PPPoA и PPPoE). Если имя назначается в формате user@domain, где domain означает имя услуги, то введите оба элемента имени в полном соответствии с данными от провайдера.
Password (Пароль)	Введите пароль для данного имени пользователя (только для инкапсуляции PPPoA и PPPoE).
Service Name (Название услуги)	Введите имя услуги PPPoE (только для PPPoE).
Multiplexing (Мультиплексирование)	Из выпадающего списка выберите метод мультиплексирования, используемый Интернет-провайдером. Вариантами являются «VC» или «LLC».
Virtual Circuit ID (Идентификатор виртуального канала)	VPI (Virtual Path Identifier — Идентификатор виртуального пути) и VCI (Virtual Channel Identifier — Идентификатор виртуального канала) определяют виртуальный канал. Более подробную информацию см. в приложении.
VPI (Идентификатор виртуального пути)	Допустимый диапазон для VPI — от 0 до 255. Введите назначенный номер VPI.
VCI (Идентификатор виртуального канала)	Допустимый диапазон для VCI — от 32 до 65535 (номера 0 - 31 зарезервированы для локального управления трафиком ATM). Введите назначенный номер VCI.

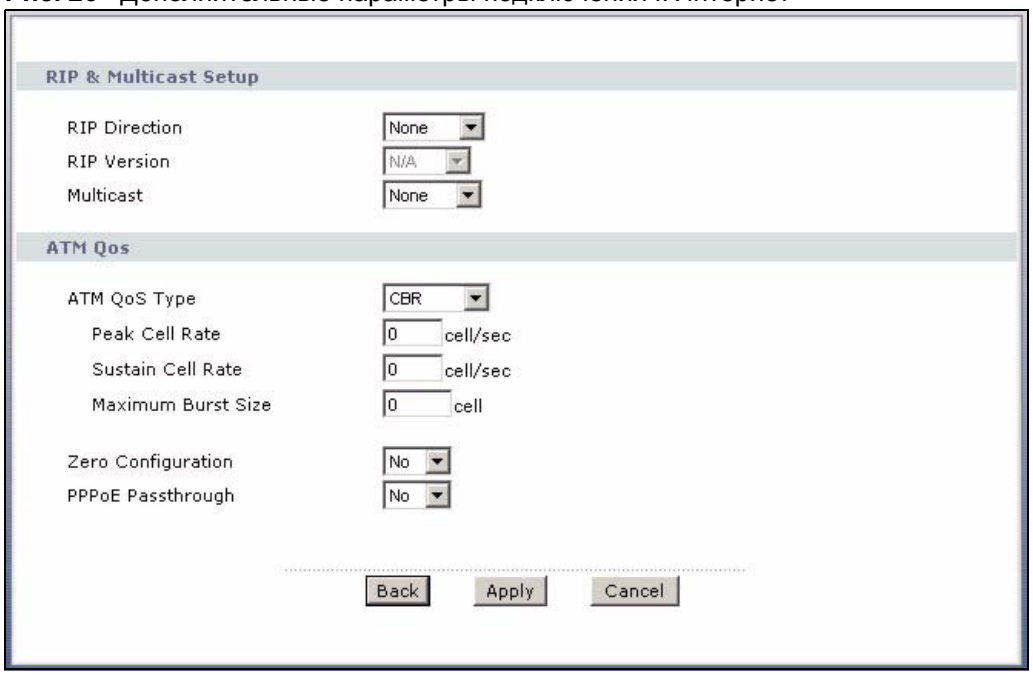
Табл. 12 Подключение к Интернету (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Это поле доступно, если в поле «Mode» (Режим) выбран режим «Routing» (Маршрутизация). Статический IP-адрес — это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является фиксированным; Интернет-провайдер назначает вам новый адрес каждый раз, когда вы подключаетесь к Интернету. Если установлен тип инкапсуляции, отличный от RFC 1483, выберите «Obtain an IP Address Automatically» (Получать IP-адрес автоматически) при использовании динамического IP-адреса; в противном случае выберите «Static IP Address» (Статический IP-адрес) и введите назначенный Интернет-провайдером IP-адрес в поле «IP Address» (IP-адрес), которое находится ниже. Если используется RFC 1483, введите IP-адрес, предоставленный вашим Интернет-провайдером, в поле «IP Address» (IP-адрес).
Subnet Mask (Маска подсети) (Только для инкапсуляции ENET ENCAP)	Введите маску подсети в десятичном виде с разделительными точками. Информацию о расчете маски подсети при создании подсетей см. в приложениях.
Gateway IP Address (IP-адрес шлюза) (Только для инкапсуляции ENET ENCAP)	Необходимо указать IP-адрес шлюза (предоставленный вашим Интернет-провайдером), если в поле «Encapsulation» (Инкапсуляция) установлен тип инкапсуляции ENET ENCAP.
Connection (Подключение) (Только для инкапсуляции PPPoA и PPPoE)	
Nailed-Up Connection (Полупостоянное соединение)	Выберите «Nailed-Up Connection» (Полупостоянное соединение), если требуется постоянное соединение. При разрыве соединения P660RT2 автоматически будет пытаться восстановить его.
Connect on Demand (Подключение по требованию)	Выберите «Connect on Demand» (Подключение по требованию), если постоянное соединение не требуется, и введите в поле «Max. Idle Timeout» (Максимальное время простоя) время простоя (в секундах).
Max Idle Timeout (Максимальное время простоя)	Если выбрано «Connect on Demand» (Подключение по требованию), введите интервал простоя в поле «Max Idle Timeout» (Максимальное время простоя). По умолчанию установлено 0, что означает, что соединение с Интернетом не будет разрываться.
Apply (Применить)	Нажмите кнопку «Apply» (Применить), чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.
Advanced Setup (Дополнительные параметры)	Щелкните по этой кнопке для отображения окна «Advanced Internet Connection Setup» (Дополнительные параметры подключения к Интернет) и установите дополнительные настройки WAN.

4.4.1 Дополнительные параметры подключения к Интернет

Это окно позволяет изменять дополнительные параметры WAN для устройства P660RT2. Щелкните по кнопке «Advanced Setup» (Дополнительные параметры) в окне «Internet Connection» (Подключение к Интернету). Появится следующее окно.

Рис. 26 Дополнительные параметры подключения к Интернет



В следующей таблице даны описания полей этого окна.

Табл. 13 Дополнительные параметры подключения к Интернет

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup (Настройка RIP и многоадресной рассылки)	
RIP Direction (Направление RIP)	RIP (Routing Information Protocol – Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Это поле определяет какую информацию о маршрутизации P660RT2 передает и принимает в данной подсети. Выберите направление RIP из раскрывающегося списка со значениями «None» (Отключить), «Both» (Оба), «In Only» (Только входящие) и «Out Only» (Только исходящие).
RIP Version (Версия RIP)	Выберите версию RIP. Вариантами являются: «RIP-1», «RIP-2B» и «RIP-2M».
Multicast (Многоадресная рассылка)	Выберите версию IGMP, которую P660RT2 будет использовать для выполнения многоадресной рассылки в локальной сети. Пакеты многоадресной рассылки передаются группе компьютеров локальной сети, пакеты одноадресной рассылки передаются конкретному компьютеру, а пакеты широковещательной рассылки передаются всем компьютерам локальной сети. P660RT2 поддерживает обе версии IGMP: IGMP-v1 и IGMP-v2. Выберите «None» (Нет) для отключения IGMP.

Табл. 13 Дополнительные параметры подключения к Интернет (продолжение)

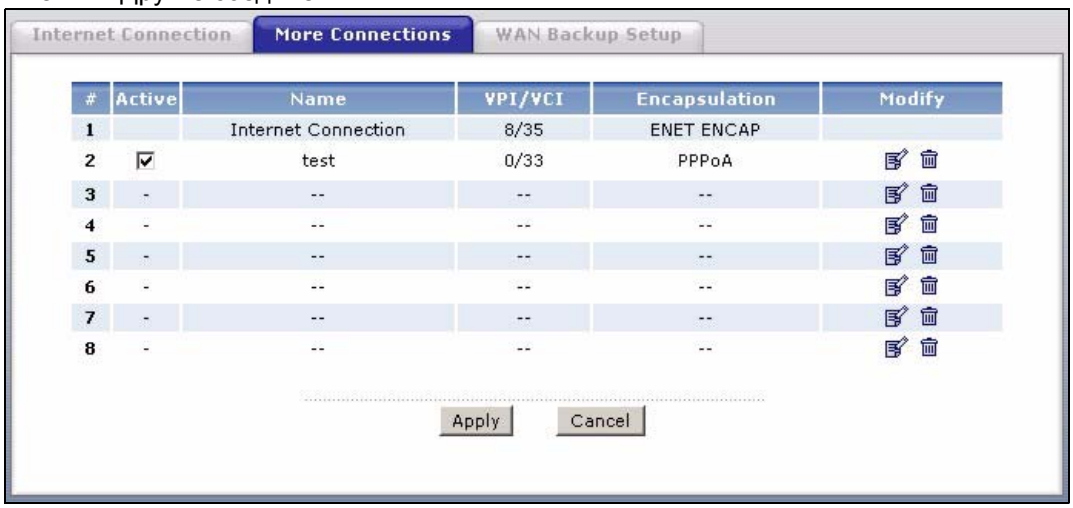
ПОЛЕ	ОПИСАНИЕ
ATM QoS (Качество услуг ATM).	
ATM QoS Type (Тип QoS ATM)	Выберите «CBR» (Continuous Bit Rate - Постоянная скорость передачи), чтобы определить фиксированную (всегда доступную) пропускную способность для голосового трафика или передачи данных. Выберите «UBR» (Неопределенная скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите «VBR-nRT» (Переменная скорость передачи вне реального времени) или «VBR-RT» (Переменная скорость передачи в реальном времени) для передачи пульсирующего трафика и разделения пропускной способности с другими приложениями.
Peak Cell Rate (Пиковая скорость ячеек)	Чтобы определить PCR (Peak Cell Rate – Пиковая скорость ячеек), разделите скорость DSL линии (бит/с) на 424 (размер ячейки ATM). Это и будет максимальная скорость, с которой отправитель может передавать ячейки. Введите в это поле значение PCR.
Sustain Cell Rate (Поддерживаемая скорость ячеек)	Параметр SCR (Sustain Cell Rate – Поддерживаемая скорость ячеек) устанавливает среднюю скорость ячеек (долговременную), с которой они могут передаваться. Введите значение SCR, оно должно быть меньше, чем PCR. Следует отметить, что по умолчанию установлено 0 ячеек/с.
Maximum Burst Size (Максимальный размер пакета)	MBS (Maximum Burst Size – Максимальный размер пакета) – это максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите значение MBS (должно быть меньше 65535).
Zero Configuration (Автоматическая настройка)	Эта функция не применяется / не доступна, если при настройке P660RT2 используется статический IP-адрес глобальной сети или режим моста. Выберите «Yes» (Да), чтобы P660RT2 автоматически определял настройки подключения к Интернету (такие как номера VCI/VPI и метод инкапсуляции), используемые Интернет-провайдером и выполнял необходимые изменения в своих настройках. Выберите «No» (Нет) для отключения этой функции. В этом случае для получения доступа в Интернет придется установить настройки P660RT2 вручную.
PPPoE Passthrough (Транзит PPPoE) (только для инкапсуляциия PPPoE)	Это поле доступно, если выбрана инкапсуляция **PPPoE**. В дополнение к встроенному в P660RT2 клиенту PPPoE, можно включить пересылку PPPoE, позволяющую 10 узлам локальной сети с установленным клиентским программным обеспечением PPPoE подключаться к Интернет-провайдеру через P660RT2. Каждый узел может иметь отдельную учетную запись и общедоступный IP-адрес в глобальной сети. Транзит PPPoE-соединений является альтернативой NAT для сфер применения, где использование NAT нецелесообразно. Отключите функцию транзита PPPoE-соединений, если не требуется, чтобы узлы локальной сети использовали программное обеспечение клиента PPPoE для подключения к Интернет-провайдеру.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку «Back» (Назад).
Apply (Применить)	Нажмите кнопку «Apply» (Применить), чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

4.5 Настройка других соединений

В этом разделе описываются не зависящие от протокола параметры для удаленной сети. Они требуются для выполнения вызовов на удаленный шлюз и расположенную за ним сеть через соединение WAN. При настройке доступа в Интернет в окне «WAN» (Глобальная сеть) > «Internet Connection» (Подключение к Интернету) устанавливается основное подключение к глобальной сети.

Щелкните «Network» (Сеть) > «WAN» (Глобальная сеть) > «More Connections» (Другие соединения) для отображения окна, показанного ниже.

Рис. 27 Другие соединения



В следующей таблице даны описания полей этого окна.

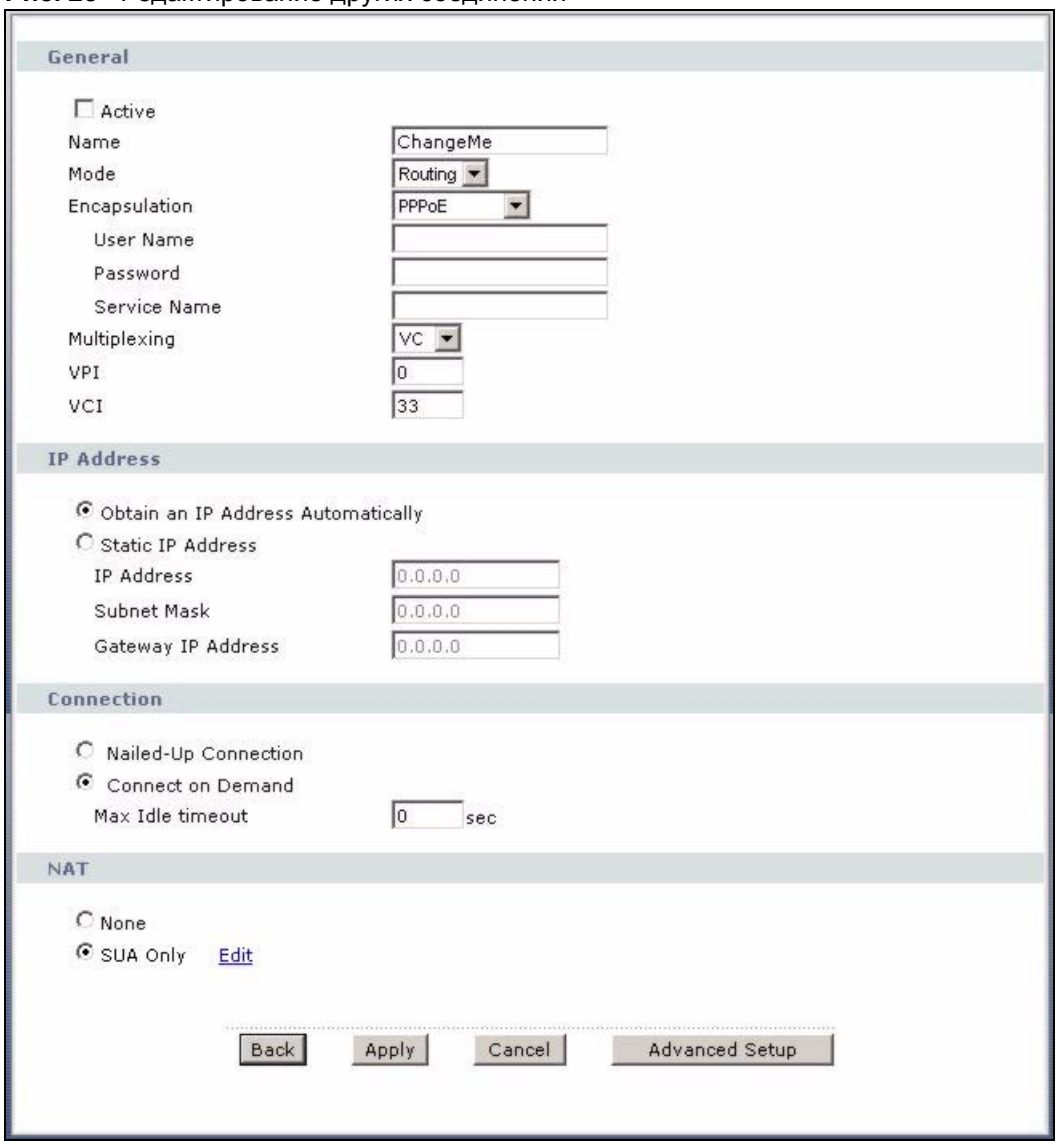
Табл. 14 Другие соединения

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер соединения.
Active (Включить)	В этом поле отображается состояние соединения. Чтобы отключить соединение, снимите флажок. Для включения соединения поставьте флажок.
Name (Имя)	В этом поле отображается описательное имя соединения.
VPI/VCI	В этом поле отображаются значения VPI и VCI для данного соединения.
Encapsulation (Инкапсуляция)	В этом поле отображается метод инкапсуляции для данного соединения.
Modify (Изменить)	В этом окне отображается основное соединение (с Интернет-провайдером) в режиме только для чтения. Изменение его параметров производится в окне «WAN» (Глобальная сеть) > «Internet Connections» (Подключение к Интернету). Щелкните по иконке редактирования для перехода к окну, где можно изменить параметры соединения. Для удаления существующего соединения щелкните по иконке удаления. Основное соединение удалить нельзя.
Apply (Применить)	Нажмите кнопку «Apply» (Применить), чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

4.5.1 Редактирование других соединений

Это окно используется для создания или редактирования подключений WAN. Щелкните по иконке редактирования в окне «More Connections» (Другие соединения) для настройки подключения.

Рис. 28 Редактирование других соединений



В следующей таблице даны описания полей этого окна.

Табл. 15 Редактирование других соединений

ПОЛЕ	ОПИСАНИЕ
Active (Включить)	Чтобы включить соединение, поставьте флажок в этом поле, чтобы отключить – снимите флажок.
Name (Имя)	Введите уникальное описательное имя для данного соединения длиной до 13 символов ASCII.

Табл. 15 Редактирование других соединений (продолжение)

ПОЛЕ	ОПИСАНИЕ
Mode (Режим)	Из выпадающего списка выберите режим «Routing» (Маршрутизация), если ваш Интернет-провайдер разрешает подключение нескольких компьютеров по одной учетной записи. При выборе режима «Bridge» (Мост) P660RT2 будет пересылать все пакеты, для которых не выполняется маршрутизация, на данный удаленный узел; в противном случае, эти пакеты будут сброшены.
Encapsulation (Инкапсуляция)	Из выпадающего списка выберите метод инкапсуляции, используемый Интернет-провайдером. Вариантами являются: «PPPoA», «RFC 1483», «ENET ENCAP» и «PPPoE».
User Name (Имя пользователя)	Введите имя пользователя, назначенное вашим Интернет-провайдером (только для инкапсуляции PPPoA и PPPoE). Если имя назначается в формате user@domain, где domain означает имя услуги, то введите оба элемента имени в полном соответствии с данными от провайдера.
Password (Пароль)	Введите пароль для данного имени пользователя (только для инкапсуляции PPPoA и PPPoE).
Service Name (Название услуги)	Введите имя услуги PPPoE (только для PPPoE).
Multiplexing (Мультиплексирование)	Из выпадающего списка выберите метод мультиплексирования, используемый Интернет-провайдером. Вариантами являются «VC» или «LLC». По предварительному соглашению каждому протоколу назначается отдельный виртуальный канал, например, по VC1 передается IP. При выборе «VC», необходимо ввести номера VPI и VCI для каждого протокола. При мультиплексировании на базе LLC или инкапсуляции PPP по одному виртуальному каналу передается несколько протоколов вместе с информацией идентификации протоколов, которая содержится в заголовке каждого пакета. В этом случае для всех протоколов нужно указать только один блок номеров VPI и VCI.
VPI (Идентификатор виртуального пути)	Допустимый диапазон для VPI — от 0 до 255. Введите назначенный номер VPI.
VCI (Идентификатор виртуального канала)	Допустимый диапазон для VCI - от 32 до 65535 (номера 0 - 31 зарезервированы для локального управления трафиком ATM). Введите назначенный номер VCI.
IP Address (IP-адрес)	Это поле доступно, если в поле «Mode» (Режим) выбран режим «Routing» (Маршрутизация). Статический IP-адрес — это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является фиксированным; Интернет-провайдер назначает вам новый адрес каждый раз, когда вы подключаетесь к Интернету. Если установлен тип инкапсуляции, отличный от RFC 1483, выберите «Obtain an IP Address Automatically» (Получать IP-адрес автоматически) при использовании динамического IP-адреса; в противном случае выберите «Static IP Address» (Статический IP-адрес) и введите назначенный Интернет-провайдером IP-адрес в поле «IP Address» (IP-адрес), которое находится ниже. Если используется RFC 1483, введите IP-адрес, предоставленный вашим Интернет-провайдером, в поле «IP Address» (IP-адрес).
Subnet Mask (Маска подсети)	Введите маску подсети в десятичном виде с разделительными точками. Информацию о расчете маски подсети при создании подсетей см. в *Прил. F на с. 191*.

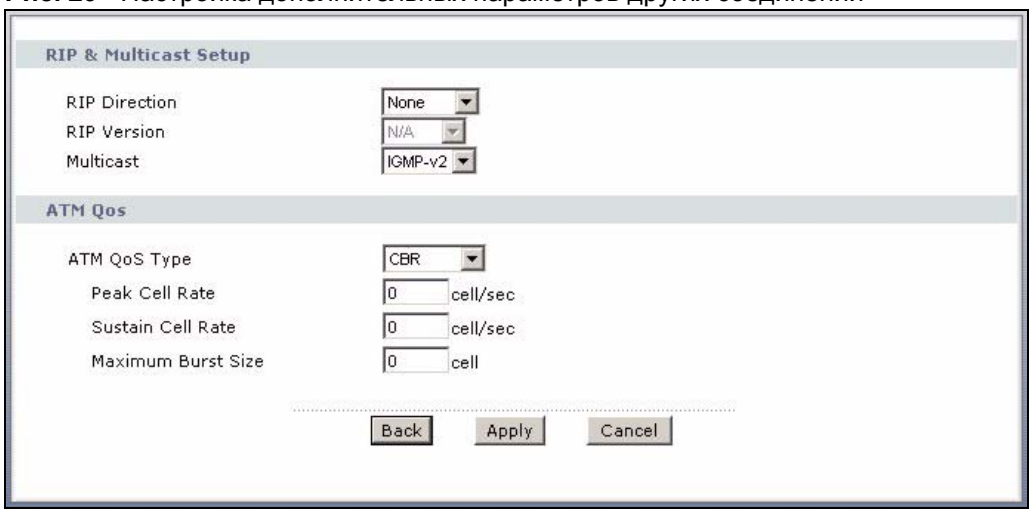
Табл. 15 Редактирование других соединений (продолжение)

ПОЛЕ	ОПИСАНИЕ
Gateway IP Address (IP-адрес шлюза)	Введите IP-адрес шлюза, предоставленный Интернет-провайдером.
Connection (Подключение)	
Nailed-Up Connection (Полупостоянное соединение)	Выберите «Nailed-Up Connection» (Полупостоянное соединение), если требуется постоянное соединение. При разрыве соединения P660RT2 автоматически будет пытаться восстановить его
Connect on Demand (Подключение по требованию)	Выберите «Connect on Demand» (Подключение по требованию), если постоянное соединение не требуется, и введите в поле «Max. Idle Timeout» (Максимальное время простоя) время простоя (в секундах).
Max Idle Timeout (Максимальное время простоя)	Если вы выбрали «Connect on Demand» (Подключение по требованию), введите интервал простоя в поле «Max Idle Timeout» (Максимальное время простоя). По умолчанию установлено 0, что означает, что соединение с Интернетом не будет разрываться.
NAT	Поле «SUA Only» (Только SUA) доступно, только если в поле «Mode» (Режим) установлено значение «Routing» (Маршрутизация). Выберите «SUA Only» (Только SUA), если имеется только один общедоступный IP-адрес и требуется использовать NAT. Щелкните по ссылке «Edit» (Редактировать) для перехода к окну «Port Forwarding» (Переадресация портов) и внесения изменений в таблицу отображения портов сервера. Чтобы отключить функцию NAT, выберите опцию «None» (Нет).
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку «Back» (Назад).
Apply (Применить)	Нажмите кнопку «Apply» (Применить), чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните по этой кнопке для отображения окна «More Connections Advanced Setup» (Дополнительные настройки других соединений) и установите дополнительные настройки глобальной сети.

4.5.2 Настройка дополнительных параметров других соединений

Это окно используется для настройки дополнительных параметров подключения P660RT2 к WAN. Щелкните по кнопке «Advanced Setup» (Дополнительные настройки) в окне «More Connections Edit» (Настройка других соединений). При этом откроется показанное ниже окно.

Рис. 29 Настройка дополнительных параметров других соединений



В следующей таблице даны описания полей этого окна.

Табл. 16 Настройка дополнительных параметров других соединений

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup (Настройка RIP и многоадресной рассылки)	
RIP Direction (Направление RIP)	Выберите направление RIP из раскрывающего списка со значениями «None» (Отключить), «Both» (Оба), «In Only» (Только входящие) и «Out Only» (Только исходящие).
RIP Version (Версия RIP)	Выберите версию RIP. Вариантами являются: «RIP-1», «RIP-2B» и «RIP-2M».
Multicast (Многоадресная рассылка)	IGMP (Internet Group Multicast Protocol/Протокол многоадресной рассылки) - это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. P660RT2 поддерживает обе версии IGMP: IGMP-v1 и IGMP-v2. Выберите «None» (Нет) для отключения IGMP.
ATM QoS (Качество услуг ATM).	
ATM QoS Type (Тип QoS ATM)	Выберите «CBR» (Continuous Bit Rate - Постоянная скорость передачи), чтобы определить фиксированную (всегда доступную) пропускную способность для голосового трафика или передачи данных. Выберите «UBR» (Неопределенная скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите «VBR-nRT» (Переменная скорость передачи вне реального времени) или «VBR-RT» (Переменная скорость передачи в реальном времени) для передачи пульсирующего трафика и разделения пропускной способности с другими приложениями.
Peak Cell Rate (Пиковая скорость ячеек)	Чтобы определить PCR (Peak Cell Rate – Пиковая скорость ячеек), разделите скорость DSL линии (бит/с) на 424 (размер ячейки ATM). Это и будет максимальная скорость, с которой отправитель может передавать ячейки. Введите в это поле значение PCR.
Sustain Cell Rate (Поддерживаемая скорость ячеек)	Параметр SCR (Sustain Cell Rate – Поддерживаемая скорость ячеек) устанавливает среднюю скорость ячеек (установившаяся скорость), с которой они могут передаваться. Введите значение SCR, оно должно быть меньше, чем PCR. Следует отметить, что по умолчанию установлено 0 ячеек/с.

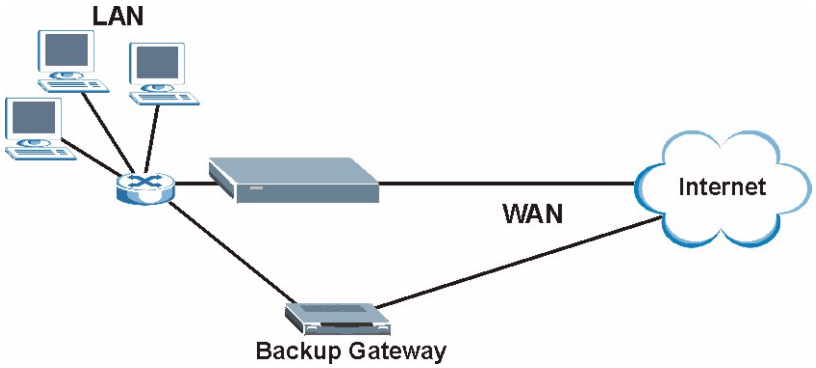
Табл. 16 Настройка дополнительных параметров других соединений (продолжение)

ПОЛЕ	ОПИСАНИЕ
Maximum Burst Size (Максимальный размер пакета)	MBS (Maximum Burst Size – Максимальный размер пакета) – это максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите значение MBS (должно быть меньше 65535).
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку «Back» (Назад).
Apply (Применить)	Нажмите кнопку «Apply» (Применить), чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

4.6 Перенаправление трафика

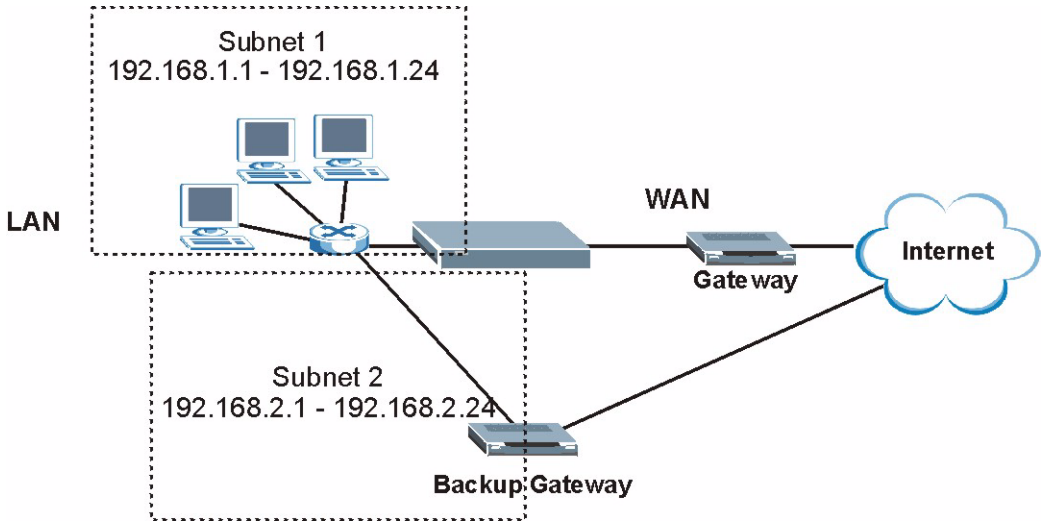
При перенаправлении трафик пересылается на резервный шлюз, если P660RT2 не может установить соединение с Интернетом. Пример показан на следующем рисунке.

Рис. 30 Пример перенаправления трафика



Топология сети, представленная ниже, позволяет избежать проблем безопасности при треугольном маршруте, если к локальной сети подключен резервный шлюз. С помощью псевдонимов IP локальную сеть можно разделить на 2 или 3 логических сети, и P660RT2 будет являться шлюзом для каждой логической сети. Поместите защищенную локальную сеть в одну подсеть (Subnet 1 на следующем рисунке), а резервный шлюз — в другую подсеть (Subnet 2). Настройте фильтры, которые пропускают пакеты от защищенной локальной сети (Subnet 1) к резервному шлюзу (Subnet 2).

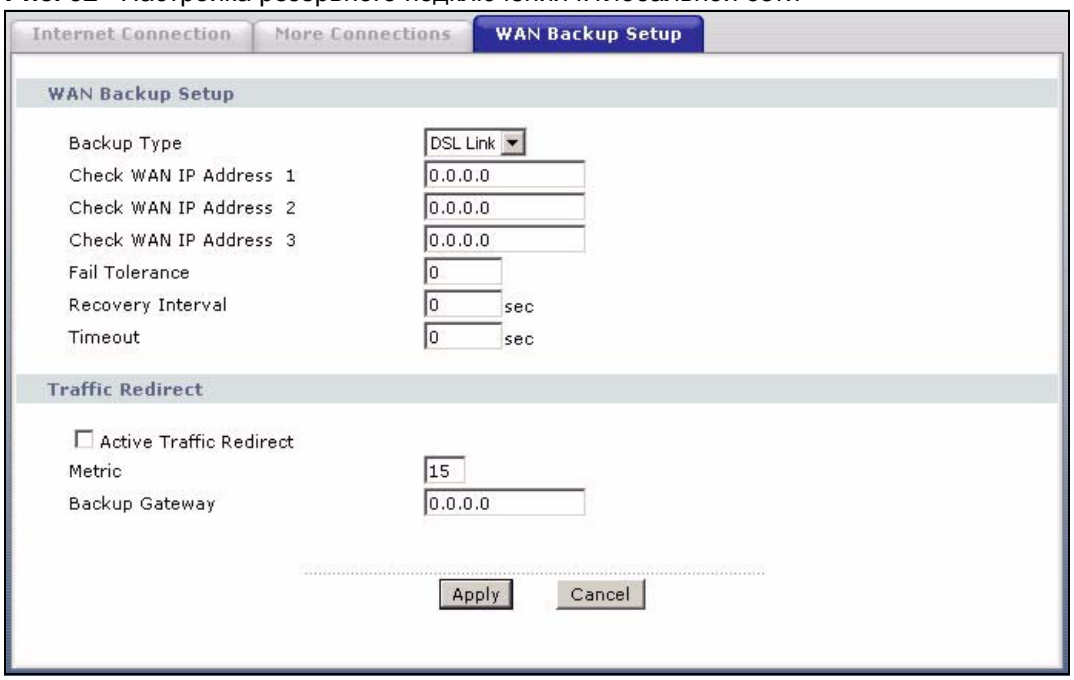
Рис. 31 Настройка локальной сети с перенаправлением трафика



4.7 Настройка резервного соединения с глобальной сетью

Это окно используется для настройки параметров резервного подключения P660RT2 к WAN. Щелкните «Network» (Сеть) > «WAN» > «WAN Backup Setup» (Настройка резервного подключения WAN). При этом откроется показанное ниже окно.

Рис. 32 Настройка резервного подключения к глобальной сети



В следующей таблице даны описания полей этого окна.

Табл. 17 Настройка резервного подключения к глобальной сети

ПОЛЕ	ОПИСАНИЕ
Backup Type (Тип резервирования)	Выберите метод, который P660RT2 будет использовать для проверки соединения DSL. Выберите «DSL Link» (Канал DSL), чтобы P660RT2 проверял, установлено ли подключение к DSL-коммутатору. Выберите «ICMP», чтобы P660RT2 периодически посылал эхо-пакеты на IP-адреса, установленные в полях «Check WAN IP Address» (Проверять IP-адреса в глобальной сети).
Check WAN IP Address1-3 (Проверять IP-адреса глобальной сети 1-3)	Заполните это поле, чтобы P660RT2 проверял доступность глобальной сети. Введите IP-адрес ближайшего надежного компьютера (например, адрес сервера DNS Интернет-провайдера). Примечание: если включена функция перенаправления трафика или резервного соединения через модем, необходимо настроить по меньшей мере один IP-адрес. При использовании резервного соединения P660RT2 периодически посылает эхо-пакеты на заданные здесь адреса и, если ответ отсутствует, переходит на следующее резевное соединение с WAN (если установлено).
Fail Tolerance (Максимальное время отсутствия ответа)	Введите время в секундах (рекомендуется 2), в течение которого P660RT2 будет посылать эхо-пакеты на IP-адреса, заданные в полях «Check WAN IP Address» (Проверять IP-адреса глобальной сети) при отсутствии ответа, прежде чем перейти на резервное соединение WAN (или другое резервное соединение WAN).
Recovery Interval (Интервал восстановления)	Если P660RT2 использует соединение с более низким приоритетом (обычно резервное соединение с WAN), он будет периодически проверять, можно ли перейти на соединение с более высоким приоритетом. Введите время в секундах (рекомендуется 30), в течение которого P660RT2 может пребывать в режиме ожидания между проверками. Увеличьте время, если устройство с IP-адресом получателя обрабатывает большой объем трафика.
Timeout (Время простоя)	Введите время в секундах (рекомендуется 3), в течение которого P660RT2 ожидает ответ на эхо-запрос от одного из IP-адресов, установленных в поле «Check WAN IP Address» (Проверять IP-адреса глобальной сети), прежде чем повторить запрос. Считается, что подключение P660RT2 к глобальной сети отсутствует, после того как пройдет время, установленое в поле «Fail Tolerance» (Максимальное время отсутствия ответа). Установите в этом поле большее значение, если ваша сеть очень занята или перегружена.
Traffic Redirect (Перенаправление трафика)	При перенаправлении трафика трафик пересылается на резервный шлюз, если P660RT2 не может установить соединение с Интернетом.
Active Traffic Redirect (Включить перенаправление трафика)	Поставьте в этом поле флажок, чтобы P660RT2 использовал перенаправление трафика, если не удается установить нормальное подключение к глобальной сети. Примечание: При включении функции перенаправления трафика, необходимо сконфигурировать хотя бы одно поле «Check WAN IP Address» (Проверять IP-адрес глобальной сети).

Табл. 17 Настройка резервного подключения к глобальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
Metric (Метрика)	В этом поле устанавливается приоритет маршрута среди маршрутов, используемых P660RT2. Метрика представляет собой «стоимость передачи данных». Маршрутизатор определяет наилучший маршрут для передачи, выбирая путь с самой низкой «стоимостью». При маршрутизации RIP для измерения стоимости используется счетчик переходов по сети, с минимальным значением, равным "1" для стоимости прямого соединения между сетями. Число должно находиться в интервале от 1 до 15; число больше 15 означает разрыв соединения. Чем меньше число, тем меньше "стоимость".
Backup Gateway (Резервный шлюз)	Введите IP-адрес резервного шлюза в десятичном виде с разделительными точками. P660RT2 автоматически пересылает трафик на данный IP-адрес при разрыве соединения с Интернетом.
Apply (Применить)	Нажмите кнопку «Apply» (Применить), чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

5

Настройка локальной сети

В этой главе описывается настройка параметров локальной сети.

5.1 Описание локальных сетей

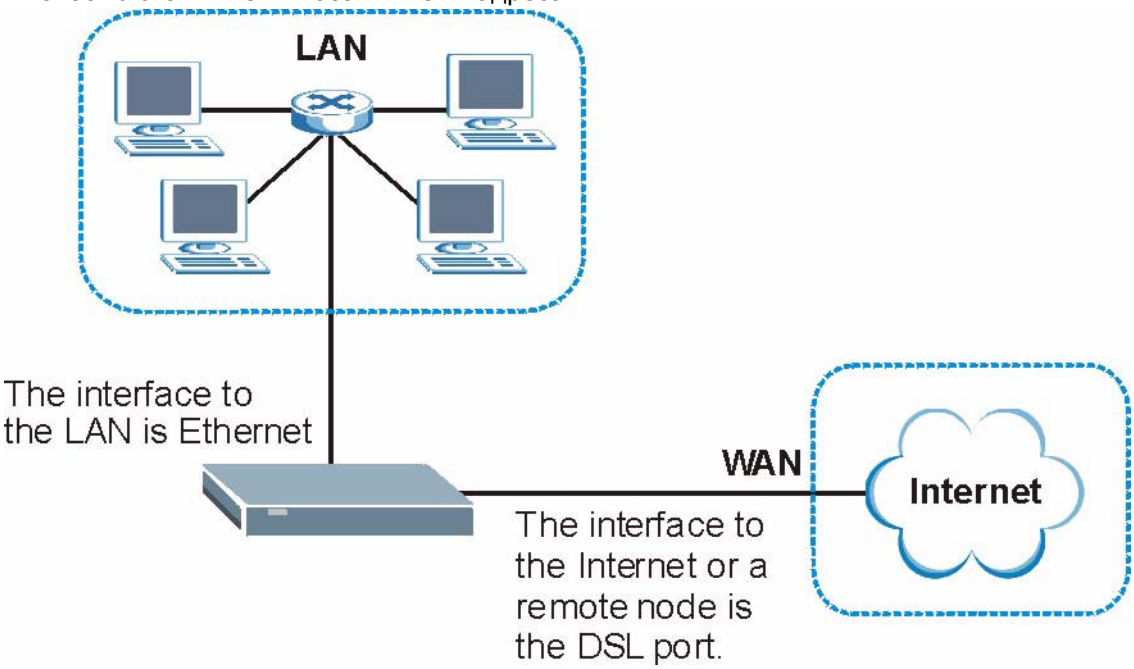
LAN (Local Area Network – Локальная сеть) – это коллективно используемая система связи, к которой подключено множество компьютеров. Локальная сеть представляет собой компьютерную сеть, ограниченную ближайшей территорией, обычно это здание или этаж в здании. Окна настройки LAN используются для настройки сервера DHCP локальной сети и управления IP-адресами.

Информацию об окнах настройки **LAN** см. в Разд. 5.4 на с. 79.

5.1.1 Локальные, глобальные сети и P660RT2

Фактическое физическое соединение определяет, являются ли порты P660RT2 портами локальной или глобальной сети. Существуют две отдельные IP-сети, одна внутренняя локальная сеть, другая внешняя глобальная сеть, как показано ниже.

Рис. 33 Локальные и глобальные IP-адреса



5.1.2 Настройка DHCP

DHCP (Dynamic Host Configuration Protocol – Протокол динамической настройки узлов, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получать настройки TCP/IP при загрузке от центрального сервера DHCP. Можно настроить P660RT2 как сервер DHCP или отключить эту функцию. При работе в режиме сервера P660RT2 предоставляет клиентами DHCP конфигурацию TCP/IP. При отключении службы DHCP требуется наличие другого сервера DHCP в локальной сети или необходимо произвести настройку компьютера вручную.

5.1.2.1 Настройка диапазона IP

В P660RT2 установлен диапазон IP-адресов клиентов DHCP (диапазон DHCP). См. характеристики изделия в приложениях. Не присваивайте компьютерам локальной сети статических IP-адресов из диапазона DHCP.

5.2 Адреса серверов DNS

Служба DNS (Domain Name System - Система имен доменов) выполняет преобразование доменного имени в соответствующий IP-адрес и наоборот. Сервер DNS играет очень важную роль, так как без него нужно было бы точно знать IP-адрес компьютера, к которому необходимо получить доступ. Адреса серверов DNS, которые задаются при настройке DHCP, передаются клиентским машинам вместе с назначенным IP-адресом и маской подсети.

Существует два способа распространения адресов серверов DNS Интернет-провайдером.

- Интернет-провайдер сообщает адреса серверов DNS, обычно в виде информационного листка при заключении договора на предоставление услуг. Если Интернет-провайдер предоставляет адреса серверов DNS, введите их в поля для серверов DNS в окне «LAN Setup» (Настройка локальной сети).
- Некоторые Интернет-провайдеры распространяют адреса серверов DNS после подключения с использованием расширений сервера DNS протокола IPCP (IP Control Protocol - протокол управления IP). Если Интернет-провайдер не предоставляет адреса серверов DNS в явной форме, значит, они передаются в процессе согласования IPCP. P660RT2 поддерживает расширения IPCP сервера DNS посредством функции прокси-сервера DNS.

  Модем P660RT2 действует как прокси-сервер DNS, если поля «Primary DNS Server» (Основной сервер DNS) и «Secondary DNS Server» (Дополнительный сервер DNS) в окне «LAN Setup» (Настройка локальной сети) оставлены пустыми.

  Следует отметить, что прокси-сервер DNS может работать, только если Интернет-провайдер использует серверные расширения DNS IPCP. Это не означает, что можно не включать серверы DNS в настройки DHCP при любых обстоятельствах. Если Интернет-провайдер предоставляет адреса серверов DNS в явной форме, убедитесь, что эти IP-адреса введены в окне «LAN Setup» (Настройка локальной сети).

5.3 Настройка TCP/IP локальной сети

P660RT2 имеет функцию встроенного сервера DHCP, которая позволяет назначать IP-адреса и серверы DNS компьютерам с установленным клиентом DHCP.

5.3.1 IP-адрес и маска подсети

Точно так же, как адреса домов на одной улице включают общее для них название этой улицы, компьютеры в локальной сети имеют один общий номер сети.

Номер сети зависит от конкретной ситуации. Если Интернет-провайдер или сетевой администратор назначают блок зарегистрированных IP-адресов, то они также дадут инструкции по выбору IP-адреса и маске подсети.

Если Интернет-провайдер не предоставляет этих данных в явной форме, то вероятнее всего он назначает динамический IP-адрес при установлении соединения. В этом случае рекомендуется выбрать IP-адрес из диапазона 192.168.0.0 – 192.168.255.0 и включить в P660RT2 функцию трансляции сетевых адресов (NAT). Агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало этот диапазон специально для частного использования. Если явно не предписано использовать другие адреса, не следует использовать номера за пределами этого диапазона. Если выбрать в качестве номера сети 192.168.1.0, получится 254 индивидуальных адреса от 192.168.1.1 до 192.168.1.254 (числа 0 и 255 зарезервированы). Другими словами, в этом случае первые три числа задают номер сети, а остальные определяют конкретный компьютер в этой сети.

Выбрав номер сети, выберите для P660RT2 IP-адрес, который легко запоминается, например, 192.168.1.1, но убедитесь, что никакое другое устройство в вашей сети не использует такой же IP-адрес.

Маска подсети определяет сетевую часть IP-адреса. P660RT2 автоматически рассчитывает маску подсети для заданного IP-адреса. Нельзя изменять маску подсети, вычисленную P660RT2, без прямых указаний.

5.3.1.1 IP-адреса для частных сетей

Каждая машина в Интернете должна иметь свой уникальный адрес. Если сеть изолирована от Интернета, например, соединяет между собой локальные сети двух филиалов, можно без проблем назначать узлам произвольные IP-адреса. Тем не менее, Агенство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало следующие три блока IP-адресов специально для частных сетей:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

IP-адрес можно получить от IANA, от Интернет-провайдера, или он может быть назначен частной сетью. Если ваша организация относительно небольшая, и доступ в Интернет осуществляется через Интернет-провайдера, Интернет-провайдер может предоставить адреса Интернета для ваших локальных сетей. С другой стороны, если организация является частью большой компании, следует проконсультироваться с сетевым администратором по поводу назначения IP-адресов.

Независимо от конкретной ситуации не стоит назначать произвольные IP-адреса; лучше следовать приведенным выше указаниям. Для получения более подробной информации по назначению адресов см. RFC 1597, *Address Allocation for Private Internets (Назначение адресов в частных сетях)* и RFC 1466, *Guidelines for Management of IP Address Space (Руководство по управлению пространством IP-адресов).*

5.3.2 Настройка RIP

RIP (Routing Information Protocol – Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Поле «RIP direction» (Направление RIP) управляет приемом и передачей пакетов RIP. Если установлено:

- «Both» (Оба) – P660RT2 осуществляет периодическую широковещательную рассылку своей маршрутной таблицы и полученных данных RIP.
- «In Only» (Только входящие) – P660RT2 не посылает пакеты RIP, но принимает все входящие пакеты RIP.
- «Out Only» (Только исходящие) – P660RT2 посылает пакеты RIP, но не принимает входящие пакеты RIP.
- «None» (Нет) – P660RT2 не посылает пакеты RIP и игнорирует все входящие пакеты RIP.

Параметр «Version» (Версия) управляет форматом и методом широковещательной рассылки пакетов RIP, которые рассылает P660RT2 (оба формата распознаются при приеме). Формат **RIP-1** является общепринятым, но формат RIP-2 содержит больше информации. Формат RIP-1 подходит для большинства сетей, если только сеть не имеет какой-либо специфической топологии.

Оба формата **RIP-2B** и **RIP-2M** осуществляют отправку данных маршрутизации в формате RIP-2. Их отличие заключается в том, что **RIP-2B** использует широковещательную рассылку для подсети, а **RIP-2M** – многоадресную рассылку.

5.3.3 Многоадресная рассылка

Обычно передача пакетов IP происходит одним из двух способов - одноадресная рассылка (1 отправитель — 1 получатель) или широковещательная рассылка (1 отправитель — все компьютеры в сети). При многоадресной рассылке IP-пакеты пересылаются конкретной группе компьютеров в сети, то есть, не одному компьютеру, но и не всем.

IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки, он не предназначен для передачи пользовательских данных. Версия 2 IGMP (RFC 2236) является усовершенствованным вариантом версии 1 (RFC 1112), однако версия 1 IGMP по-прежнему широко используется. Если Вы хотите узнать более подробную информацию о взаимодействии между версией 2 IGMP и версией 1, см. разделы 4 и 5 RFC 2236. Для идентификации групп узлов используются IP-адреса

класса D, которые находятся в диапазоне от 224.0.0.0 до 239.255.255.255. Адрес 224.0.0.0 не назначается ни одной группе и используется компьютерами, осуществляющими многоадресную рассылку IP. Адрес 224.0.0.1 используется для запросов и назначается постоянной группе, в которую входят все узлы IP (включая шлюзы). Для участия в IGMP узел должен принадлежать к группе 224.0.0.1. Адрес 224.0.0.2 назначается группе маршрутизаторов, осуществляющих многоадресную рассылку.

P660RT2 поддерживает версии IGMP 1 (IGMP-v1) и IGMP 2 (IGMP-v2). При запуске P660RT2 запрашивает все непосредственно подключенные сети о принадлежности к группе. После получения информации P660RT2 периодически обновляет ее. Многоадресную рассылку IP можно включить/отключить для интерфейсов LAN и/или WAN P660RT2 с помощью Web-конфигуратора (окна «LAN» (Локальная сеть), «WAN» (Глобальная сеть)). Для отключения многоадресной рассылки для этих интерфейсов установите «None» (Отключить).

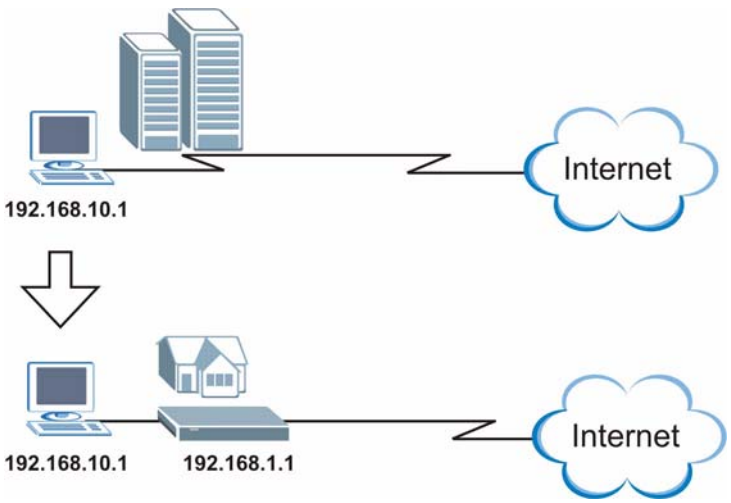
5.3.4 Any IP (Любой IP)

Чтобы предоставить компьютеру доступ в Интернет через P660RT2, необходимо, чтобы IP-адреса и маски подсети компьютера и P660RT2 находились в одной и той же подсети. В случае, если компьютеру необходимо использовать статический IP-адрес, принадлежащий другой сети, вам придется устанавливать сетевые настройки компьютера вручную каждый раз, когда нужно получить доступ в Интернет через P660RT2.

Если в P660RT2 включены функции Any IP и NAT, компьютер может получить доступ в Интернет без изменения сетевых настроек (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и P660RT2 находятся в разных подсетях. Независимо от того, динамический или статический IP-адрес назначен компьютеру, вы можете просто подключить компьютер к P660RT2 для получения доступа в Интернет.

На следующем рисунке представлен сценарий, где компьютеру назначен статический частный IP-адрес в корпоративной сети. При установке P660RT2 в жилом доме можно получить доступ в Интернет без изменения сетевых настроек компьютера, даже если IP-адреса компьютера и P660RT2 находятся в разных подсетях.

Рис. 34 Пример: Любой IP



Функция «Any IP» (Любой IP) не применяется к компьютерам с динамическим или статическим IP-адресом, принадлежащим к той же подсети, что и IP-адрес P660RT2.

Для использования в P660RT2 функции «Any IP» (Любой IP) *необходимо* включить NAT/SUA.

5.3.4.1 Как работает функция «Any IP» (Любой IP)

ARP (Address Resolution Protocol – Протокол разрешения адресов) служит для установления соответствия между адресом межсетевого протокола IP (IP-адрес) и аппаратным адресом компьютера в локальной сети, известного также как Media Access Control (Управление доступом к среде) или MAC-адрес. Таблица маршрутизации IP устройства Ethernet (P660RT2) определяет следующий транзитный пункт, который необходимо использовать для пересылки данных конкретному адресату.

Когда компьютер пытается в первый раз получить доступ в Интернет через P660RT2, выполняются следующие действия.

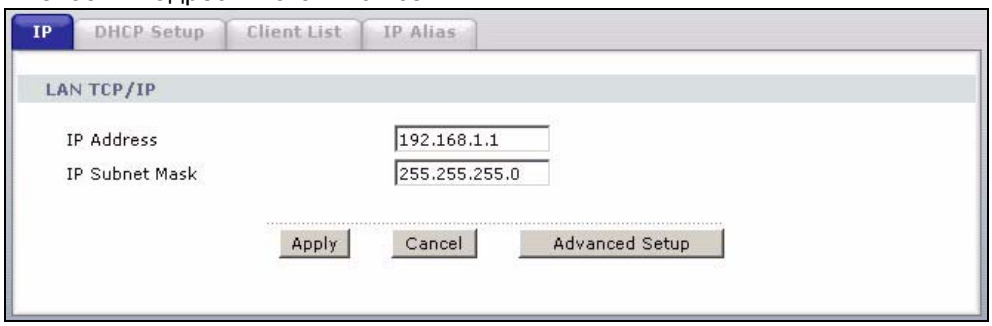
1. Если компьютер (находящийся в другой подсети) пытается в первый раз получить доступ в Интернет, он посылает пакеты на шлюз по умолчанию (не P660RT2) с помощью поиска его MAC-адреса в своей таблице ARP.
2. Если компьютер не может обнаружить шлюз по умолчанию, посылается широковещательный запрос ARP по локальной сети.
3. P660RT2 принимает запрос ARP и отвечает компьютеру, посылая ему свой MAC-адрес.
4. Компьютер обновляет MAC-адрес шлюза по умолчанию в таблице ARP. Обновив таблицу ARP, компьютер может подключаться к Интернету через P660RT2.
5. При получении пакетов от компьютера P660RT2 создает запись в таблице маршрутизации IP, с тем чтобы правильно пересылать пакеты, предназначенные для этого компьютера.

После обновления информации о маршрутизации, компьютер получает доступ к P660RT2 и к Интернет, как будто он находится в той же подсети, что и P660RT2.

5.4 Настройка IP-адреса в локальной сети

Это окно используется для настройки IP-адреса P660RT2 в локальной сети. Щелкните «LAN» (Локальная сеть), чтобы открыть окно «IP». Более подробную информацию см. в Разд. 5.1 на с. 73.

Рис. 35 IP-адрес в локальной сети



В следующей таблице даны описания полей этого окна.

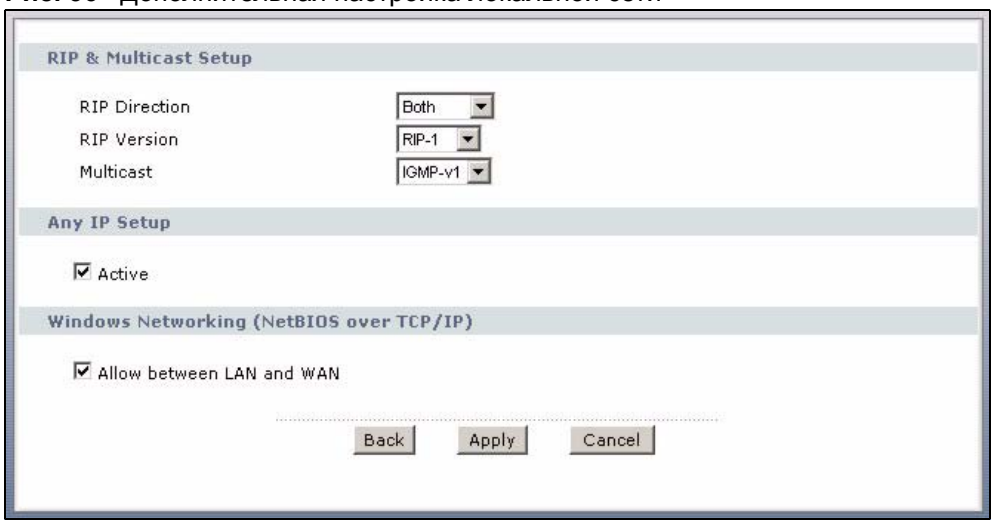
Табл. 18 IP-адрес в локальной сети

ПОЛЕ	ОПИСАНИЕ
TCP/IP	
IP-Address (IP-адрес)	Введите IP-адрес P660RT2 в десятичном виде с разделительными точками, например, 192.168.1.1 (установлен изготовителем по умолчанию).
IP Subnet Mask (Маска IP подсети)	Введите маску подсети, назначенную вашим Интернет-провайдером (если есть).
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните по этой кнопке для отображения окна «Advanced LAN Setup» (Дополнительная настройка локальной сети) и установите дополнительные настройки локальной сети.

5.4.1 Настройка дополнительных параметров локальной сети

Это окно используется для настройки дополнительных параметров подключения P660RT2 к LAN. Щелкните по кнопке «Advanced Setup» (Дополнительные настройки) в окне «LAN IP» (IP-адрес LAN). При этом откроется показанное ниже окно.

Рис. 36 Дополнительная настройка локальной сети



В следующей таблице даны описания полей этого окна.

Табл. 19 Дополнительная настройка локальной сети

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup (Настройка RIP и многоадресной рассылки)	
RIP Direction (Направление RIP)	RIP (Routing Information Protocol – Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Это поле определяет какую информацию о маршрутизации P660RT2 передает и принимает в данной подсети. Выберите направление RIP из раскрывающего списка со значениями «None» (Отключить), «Both» (Оба), «In Only» (Только входящие) и «Out Only» (Только исходящие).
RIP Version (Версия RIP)	Выберите версию RIP. Вариантами являются: «RIP-1», «RIP-2B» и «RIP-2M».
Multicast (Многоадресная рассылка)	Выберите версию IGMP, которую P660RT2 будет использовать для выполнения многоадресной рассылки в локальной сети. Пакеты многоадресной рассылки передаются группе компьютеров локальной сети, пакеты одноадресной рассылки передаются конкретному компьютеру, а пакеты широковещательной рассылки передаются всем компьютерам локальной сети. P660RT2 поддерживает обе версии IGMP: IGMP-v1 и IGMP-v2. Выберите «None» (Нет) для отключения IGMP.

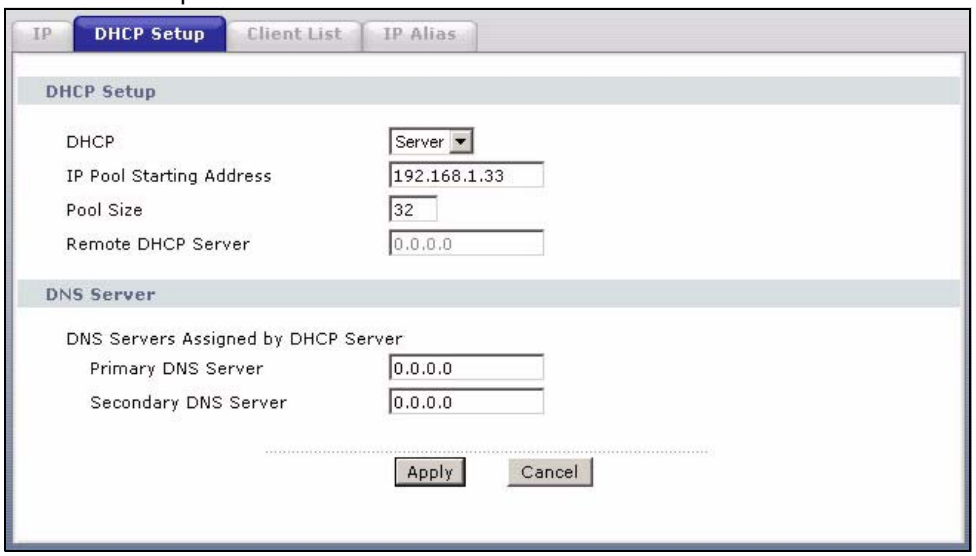
Табл. 19 Дополнительная настройка локальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
Any IP Setup (Настройка Any IP)	Поставьте флажок в окошке «Active» (Включить) для включения функции «Any IP» (Любой IP). Функция «Any IP» (Любой IP) позволяет компьютеру получить доступ в Интернет без изменения сетевых настроек (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и P660RT2 находятся в разных подсетях. При отключении функции «Any IP» (Любой IP) только компьютеры с динамическими или статическими IP-адресами, принадлежащими той же подсети, что и IP-адрес P660RT2 в локальной сети, смогут подключиться к P660RT2 или получить доступ в Интернет через P660RT2.
Windows Networking (Средства Windows для удаленного доступа в сеть (NetBIOS по TCP/IP))	Пакеты NetBIOS (Network Basic Input/Output System – Сетевая базовая система ввода-вывода) представляют собой широковещательные пакеты TCP или UDP, позволяющие устанавливать соединение и обмен данными между компьютером и локальной сетью. Для некоторых служб с автоматическим набором номера, например PPPoE или PPTP, пакеты NetBIOS могут инициировать нежелательные вызовы. Несмотря на это, иногда необходимо разрешить прохождение пакетов NetBIOS в глобальную сеть для того, чтобы найти компьютер в глобальной сети.
Allow between LAN and WAN (Разрешить передачу между LAN и WAN)	Поставьте в этом поле флажок, чтобы разрешить передачу пакетов NetBIOS из локальной сети в глобальную сеть и наоборот. Если в межсетевом экране установлена политика по умолчанию, которая блокирует трафик из глобальной сети в локальную сеть, необходимо включить правило межсетевого экрана, которое пропускает трафик NetBIOS из глобальной сети в локальную. Снимите флажок в этом поле, чтобы блокировать передачу всех пакетов NetBIOS из локальной сети в глобальную сеть и наоборот.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку «Back» (Назад).
Apply (Применить)	Нажмите кнопку «Apply» (Применить), чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

5.5 Настройка DHCP

В этом окне устанавливаются параметры сервера DNS, которые P660RT2 посылает клиентам DHCP в локальной сети.

Рис. 37 Настройка DHCP



В следующей таблице даны описания полей этого окна.

Табл. 20 Настройка DHCP

ПОЛЕ	ОПИСАНИЕ
DHCP Setup (Настройка DHCP)	
DHCP	Если в данном поле установлено значение «Server» (Сервер), то P660RT2 может назначать IP-адреса, IP-шлюз по умолчанию и серверы DNS для Windows 95, Windows NT и других систем, поддерживающих клиента DHCP. Если установлено значение «None» (Отключить), функция сервера DHCP отключена. Если установлено значение «Relay» (Ретранслятор), P660RT2 выступает в качестве фиктивного DHCP-сервера и передает запросы и ответы между удаленным сервером и клиентами. В этом случае необходимо ввести IP-адрес фактического удаленного сервера DHCP в поле «Remote DHCP Server» (Удаленный сервер DHCP). Если функция DHCP включена, необходимо установить следующие параметры:
IP Pool Starting Address (Первый адрес пула IP-адресов)	В этом поле задается первый адрес из пула непрерывных IP-адресов.
Pool Size (Размер пула)	В этом поле задается размер пула непрерывных IP-адресов.
Remote DHCP Server (Удаленный сервер DHCP)	Если в поле **«DHCP»** выбрано значение **«Relay» (Ретранслятор)**, следует ввести IP-адрес фактического удаленного сервера DHCP.
DNS Server (Сервер DNS)	

Табл. 20 Настройка DHCP

ПОЛЕ	ОПИСАНИЕ
DNS Servers Assigned by DHCP Server (Серверы DNS, назначаемые сервером DHCP)	P660RT2 пересылает IP-адрес сервера DNS (Domain Name System – Система доменных имен) клиентам DHCP.
Primary DNS Server (Основной сервер DNS) Secondary DNS Server (Вторичный DNS-сервер)	Это поле недоступно, если в поле «DHCP» установлено значение «Relay» (Ретранслятор). Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети. Если в этих полях оставлены значения **0.0.0.0**, P660RT2 выступает в качестве proxy-сервера DNS и пересылает запросы DNS от клиентов DHCP истинному серверу DNS, определенному с помощью протокола IPCP, и ретранслирует ответ назад компьютеру.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Reset (Сброс)	Нажмите «Reset» (Сброс), чтобы начать настройку заново.

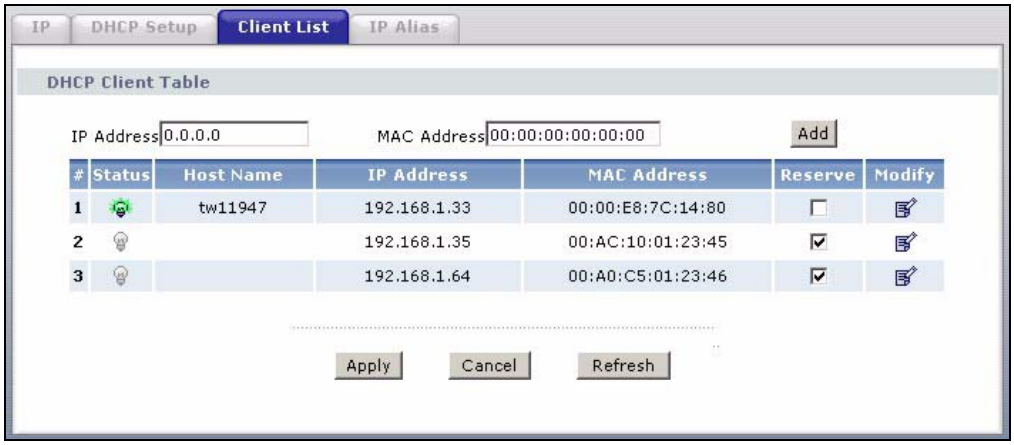
5.6 Список клиентов LAN

С помощью этой таблицы можно назначать IP-адреса отдельным компьютерам локальной сети на основе их MAC-адресов.

Каждое устройство Ethernet имеет уникальный MAC-адрес (MAC — Media Access Control — Управление доступом к среде передачи). MAC-адрес присваивается изготовителем и состоит из шести пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02.

Для изменения в P660RT2 статических настроек DHCP, нажмите кнопку «Network» (Сеть) > «LAN» (Локальная сеть) > «Client List» (Список клиентов). При этом откроется показанное ниже окно.

Рис. 38 Список клиентов LAN



В следующей таблице даны описания полей этого окна.

Табл. 21 Список клиентов LAN

ПОЛЕ	ОПИСАНИЕ
IP-Address (IP-адрес)	Введите IP-адрес, который вы хотите назначить компьютеру в локальной сети, а также его MAC-адрес в соседнее поле. IP-адрес должен находится в диапазоне IP-адресов, установленном в окне «DHCP Setup» (Настройка DHCP) для клиентов DHCP.
MAC Address (MAC-адрес)	Введите MAC-адрес компьютера локальной сети.
Add (Добавить)	Щелкните по кнопке «Add» (Добавить) для добавления статической записи DHCP.
#	Это порядковый номер записи в таблице статических IP-адресов (строки).
Status (Состояние)	Это поле показывает подключен ли данный клиент к P660RT2.
Host Name (Имя узла)	В этом поле отображается имя компьютера.
IP-Address (IP-адрес)	В этом поле отображается IP-адрес компьютера с номером, указанном выше.
MAC Address (MAC-адрес)	MAC-адрес (Media Access Control – Управление доступом к среде) или адрес Ethernet в локальной сети является уникальным для каждого компьютера (шесть пар шестнадцатеричных символов). Сетевая интерфейсная карта, такая как Ethernet-адаптер, имеет постоянный адрес, присваиваемый на заводе. Этот адрес отвечает промышленному стандарту, который обеспечивает уникальность этого адреса среди других адаптеров.
Reserve (Резервирование)	Поставьте флажки в этих полях, чтобы P660RT2 всегда назначал данные IP-адреса компьютерам с соответствующими MAC-адресами. В данной таблице можно выбрать до 32 записей.
Modify (Изменить)	Щелкните по иконке «Modify» (Изменить) для изменения **IP-адреса**.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.
Refresh (обновить)	Щелкните по кнопке «Refresh» (Обновить) для перезагрузки таблицы DHCP.

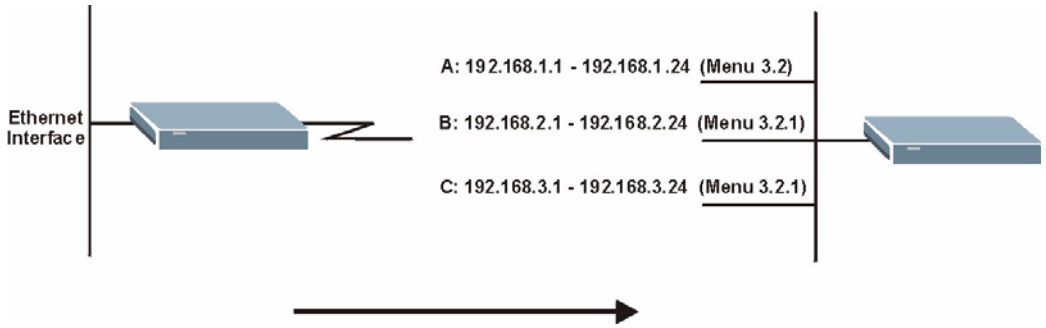
5.7 Псевдоним IP локальной сети

Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей с помощью одного интерфейса Ethernet. P660RT2 поддерживает три логических интерфейса локальной сети через один физический интерфейс Ethernet, выступая в качестве шлюза для каждой локальной сети.P660RT2

Необходимо следить, чтобы логические сети не перекрывались.

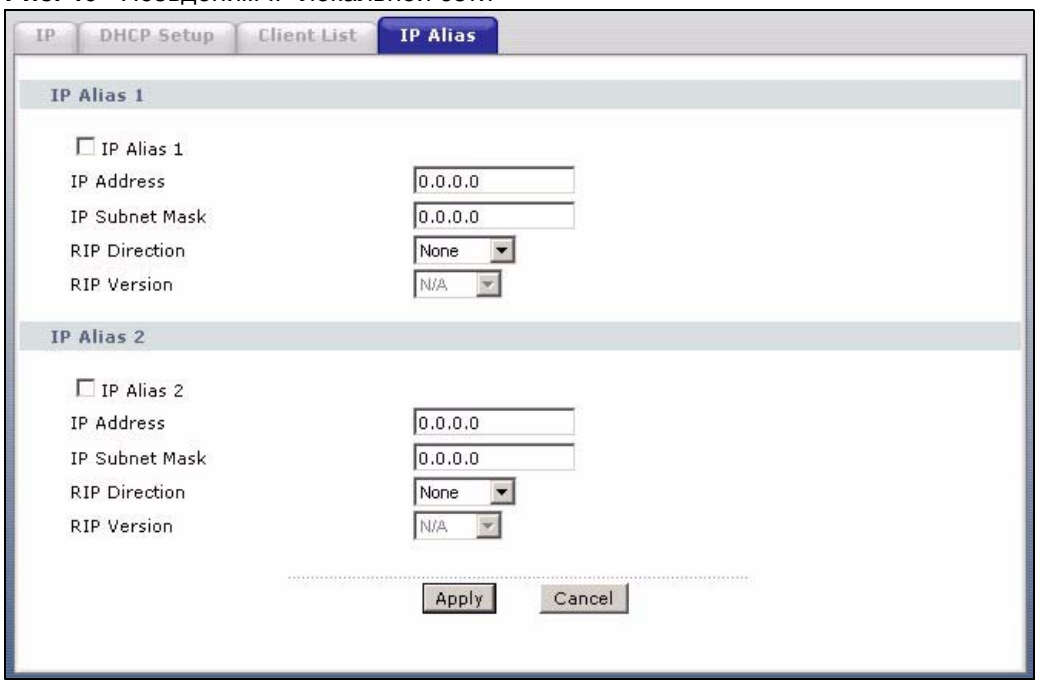
На следующем рисунке показано разделение локальной сети на подсети A, B, и C.

Рис. 39 Физическая сеть и ее разделение на логические сети



Для изменения в P660RT2 настроек псевдонимов IP щелкните «Network» (Сеть) > «LAN» (Локальная сеть) > «IP Alias» (Псевдоним IP). При этом откроется показанное ниже окно.

Рис. 40 Псевдоним IP локальной сети



В следующей таблице даны описания полей этого окна.

Табл. 22 Псевдоним IP локальной сети

ПОЛЕ	ОПИСАНИЕ
IP Alias 1, 2 (Псевдоним IP 1, 2)	Поставьте флажок для настройки другой локальной сети в P660RT2.
IP-Address (IP-адрес)	Введите IP-адрес P660RT2 в десятичном виде с разделительными точками. Или щелкните правой кнопкой мыши для копирования и/или вставки IP-адреса.

Табл. 22 Псевдоним IP локальной сети

ПОЛЕ	ОПИСАНИЕ
IP Subnet Mask (Маска IP подсети)	P660RT2 вычисляет маску подсети автоматически на основании назначенного IP-адреса. Пока не реализована структура подсетей, следует использовать маску подсети, вычисленную P660RT2.
RIP Direction (Направление RIP)	RIP (Routing Information Protocol – Протокол обмена информацией о маршрутизации, RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Поле «RIP direction» (Направление RIP) управляет приемом и передачей пакетов RIP. Выберите направление RIP из раскрывающего списка со значениями «Both» (Оба) / «In Only» (Только входящие) / «Out Only» (Только исходящие) / «None» (Нет). Если установлено «Both» (Оба) или «Out Only» (Только исходящие), P660RT2 будет периодически выполнять широковещательную рассылку своей таблицы маршрутизации. Если установлено «Both» (Оба) или «In Only» (Только входящие), модем будет объединять свои данные и полученные данные RIP; при установке «None» (Нет) модем не будет посылать пакеты RIP и будет игнорировать все входящие пакеты RIP.
RIP Version (Версия RIP)	Параметр «RIP Version» (Версия RIP) управляет форматом и методом широковещательной рассылки пакетов RIP, которые рассылает P660RT2 (оба формата распознаются при приеме). Формат RIP-1 является общепринятым, но формат RIP-2 содержит больше информации. Формат RIP-1 подходит для большинства сетей, если только сеть не имеет какой-либо специфической топологии. Оба формата **RIP-2B** и **RIP-2M** осуществляют отправку данных маршрутизации в формате RIP-2. Их отличие заключается в том, что **RIP-2B** использует широковещательную рассылку для подсети, а **RIP-2M** – многоадресную рассылку. Многоадресная рассылка снижает нагрузку на машины, которые не являются маршрутизаторами, так как они, как правило, не "прослушивают" групповой адрес пакетов RIP и, следовательно, не принимают эти пакеты. Тем не менее, если хотя бы один маршрутизатор в сети использует многоадресную рассылку, остальные маршрутизаторы также должны использовать многоадресную рассылку. По умолчанию в поле «RIP direction» (Направление RIP) установлено «Both» (Оба), а в поле «Версия RIP» установлено «RIP-1».
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

6

Окна NAT (Трансляция сетевых адресов)

В этой главе рассказывается, как настроить функцию NAT в P660RT2.

6.1 Обзор NAT

NAT (Network Address Translation – Трансляция сетевых адресов, RFC 1631) – является преобразованием IP-адреса узла в пакете, например, адреса источника исходящего пакета, используемого внутри одной сети в другой IP-адрес, известный в другой сети.

6.1.1 Определения NAT

«Внутренний/внешний» означает расположение узла относительно P660RT2, например, компьютеры ваших абонентов являются внутренними узлами, тогда как web-серверы Интернета являются внешними узлами.

Определение «глобальный/локальный» означает IP-адрес узла в пакете при прохождении этого пакета через маршрутизатор, например локальный адрес обозначает IP-адрес узла при нахождении пакета в локальной сети, тогда как глобальный адрес обозначает IP-адрес узла, когда тот же самый пакет перемещается по глобальной сети.

Следует помнить, что определение «внутренний/внешний» относится к местонахождению узла, тогда как определение «глобальный/локальный» относится к IP-адресу узла в пакете. Таким образом, внутренний локальный адрес (Inside Local Address – ILA) – это IP-адрес внутреннего узла в пакете, когда пакет находится в пределах локальной сети, тогда как внутренний глобальный адрес (Inside Global Address – IGA) – это IP-адрес того же внутреннего узла, когда пакет находится в глобальной сети. В следующей таблице приведена сводная информация.

Табл. 23 Определения NAT

ПАРАМЕТР	ОПИСАНИЕ
Внутренний	Относится к узлу в локальной сети.
Внешний	Относится к узлу в глобальной сети.
Локальный	Относится к адресу пакета (источника или адресата), когда пакет перемещается в локальной сети.
Глобальный	Относится к адресу пакета (источника или адресата), когда пакет перемещается в глобальной сети.

NAT никогда не изменяет IP-адрес (ни локальный, ни глобальный) внешнего узла.

6.1.2 Назначение NAT

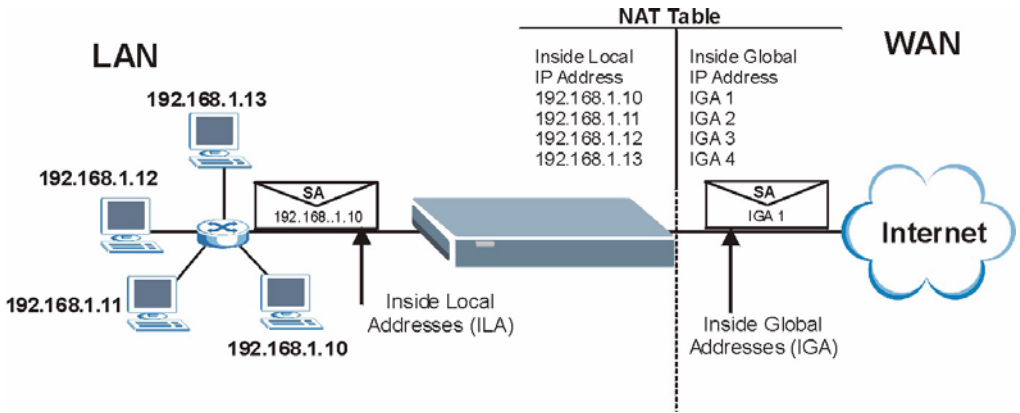
В простейшем случае NAT изменяет IP-адрес источника в пакете, принятом от абонента (внутренний локальный адрес) на другой (внутренний глобальный адрес) перед передачей пакета в глобальную сеть. При получении ответа NAT преобразовывает адрес получателя (внутренний глобальный адрес) обратно во внутренний локальный адрес перед передачей его исходному внутреннему узлу. Следует отметить, что IP-адрес (ни локальный, ни глобальный) внешнего узла никогда не изменяется.

Глобальные IP-адреса внутренних узлов могут быть статическими, или могут динамически назначаться Интернет-провайдером. Кроме того, вы можете определить серверы, например, web-сервер и сервер Telnet, находящиеся в вашей локальной сети, и сделать их доступными для внешних пользователей. Если вы не определили серверы (с отображением «много-к-одному» и «много-ко-многим с перегрузкой» – см. Табл. 24 на с. 90), NAT предлагает дополнительное преимущество защиты сети с помощью межсетевого экрана. Если серверы не установлены, P660RT2 отфильтровывает все входящие запросы, таким образом предотвращая зондирование сети злоумышленниками. Дополнительные сведения о трансляции IP-адресов см. в RFC *1631*, *"Транслятор сетевых IP-адресов (NAT)*".

6.1.3 Как работает NAT

Каждый пакет имеет два адреса – адрес источника и адрес назначения. Для исходящих пакетов внутренним локальным адресом (ILA) является адрес источника в локальной сети, а внутренним глобальным адресом (IGA) - адрес источника в глобальной сети. Для входящих пакетов ILA - это адрес назначения в локальной сети, а IGA - адрес назначения в глобальной сети. NAT преобразовывает частные (локальные) IP-адреса в уникальные глобальные, что необходимо для связи с узлами в других сетях. NAT заменяет исходный IP-адрес источника (и номера портов источника TCP или UDP на отображение много-к-одному и много-ко-многим с перекрытием) в каждом пакете и затем пересылает его в Интернет. P660RT2 отслеживает оригинальные адреса и номера портов, и, таким образом, во входящих ответных пакетах восстанавливаются исходные значения. Это иллюстрирует следующий рисунок.

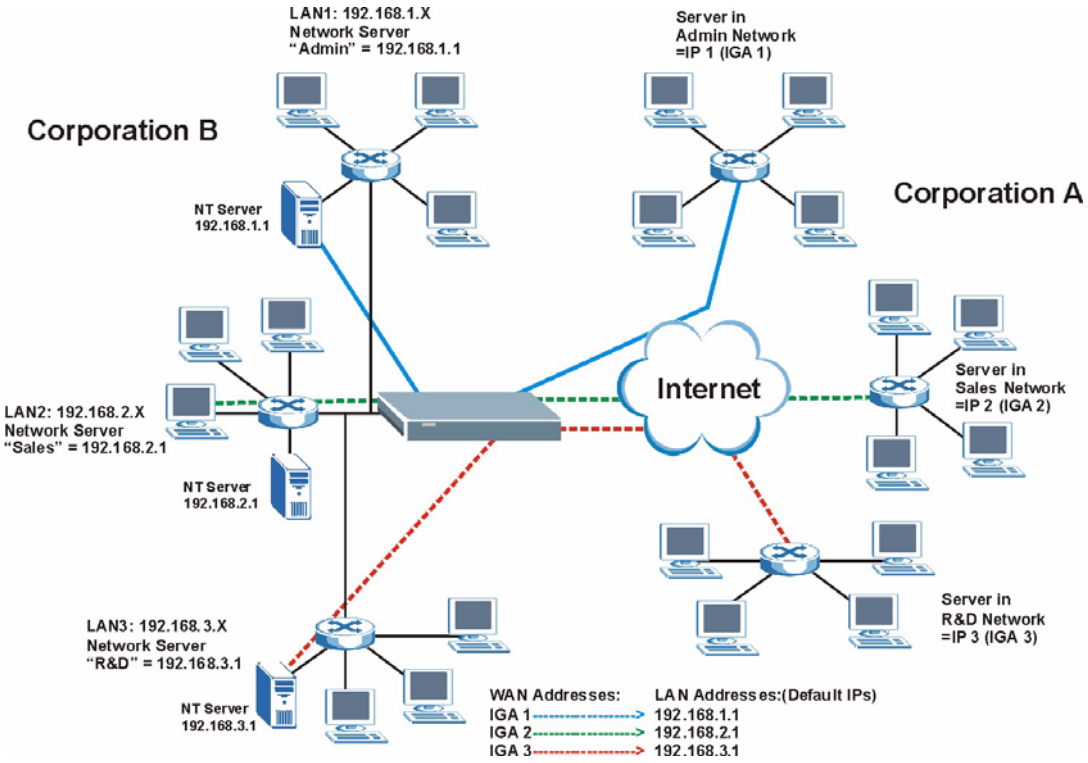
Рис. 41 Как работает NAT



6.1.4 Применение NAT

На следующем рисунке приведен вариант применения NAT, где три внутренних локальных сети (логические локальные сети, образованные с помощью псевдонимов IP), расположенные за P660RT2, взаимодействуют с тремя различными глобальными сетями. Дополнительные примеры приведены в конце данной главы.

Рис. 42 Применение NAT с использованием псевдонимов IP



6.1.5 Типы отображения NAT

NAT поддерживает пять типов преобразования адресов IP/портов, а именно:

- **Один к одному**: в режиме «один-к-одному» P660RT2 преобразовывает один локальный IP-адрес в один глобальный IP-адрес.
- **Много-к-одному**: в режиме «много-к-одному» P660RT2 преобразовывает несколько локальных IP-адресов в один глобальный IP-адрес. Эта функция эквивалентна SUA (например, PAT – Port Address Translation – Преобразование адресов портов), т. е. функции ZyXEL "Учетная запись одиночного пользователя", которая поддерживалась в предыдущих моделях маршрутизаторов ZyXEL (опция «SUA Only» (Только SUA) в современных маршрутизаторах).
- **Много-ко-многим с перегрузкой**: в режиме «много-ко-многим с перегрузкой» P660RT2 преобразовывает несколько локальных IP-адресов в несколько общих глобальных IP-адресов.
- **Много-ко-многим без перегрузки**: в режиме «много-ко-многим без перегрузки» P660RT2 преобразовывает каждый локальный IP-адрес в уникальный глобальный IP-адрес.

- **Сервер**: этот режим позволяет установить внутренние серверы для различных служб, расположенных за NAT, и сделать их доступными для внешних пользователей.

Номера портов НЕ изменяются при использовании типов отображения NAT **«один-к-одному»** и NAT **«много-ко-многим без перекрытия»**.

В следующей таблице приведена сводная информация о типах NAT.

Табл. 24 Типы отображения NAT

TYPE (ТИП)	ОТОБРАЖЕНИЕ IP
Один-к-одному	ILA1←→ IGA1
Много-к-одному (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …
Много-ко-многим с перегрузкой	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …
Много-ко-многим без перегрузки	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …
Сервер	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1

6.2 SUA (Учетная запись одиночного пользователя) в сравнении с NAT

SUA (Single User Account – Учетная запись одиночного пользователя) – это реализация в операционной системе ZyNOS подмножества NAT, которое поддерживает два типа отображения: «Many-to-One» (Много-к-одному) и «Server» (Сервер). Кроме того, P660RT2 поддерживает преобразование типа «Full Feature» (Полный набор функций), что обеспечивает преобразование нескольких глобальных IP-адресов в несколько частных локальных IP-адресов клиентов или серверов с использованием типов преобразования согласно Табл. 24 на с. 90.

- Выберите «SUA Only» (Только SUA), если P660RT2 имеет только один общедоступный IP-адрес в глобальной сети.
- Выберите «Full Feature» (Полный набор функций), если P660RT2 имеет несколько общедоступных IP-адресов в глобальной сети.

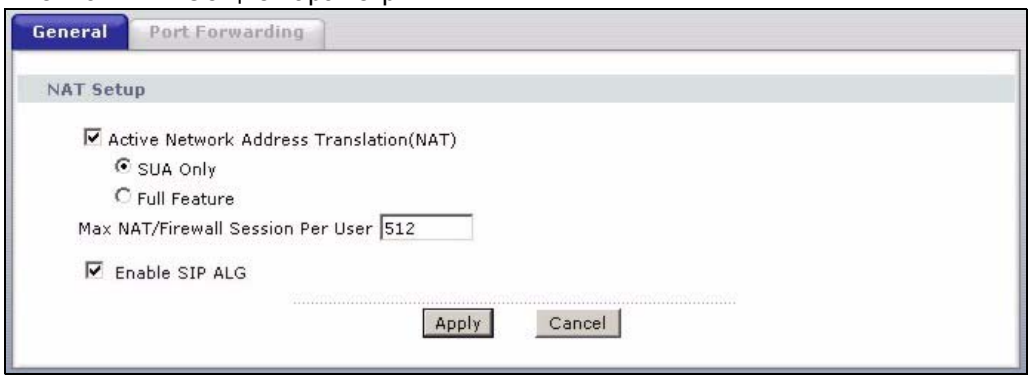
6.2.1 Шлюз SIP ALG

Некоторые NAT маршрутизаторы могут включать функцию SIP ALG (Session Initialization Protocol Application Layer Gateway – встроенный программный шлюз для приложений, использующих протокол SIP). SIP ALG позволяет вызовам SIP проходить через NAT с помощью анализа и преобразования IP-адресов, содержащихся в потоке данных. Когда P660RT2 регистрируется в сервере SIP, шлюз SIP ALG производит преобразование частного IP-адреса P660RT2 внутри потока данных SIP в общедоступный IP-адрес. При этом не требуется использовать STUN или исходящий прокси-сервер, если P660RT2 находится за шлюзом SIP ALG.

6.3 Настройка общих параметров NAT

Чтобы разрешить прохождение трафика из глобальной сети через P660RT2, необходимо в дополнение к SUA/NAT создать правило межсетевого экрана. Щелкните «Network» (Сеть) > «NAT» для отображения следующего окна. В некоторых моделях устройства не все поля являются доступными.

Рис. 43 NAT: Общие параметры



В следующей таблице даны описания полей этого окна.

Табл. 25 NAT: Общие параметры

ПОЛЕ	ОПИСАНИЕ
Active Network Address Translation (NAT) (Включить трансляцию сетевых адресов)	Поставьте флажок в этом поле, чтобы включить NAT.
SUA Only (Только SUA)	Выберите эту опцию, если P660RT2 имеет только один общедоступный IP-адрес в глобальной сети.
Full Feature (Полный набор функций)	Выберите эту опцию, если P660RT2 имеет несколько общедоступных IP-адресов в глобальной сети.

Табл. 25 NAT: Общие параметры (продолжение)

ПОЛЕ	ОПИСАНИЕ
Max NAT/ Firewall Session Per User (Макс. кол-во сеансов NAT / межсетевой экран для одного пользователя)	Когда компьютеры используют равноправное соединение (без выделеного сервера), например, при совместном использовании файлов, они могут использовать большое количество сеансов NAT. Если не ограничить количество сеансов, устанавливаемых одним клиентом, это может привести к тому, что все доступные сеансы NAT будут использованы. В таком случае, другие пользователи не смогут установить сеансы NAT и, следовательно, получить доступ в Интернет. При каждом сеансе NAT устанавливается соответствующий сеанс межсетевго экрана. Это поле предназначено для ограничения количества сеансов NAT / межсетевого экрана, которые каждый клиентский компьютер может устанавливать через P660RT2. Если в вашей сети небольшое количество пользователей использует равноправные приложения, это число можно увеличить, чтобы не снижать качество обслуживания из-за ограничения доступных каждому клиенту сеансов NAT. Если в сети большое число пользователей использует равноправные приложения, это число следует уменьшить, чтобы не допустить ситуации, когда один клиент занимает все доступные сеансы NAT.
Включить SIP ALG	Установите флажок для корректной работы SIP (VoIP) с правилами переадресации и переключения портов.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Щелкните по кнопке «Cancel» (Отменить) для восстановления предыдущей конфигурации в этом окне.

6.4 Переадресация портов

Набор переадресации портов – это список внутренних серверов (расположенных в локальной сети за NAT), например, web или FTP, которые можно сделать видимыми для внешних пользователей, несмотря на то, что NAT представляет всю внутреннюю сеть внешним пользователям как одиночный компьютер.

Можно ввести либо номер одного порта, либо диапазон номеров портов, подлежащих пересылке, и локальный IP-адрес требуемого сервера. Номер порта определяет службу, например, служба web использует порт 80, а FTP – порт 21. В некоторых случаях, когда служба неизвестна или один сервер поддерживает более одной службы (например, FTP и web), лучше указать диапазон номеров портов. Вы можете назначить IP-адрес сервера, который соответствует порту или диапазону портов.

Многие Интернет-провайдеры, предоставляющие широкополосные услуги в жилых районах, не позволяют запускать серверные приложения (такие как Web или FTP сервер) на вашем компьютере. Ваш Интернет-провайдер может периодически делать проверку на наличие серверов и может приостановить действие вашего договора, если обнаружит у вас активные службы. Для прояснения этого вопроса обратитесь к своему Интернет-провайдеру.

6.4.1 IP-адрес сервера по умолчанию

Кроме серверов для конкретных служб, NAT поддерживает IP-адрес сервера по умолчанию. Сервер по умолчанию принимает пакеты от портов, которые не указаны в представленной ниже таблице.

Если **серверу по умолчанию** не назначен IP-адрес, P660RT2 сбрасывает все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

6.4.2 Переадресация портов: Службы и номера портов

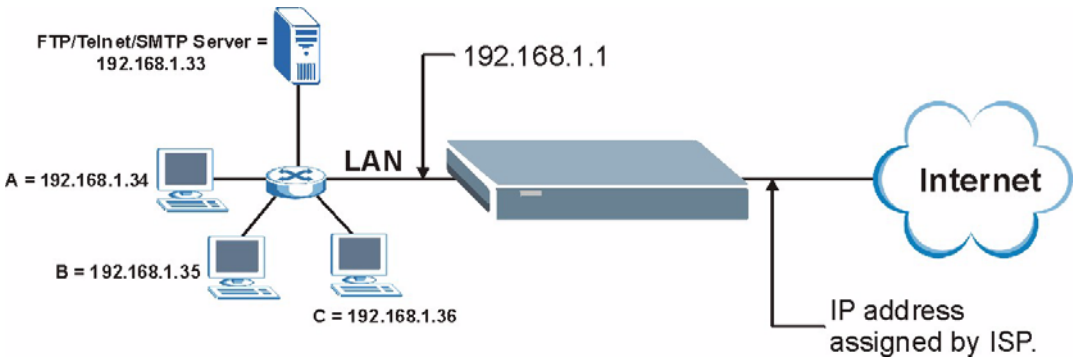
Окно «Port Forwarding» (Переадресация портов) служит для направления входящих запросов служб на соответствующие сервер(ы) локальной сети.

Соответствие служб и номеров портов см. в Прил. H на с. 205.

6.4.3 Пример настройки серверов, находящихся за преобразованием портов

Предположим, вы назначили порты с 21-го по 25-ый одному серверу FTP, Telnet и SMTP (Сервер A в примере), порт 80 другому серверу (Сервер B в примере) и назначили IP-адрес 192.168.1.35 сервера по умолчанию третьему серверу (Сервер C в примере). Вы назначили IP-адрес локальной сети, а Интернет-провайдер назначил IP-адрес в глобальной сети. Сеть с NAT для сети Интернет выглядит как одиночный узел.

Рис. 44 Пример: несколько серверов расположены за NAT



6.5 Настройка переадресации портов

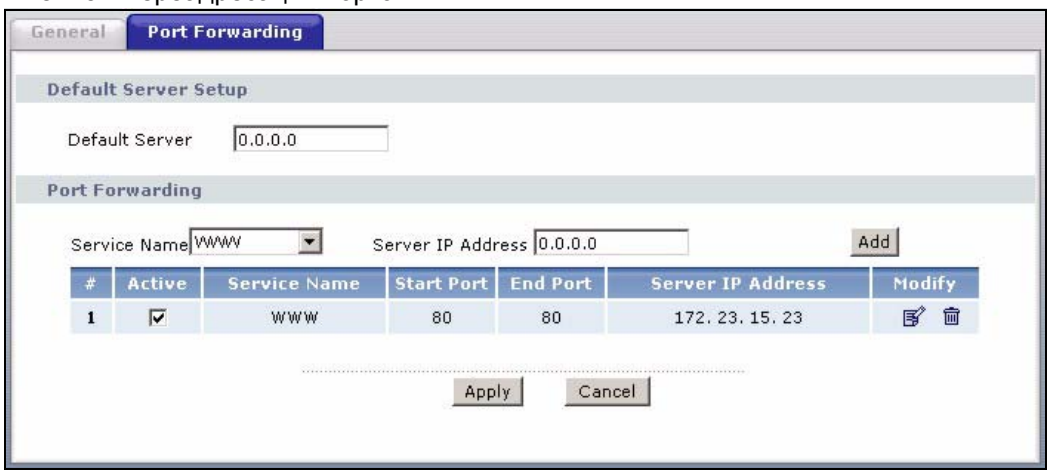
Окно «Port Forwarding» (Переадресация портов) доступно, только если установлен режим «SUA Only» (Только SUA) в окне «NAT» > «General» (Общие настройки).

Если **серверу по умолчанию** не назначен IP-адрес, P660RT2 сбрасывает все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

Щелкните «Network» (Сеть) > «NAT» > «Port Forwarding» (Переадресация портов) для отображения следующего окна.

Информацию по номерам портов, обычно используемых для конкретных служб см. в Прил. H на с. 205.

Рис. 45 Переадресация портов NAT



В следующей таблице даны описания полей этого окна.

Табл. 26 Переадресация портов NAT

ПОЛЕ	ОПИСАНИЕ
Default Server Setup (Настройка сервера по умолчанию)	
Default Server (Сервер по умолчанию)	Кроме серверов определенных видов служб NAT поддерживает сервер по умолчанию. Сервер по умолчанию принимает пакеты от портов, которые не указаны в представленной ниже таблице. Если **серверу по умолчанию** не назначен IP-адрес, P660RT2 сбрасывает все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

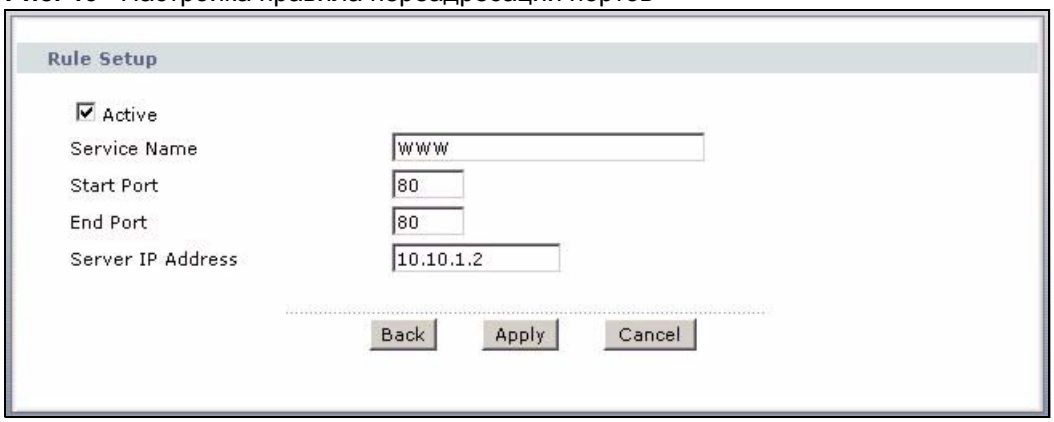
Табл. 26 Переадресация портов NAT

ПОЛЕ	ОПИСАНИЕ
Port Forwarding (Переадресация портов)	
Service Name (Название услуги)	Выберите услугу из выпадающего списка.
Server IP Address (IP-адрес сервера)	Введите IP-адрес сервера для данной услуги.
Add (Добавить)	Щелкните по этой кнопке, чтобы добавить в таблицу новое правило.
#	Это порядковый номер правила (только для чтения).
Active (Включить)	Поставьте флажок для включения правила.
Service Name (Название услуги)	Здесь отображается имя услуги.
Start Port (Начальный порт)	Это номер первого порта, определяющего услугу.
End Port (Последний порт)	Это номер последнего порта, определяющего услугу.
Server IP Address (IP-адрес сервера)	Это IP-адрес сервера.
Modify (Изменить)	Щелкните по иконке редактирования для перехода к окну, где можно изменить параметры правила переадресации портов. Щелкните по иконке удаления, чтобы удалить существующее правило переадресации портов. Следует отметить, что при удалении правила все последующие правила сдвигаются на позицию вверх.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы вернуться к предыдущей конфигурации.

6.5.1 Изменение правила переадресации портов

Это окно используется для редактирования правила переадресации портов. Щелкните по значку редактирования для соответствующего правила в окне «Port Forwarding» (Переадресация портов) для отображения следующего окна.

Рис. 46 Настройка правила переадресации портов



В следующей таблице даны описания полей этого окна.

Табл. 27 Настройка правила переадресации портов

ПОЛЕ	ОПИСАНИЕ
Active (Включить)	Поставьте флажок для включения правила.
Service Name (Название услуги)	Введите описательное имя для правила переадресации портов.
Start Port (Начальный порт)	Введите в это поле номер порта. Для переадресации трафика только одного порта, введите его номер еще раз в поле «End Port» (Последний порт). Для переадресации трафика серии портов введите в это поле номер первого порта, а в поле «End Port» (Последний порт) – номер последнего порта.
End Port (Последний порт)	Введите в это поле номер порта. Для переадресации трафика только одного порта, введите его номер в поле «Start Port» (Начальный порт), а затем введите этот же номер еще раз в это поле. Для переадресации трафика серии портов введите номер последнего порта серии портов, которая начинается с номера порта, установленного в поле «Start Port» (Начальный порт).
Server IP Address (IP-адрес сервера)	Введите в это поле внутренний IP-адрес сервера.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку «Back» (Назад).
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

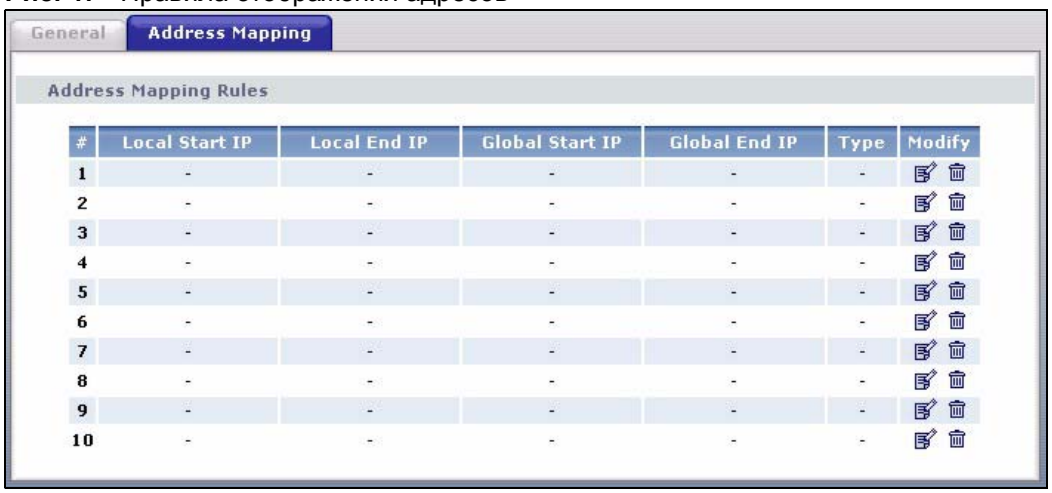
6.6 Отображение адресов

Окно «Address Mapping» (Отображение адресов) доступно, только если установлен режим «Full Feature» (Полный набор функций) в окне «NAT» > «General» (Общие настройки).

Порядок следования правил имеет большое значение, так как P660RT2 применяет правила в установленном порядке. Когда текущий пакет соответствует какому-либо правилу P660RT2 выполняет соответствующее действие и игнорирует остальные правила. Если в таблице существуют пустые правила перед новым создаваемым правилом, это правило перемещается вверх на количество позиций, равное числу пустых правил. Например, если в текущем наборе уже имеются правила с 1 по 6 и теперь создается правило под номером 9, в сводном окне набора правил новое правило будет иметь номер 7, а не 9. Теперь, если удалить правило 4, то правила с 5-го по 7-е переместятся вверх на 1 позицию, так что старые правила 5, 6 и 7 будут иметь номера 4, 5 и 6.

Для изменения в P660RT2 параметров отображения адресов, щелкните «Network» (Сеть) > «NAT» > «Address Mapping» (Отображение адресов). Появится следующее окно.

Рис. 47 Правила отображения адресов



В следующей таблице даны описания полей этого окна.

Табл. 28 Правила отображения адресов

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер правила.
Local Start IP (Начальный локальный IP-адрес)	Это начальный внутренний локальный IP-адрес (ILA). Поля локальных IP-адресов недоступны для типа отображения портов «Server» (Сервер).

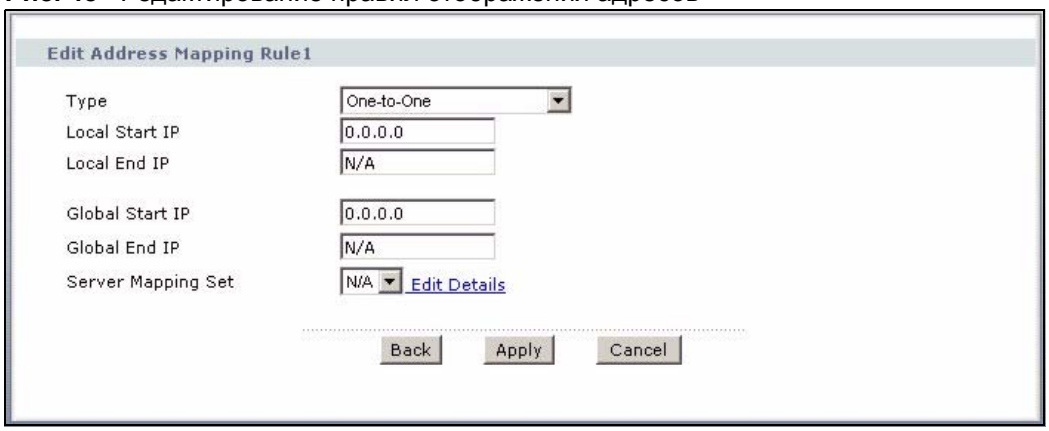
Табл. 28 Правила отображения адресов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Local End IP (Конечный локальный IP-адрес)	Это конечный внутренний локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, то в поле «Local Start IP» (Начальный локальный IP-адрес) отображается 0.0.0.0, а в поле «Local End IP» (Конечный локальный IP-адрес) отображается 255.255.255.255. В этом поле отображается «N/A» (Не применяется) для типов отображения «One-to-one» (Один-к-одному) и «Server» (Сервер).
Global Start IP (Начальный глобальный IP-адрес)	Это начальный внутренний глобальный IP-адрес (IGA). Если вы используете динамический IP-адрес, назначаемый Интернет-провайдером, введите в это поле 0.0.0.0. В этом случае используются только отображения «Many-to one» (Много-к-одному) и «Server» (Сервер).
Global End IP (Конечный глобальный IP-адрес)	Это конечный внутренний глобальный IP-адрес (IGA). В этом поле отображается «N/A» (Не применяется) для типов отображения «One-to-one» (Один-к-одному), «Many-to-One» (Много-к-одному) и «Server» (Сервер).
Type (Тип)	**1-1**: в режиме «One-to-one» (Один-к-одному) один локальный IP-адрес отображается на один глобальный IP-адрес. Следует отметить, что в режиме отображения NAT один-к-одному номера портов не изменяются. **M-1**: в режиме «Many-to-One» (Много-к-одному) несколько локальных IP-адресов отображаются на один глобальный IP-адрес. Этот режим аналогичен SUA (например, PAT, port address translation — преобразование адресов портов) — функции ZyXEL "Учетная запись одиночного пользователя", которую поддерживали предыдущие модели маршрутизаторов ZyXEL. **M-M Ov (Overload)**: в режиме «Many-to-Many Overload» (Много-ко-многим с перегрузкой) несколько локальных IP-адресов отображаются на несколько общих глобальных IP-адресов. **MM No (No Overload)**: в режиме «Many-to-Many No Overload» (Много-ко-многим без перегрузки) каждый локальный IP-адресов отображается на уникальный глобальный IP-адрес. **Server (Сервер)**: Этот режим позволяет установить внутренние серверы для различных служб, расположенных за NAT, и сделать их доступными для внешних пользователей.
Modify (Изменить)	Щелкните по иконке редактирования для перехода к окну, где можно изменить правило отображения адресов. Щелкните по иконке удаления, чтобы удалить существующее правило отображения портов. Следует отметить, что при удалении правила все последующие правила сдвигаются на позицию вверх.

6.6.1 Редактирование правил отображения адресов

Это окно используется для редактирования правила отображения адресов. Щелкните по значку редактирования для соответствующего правила в окне «Address Mapping» (Отображение адресов) для отображения следующего окна.

Рис. 48 Редактирование правил отображения адресов



В следующей таблице даны описания полей этого окна.

Табл. 29 Edit Address Mapping Rule (Редактирование правил отображения адресов)

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	Выберите тип отображения портов из следующих вариантов. • **One-to-one (Один к одному)**: В этом режиме один локальный IP-адрес отображается на один глобальный IP-адрес. Следует отметить, что номера портов не меняются при типе преобразования «Один-к-одному». • **Many-to-One (Много-к-одному)**: В режиме «много-к-одному» несколько локальных IP-адресов отображается на один глобальный IP-адрес. Этот режим аналогичен SUA (например, PAT, port address translation — преобразование адресов портов) — функции ZyXEL "Учетная запись одиночного пользователя", которую поддерживали предыдущие модели маршрутизаторов ZyXEL. • **Many-to-Many Overload (Много-ко-многим с перегрузкой)**: В режиме «много-ко-многим с перегрузкой» несколько локальных IP-адресов отображается на несколько общих глобальных IP-адресов. • **Many-to-Many No Overload (Много-ко-многим без перегрузки)**: В режиме «много-ко-многим без перегрузки» каждый локальный IP-адрес отображается на уникальный глобальный IP-адрес. • **Server (Сервер)**: Этот режим позволяет установить внутренние серверы для различных служб, расположенных за NAT, и сделать их доступными для внешних пользователей.
Local Start IP (Начальный локальный IP-адрес)	Это начальный локальный IP-адрес (ILA). Поля локальных IP-адресов недоступны для отображения портов **«Server» (Сервер)**.
Local End IP (Конечный локальный IP-адрес)	Это конечный локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, то в поле «Local Start IP» (Начальный локальный IP-адрес) введите 0.0.0.0, а в поле «Local End IP» (Конечный локальный IP-адрес) введите 255.255.255.255. В этом поле отображается «N/A» (Не применяется) для типов отображения «One-to-one» (Один-к-одному) и «Server» (Сервер).
Global Start IP (Начальный глобальный IP-адрес)	Это начальный глобальный IP-адрес (IGA). Если вы используете динамический IP-адрес, назначаемый Интернет-провайдером, введите в это поле 0.0.0.0.

Табл. 29 Edit Address Mapping Rule (Редактирование правил отображения адресов)

ПОЛЕ	ОПИСАНИЕ
Global End IP (Конечный глобальный IP-адрес)	Это конечный глобальный IP-адрес (IGA). В этом поле отображается «N/A» (Не применяется) для типов отображения «One-to-one» (Один-к-одному), «Many-to-One» (Много-к-одному) и «Server» (Сервер).
Server Mapping Set (Набор отображения серверов)	Это поле доступно, только если в поле «Type» (Тип) установлено значение «Server» (Сервер). Выберите число из выпадающего списка, чтобы установить набор отображения серверов.
Edit Details (Редактировать параметры)	Щелкните по этой ссылке для перехода к окну «Port Forwarding» (Переадресация портов) для внесения изменений в набор отображения серверов, установленный в поле «Server Mapping Set» (Набор отображения серверов).
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку «Back» (Назад).
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

7

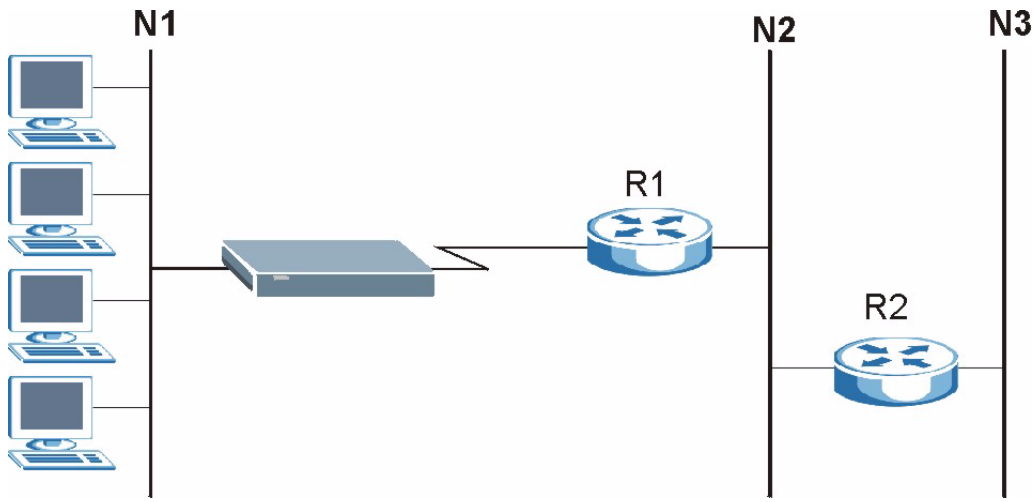
Статический маршрут

В этой главе рассказывается о настройке статических маршрутов P660RT2.

7.1 Статический маршрут

Каждый удаленный узел определяет только ту сеть, к шлюзу которой он непосредственно подключается. Аналогично и P660RT2 не имеет никакой информации о сетях, находящихся за ним. В примере на следующем рисунке P660RT2 получает информацию о сети N2 через маршрутизатор R1 удаленного узла. Несмотря на это, P660RT2 не может отправить пакет в сеть N3, так как он «не знает», что существует маршрут через маршрутизатор R1 удаленного узла и маршрутизатор R2. Статические маршруты предназначены для того, чтобы предоставлять P660RT2 информацию о сетях за пределами удаленных узлов.

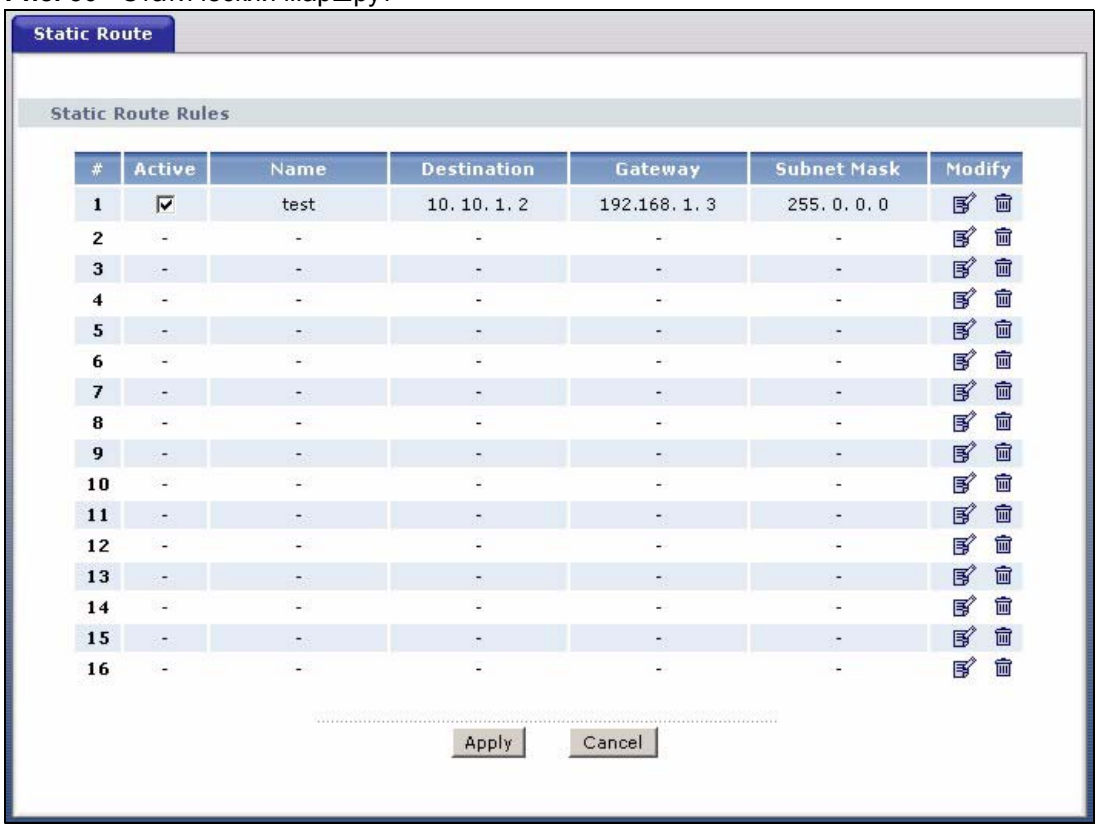
Рис. 49 Пример топологии статической маршрутизации



7.2 Настройка статических маршрутов

Щелкните «Advanced» (Дополнительно) > «Static Route» (Статический маршрут) для отображения окна «Static Route» (Статический маршрут).

Рис. 50 Статический маршрут



В следующей таблице даны описания полей этого окна.

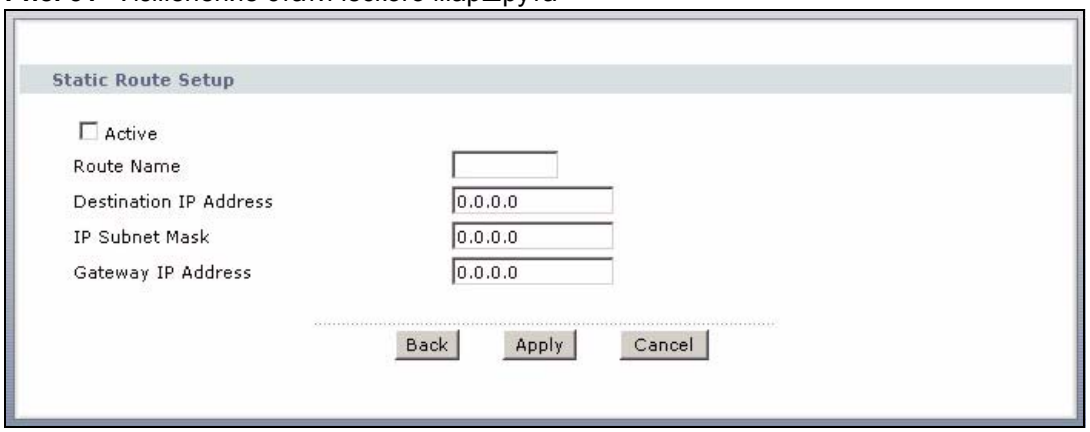
Табл. 30 Статический маршрут

ПОЛЕ	ОПИСАНИЕ
#	Это номер конкретного маршрута.
Active (Включить)	Установите флажок, чтобы включить данный статический маршрут. В другом случае, снимите флажок.
Name (Имя)	Это описательное имя данного маршрута.
Destination (Получатель)	Данный параметр определяет IP-адрес сети конечного адресата. Маршрутизация всегда выполняется на основе номера сети.
Gateway (Шлюз)	В этом поле отображается IP-адрес шлюза. Шлюз – это маршрутизатор или коммутатор, находящийся в том же сегменте сети, что и порт LAN или WAN устройства. Шлюз помогает отправлять пакеты в пункты назначения.
Subnet Mask (Маска подсети)	Это маска IP подсети.
Modify (Изменить)	Щелкните по иконке редактирования для перехода к окну, где можно изменить параметры статического маршрута P660RT2. Щелкните по иконке удаления для удаления статического маршрута P660RT2. Появится окно с запросом на подтверждение операции удаления маршрута.

7.2.1 Изменение статического маршрута

Выберите номер статического маршрута и щелкните по иконке «Edit» (Редактирование). При этом откроется показанное ниже окно. В этом окне выполняется настройка параметров статического маршрута.

Рис. 51 Изменение статического маршрута



В следующей таблице даны описания полей этого окна.

Табл. 31 Изменение статического маршрута

ПОЛЕ	ОПИСАНИЕ
Active (Включить)	Это поле позволяет включать/выключать статический маршрут.
Route Name (Имя маршрута)	Введите имя статического маршрута IP. Чтобы удалить данный статический маршрут, оставьте это поле пустым.
Destination IP Address (IP-адрес получателя)	Данный параметр определяет IP-адрес сети конечного адресата. Маршрутизация всегда выполняется на основе номера сети. Для указания маршрута к отдельному узлу, в поле маски подсети устанавливается 255.255.255.255, чтобы номер сети был таким же, как и идентификационный номер (ID) узла.
IP Subnet Mask (Маска IP подсети)	Введите маску подсети IP.
Gateway IP Address (IP-адрес шлюза)	Ввод IP-адреса шлюза. Шлюз – это маршрутизатор или коммутатор, находящийся в том же сегменте сети, что и порт LAN или WAN устройства. Шлюз помогает отправлять пакеты в пункты назначения.
Back (Назад)	Для возврата к предыдущему окну без сохранения изменений нажмите кнопку «Back» (Назад).
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы заново начать настройку в этом окне.

8

Настройка динамической системы доменных имен (DYNDNS)

В этой главе рассказывается, как выполнить настройку P660RT2 для использования динамической службы доменных имен.

8.1 Динамическая система доменных имен (DYNDNS) – общая информация

Динамическая система доменных имен (DYNDNS) позволяет обновлять ваш текущий динамический IP-адрес с помощью одной или нескольких служб динамических DNS, чтобы любой компьютер мог взаимодействовать с вашим (посредством NetMeeting, CU-SeeMe и т. д.). Вы также можете обеспечить доступ к серверу FTP или Web-сайту на вашем компьютере, с использованием доменного имени (например, myhost.dhs.org, где myhost – имя по вашему выбору), которое остается постоянным, вместо использования IP-адреса, который назначается заново при каждом подключении. Ваши друзья или родственники всегда смогут получить доступ к вашему ресурсу, даже если они не знают точного IP-адреса.

Прежде всего необходимо зарегистрировать учетную запись динамического DNS на сайте www.dyndns.org. Эта услуга предназначена для тех, кто использует динамический IP-адрес, назначаемый Интернет-провайдером или сервером DHCP, и кто хотел бы иметь доменное имя. Провайдер услуг динамической DNS предоставляет пароль или ключ.

8.1.1 Маски DYNDNS

Включение функции шаблонов приводит к тому, что адреса вида *.yourhost.dyndns.org привязываются к тому же IP-адресу, что и yourhost.dyndns.org. Данная функция полезна, если вы хотите иметь возможность использовать, например, адрес www.yourhost.dyndns.org и при этом предоставлять доступ к вашему узлу.

Если вы имеете частный IP-адрес в глобальной сети, то динамическую DNS использовать нельзя.

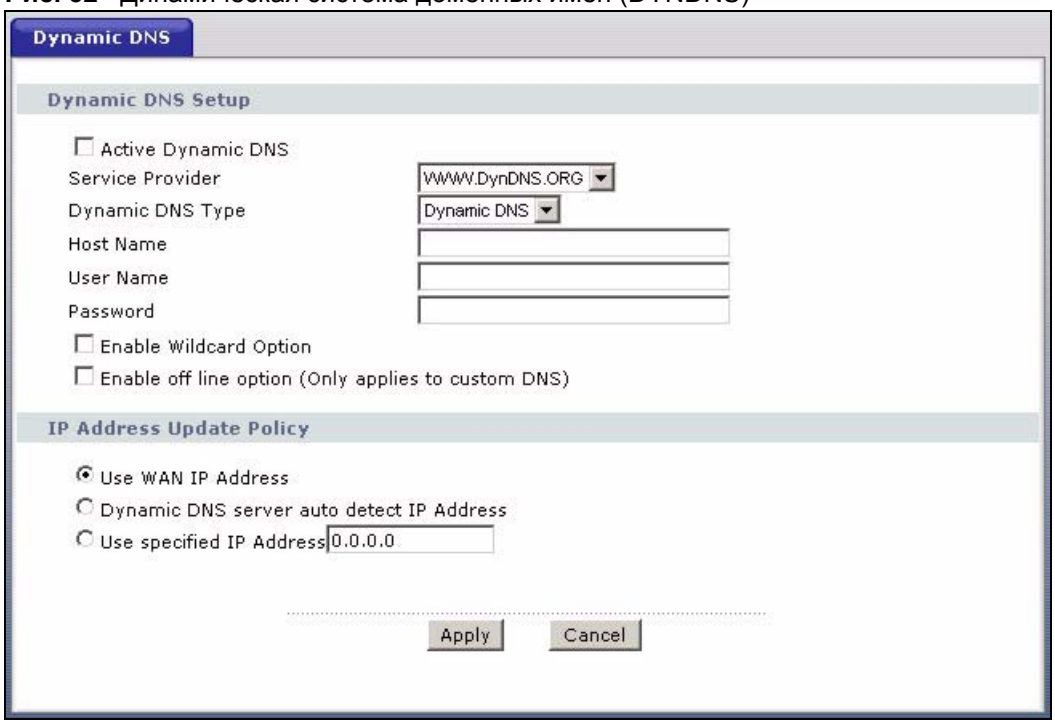
Инструкции по настройке см. в Разд. 8.2 на с. 106.

8.2 Настройка динамической DNS (DYNDNS)

Это окно используется для изменения параметров DDNSP660RT2. Щелкните «Advanced» (Дополнительно) > «Dynamic DNS» (Динамическая DNS). При этом откроется показанное ниже окно.

Более подробную информацию см. в Разд. 8.1 на с. 105.

Рис. 52 Динамическая система доменных имен (DYNDNS)



В следующей таблице даны описания полей этого окна.

Табл. 32 Динамическая система доменных имен (DYNDNS)

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS Setup (Настройка динамической DNS)	
Active Dynamic DNS (Включить динамическую DNS)	Установите флажок в этом окошке для использования динамической службы доменных имен.
Service Provider (Провайдер услуг)	В этом поле отображается имя провайдера услуг динамической DNS.
Dynamic DNS Type (Тип динамической DNS)	Выберите тип службы, предоставляемой вашим провайдером услуг динамической DNS
Host Name (Имя узла)	Введите доменное имя, назначенное модему P660RT2 провайдером услуг динамической DNS. Можно ввести в это поле 2 имени, разделенных запятой (",").
User Name (Имя пользователя)	Введите имя пользователя.
Password-(Пароль)	Введите назначенный пароль.

Табл. 32 Динамическая система доменных имен (DYNDNS) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Enable Wildcard Option (Включить маску)	Установите этот флажок для включения маски DYNDNS.
Enable off line option (Включить автономный режим)	Это поле доступно, только если в поле «DDNS Type» (Тип DDNS) установлено «Custom DNS» (Пользовательская DNS). Проверьте, что провайдер услуг динамической DNS обеспечивает перенаправление трафика на указаный вами URL во время отсутствия подключения к сети.
IP Address Update Policy (Политика обновления IP-адреса)	
Use WAN IP Address (Использовать IP-адрес в глобальной сети)	Выберите эту опцию для обновления IP-адреса для имени узла(ов) на IP-адрес в глобальной сети.
Dynamic DNS server auto detect IP Address (IP-адрес автоматически обнаруженного сервера DDNS)	Выберите эту опцию, если присутствует один или несколько NAT-маршрутизаторов между P660RT2 и сервером DDNS. Эта функция обеспечивает автоматическое обнаружение сервера DDNS и использование IP-адреса NAT-маршрутизатора, который имеет общедоступный IP-адрес. Примечание: если между P660RT2 и сервером DDNS присутствует proxy-сервер HTTP, сервер DDNS не сможет обнаружить соответстующий IP-адрес.
Use WAN IP Address (Использовать IP-адрес)	Введите IP-адрес для имени узла(ов). Выберите эту опцию, если используется статический IP-адрес.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

9

Настройка удаленного управления

В этой главе рассказывается как настроить удаленное управление устройством.

9.1 Удаленное управление – общая информация

При помощи удаленного управления можно определить службы/протоколы для доступа к P660RT2, интерфейс управления, а также компьютеры, с которых можно выполнять управление модеммодемом.

Возможны следующие режимы удаленного управления P660RT2:

- Интернет (только глобальная сеть)
- Все (локальная и глобальная сети)
- Только LAN
- Отключено

Для отключения удаленного управления конкретной службой выберите «Disable» (Отключить) в соответствующем поле «Access Status» (Статус доступа).

Одновременно допускается проведение только одного сеанса удаленного управления. P660RT2 автоматически завершает сеанс удаленного управления с более низким приоритетом, если запускается другой сеанс удаленного управления, имеющий более высокий приоритет. Для сеансов удаленного управления существуют следующие приоритеты:

1. Управление с помощью Telnet
2. HTTP

9.1.1 Ограничения на удаленное управление

Удаленное управление через локальную или глобальную сеть не будет работать, если:

- Эта служба отключена в окне настройки удаленного управления.
- IP-адрес, установленный в поле «Secured Client IP» (IP-адрес доверенного клиента), не совпадает с IP-адресом клиента. В случае несовпадения P660RT2 немедленно завершает сеанс связи.
- Уже выполняется другой сеанс удаленного управления с равным или более высоким приоритетом. Одновременно допускается проведение только одного сеанса удаленного управления.

- Существует правило межсетевого экрана, блокирующее удаленное управление.

9.1.2 Удаленное управление и NAT

Если функция трансляции сетевых адресов (NAT) включена, то:

- при управлении из глобальной сети необходимо использовать IP-адрес P660RT2 в глобальной сети;
- при управлении из локальной сети необходимо использовать IP-адрес P660RT2 в локальной сети.

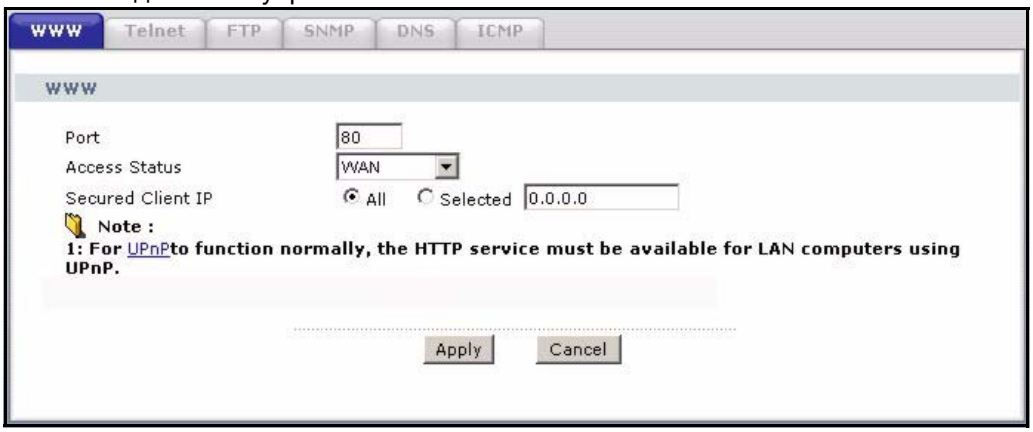
9.1.3 Время простоя системы

По умолчанию время простоя системы при выполнении сеанса управления установлено 5 минут (300 секунд). Модем P660RT2 автоматически завершает сеанс управления при простое, продолжающемся более этого периода. Сеанс управления не разрывается, если в окне статистики проводится опрос системы.

9.2 WWW

Это окно используется для изменения параметров WWW P660RT2 (World Wide Web – "Всемирная паутина". Щелкните «Advanced» (Дополнительно) > «Remote MGMT» (Удаленное управление) для отображения окна **WWW**.

Рис. 53 Удаленное управление: WWW



В следующей таблице даны описания полей этого окна.

Табл. 33 Удаленное управление: WWW

ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Статус доступа)	Выберите интерфейс(ы), через который компьютер сможет получить доступ к P660RT2 при использовании этой службы.

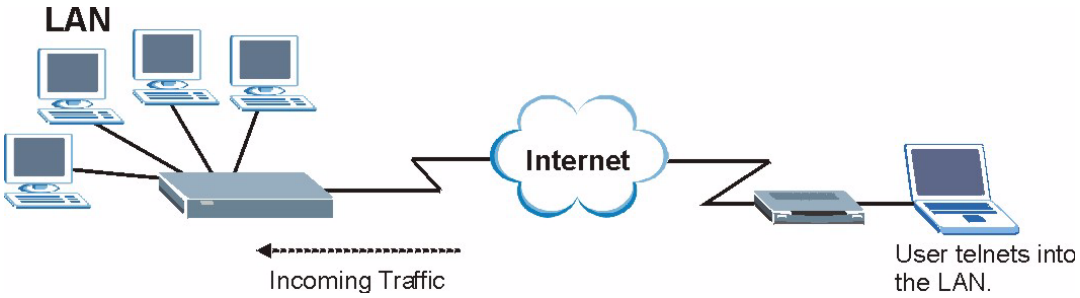
Табл. 33 Удаленное управление: WWW

ПОЛЕ	ОПИСАНИЕ
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660RT2 при использовании этой службы. Выберите «All» (Все), чтобы разрешить любому компьютеру доступ к P660RT2 при использовании этой службы. Выберите «Selected» (Выбранный), чтобы разрешить доступ к P660RT2 только компьютеру с указанным IP-адресом при использовании этой службы.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

9.3 Управление с помощью Telnet

Можно настроить удаленный доступ к P660RT2 через Telnet, как показано ниже. Администратор с компьютера в удаленной сети подключается к P660RT2 с помощью Telnet.

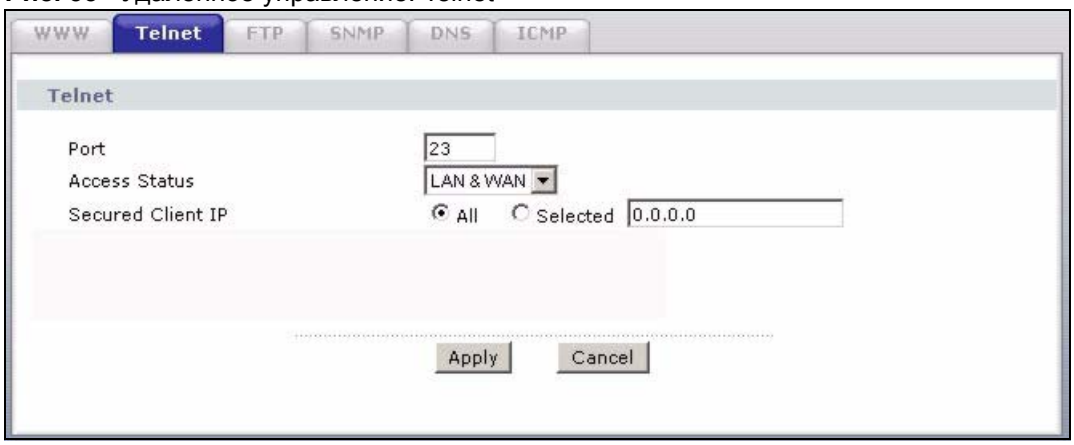
Рис. 54 Настройка Telnet в сети TCP/IP



9.4 Настройка Telnet

Щелкните «Advanced» (Дополнительно) > «Remote MGMT» (Удаленное управление) > и закладку «Telnet» для отображения окна, показанного ниже. Это окно используется для настройки параметров доступа к P660RT2 с помощью Telnet.

Рис. 55 Удаленное управление: Telnet



В следующей таблице даны описания полей этого окна.

Табл. 34 Удаленное управление: Telnet

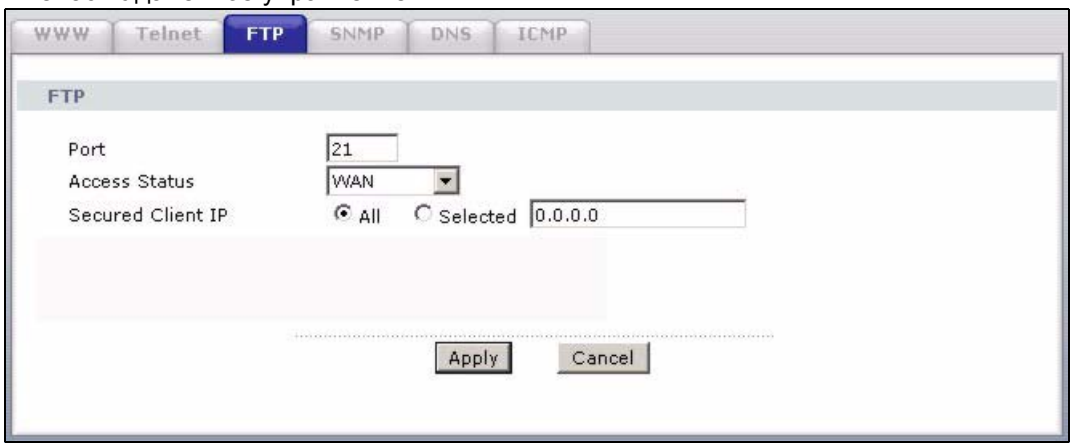
ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Статус доступа)	Выберите интерфейс(ы), через который компьютер сможет получить доступ к P660RT2 при использовании этой службы.
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660RT2 при использовании этой службы. Выберите «All» (Все), чтобы разрешить любому компьютеру доступ к P660RT2 при использовании этой службы. Выберите «Selected» (Выбранный), чтобы разрешить доступ к P660RT2 только компьютеру с указанным IP-адресом при использовании этой службы.
Apply (Применить)	Щелкните «Apply» (Применить) для сохранения сделанных настроек и выхода из этого окна.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

9.5 Настройка FTP

С помощью FTP можно выполнять загрузку и выгрузку микропрограммы P660RT2, а также файлов конфигурации, подробнее см. главу о микропрограмме и сопровождении файлов конфигурации. Чтобы использовать эту функцию, на компьютере должен быть установлен FTP-клиент..

Для изменения настроек FTP в P660RT2 щелкните «Advanced» (Дополнительно) > «Remote MGMT» (Удаленное управление) > и закладку «FTP». При этом откроется показанное ниже окно.

Рис. 56 Удаленное управление: FTP



В следующей таблице даны описания полей этого окна.

Табл. 35 Удаленное управление: FTP

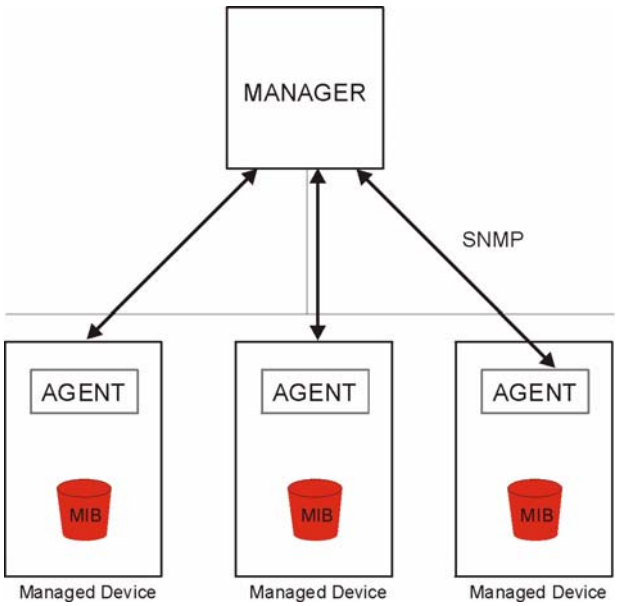
ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Статус доступа)	Выберите интерфейс(ы), через который компьютер сможет получить доступ к P660RT2 при использовании этой службы.
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660RT2 при использовании этой службы. Выберите «All» (Все), чтобы разрешить любому компьютеру доступ к P660RT2 при использовании этой службы. Выберите «Selected» (Выбранный), чтобы разрешить доступ к P660RT2 только компьютеру с указанным IP-адресом при использовании этой службы.
Apply (Применить)	Щелкните «Apply» (Применить) для сохранения сделанных настроек и выхода из этого окна.
Отмена	Щелкните **Cancel**, чтобы начать настройку заново.

9.6 Протокол SNMP

Простой протокол управления сетью (SNMP – Simple Network Management Protocol) используется для осуществления обмена управляющей информацией между сетевыми устройствами. SNMP входит в состав стека протоколов TCP/IP. Модем P660RT2 функцию агента SNMP, что позволяет выполнять управление и мониторинг P660RT2 с управляющей станции по сети. P660RT2 поддерживает протокол SNMP версии один (SNMPv1) и версии два (SNMPv2). На следующем рисунке показана модель управления по протоколу SNMP.

Протокол SNMP доступен только при настроенном TCP/IP.

Рис. 57 Модель управления SNMP



Сети под управлением протокола SNMP состоят из двух основных компонентов: агентов и управляющей программы.

Агент представляет собой модуль программы управления, находящийся в управляемом устройстве (P660RT2). Агент преобразует информацию о локальном управлении, получаемую от управляемого устройства, в форму, совместимую с протоколом SNMP. Управляющая программа – это консоль управления, с помощью которой сетевые администраторы осуществляют функции управления сетью. Через консоль происходит запуск приложений, предназначенных для контроля и мониторинга управляемых устройств.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют каждый фрагмент информации, собираемой об устройстве. В качестве примеров переменных можно назвать число полученных пакетов, статус порта узла и т. д. База управляющей информации (MIB) – это совокупность управляемых объектов. Протокол SNMP позволяет управляющей программе и агентам взаимодействовать друг с другом с целью доступа к этим объектам.

Сам по себе протокол SNMP является простым протоколом типа "запрос-ответ", работающим по модели "управляющая станция/агент". Управляющая программа выдает запрос, а агент возвращает ответы с помощью следующих протокольных операций:

- Get (Получить) – позволяет управляющей программе извлечь объектную переменную из агента.
- GetNext (Получить следующее) — позволяет управляющей программе извлечь следующую объектную переменную из таблицы или списка внутри агента. В версии 1 SNMP (SNMPv1), если управляющая станция хочет извлечь все элементы из таблицы внутри агента, она инициирует сначала операцию 'Get', а затем серию операций 'GetNext'.
- Set (Установить) — позволяет управляющей программе установить значения для объектных переменных в агенте.
- Trap (Прерывание) – используется агентом для информирования управляющей программы о произошедших событиях.

9.6.1 Поддерживаемые базы управляющей информации

P660RT2 поддерживает MIB II (Management Information Base – База управляющей информации), параметры которой описываются в комментариях RFC-1213 и RFC-1215. Базы управляющей информации позволяют сетевым администраторам собирать статистические данные и контролировать состояние и производительность сети.

9.6.2 Прерывания SNMP

P660RT2 посылает прерывания на управляющую станцию SNMP, когда происходит какое-либо из следующих событий:

Табл. 36 Прерывания SNMP

НОМЕР ПРЕРЫВАНИЯ	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
0	coldStart (описывается в *RFC-1215*)	Прерывание посылается после загрузки (при включении питания).
1	warmStart (описывается в *RFC-1215*)	Прерывание посылается после загрузки (при перезагрузке программного обеспечения).
6	whyReboot (определено в MIB ZYXEL)	Прерывание посылается вместе с причиной перезапуска перед перезагрузкой, когда система готовится к перезапуску ("горячий" запуск).

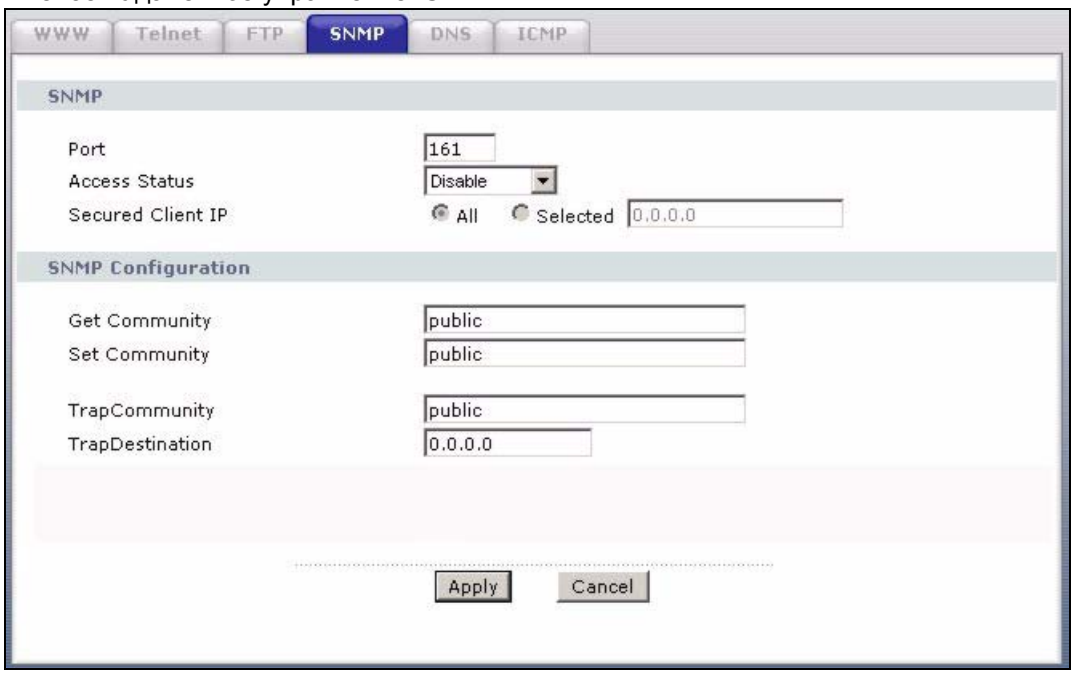
Табл. 36 Прерывания SNMP

НОМЕР ПРЕРЫВАНИЯ	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
6a	Для преднамеренной перезагрузки:	Прерывание посылается с сообщением "System reboot by user!" (перезагрузка системы пользователем), когда перезагрузка производится намеренно (например, загрузка новых файлов, команда "sys reboot" и т.д.).
6b	Для критической ошибки:	Прерывание посылается с кодом критической ошибки, если система перезагружается из-за возникновения критических ошибок.

9.6.3 Конфигурирование SNMP

Это окно используется для изменения параметров SNMP P660RT2. Щелкните «Advanced» (Дополнительно) > «Remote MGMT» (Удаленное управление) > «SNMP». При этом откроется показанное ниже окно.

Рис. 58 Удаленное управление: SNMP



В следующей таблице даны описания полей этого окна.

Табл. 37 Удаленное управление: SNMP

ПОЛЕ	ОПИСАНИЕ
SNMP	
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Статус доступа)	Выберите интерфейс(ы), через который(е) компьютер сможет получить доступ к P660RT2 при использовании этой службы.

Табл. 37 Удаленное управление: SNMP

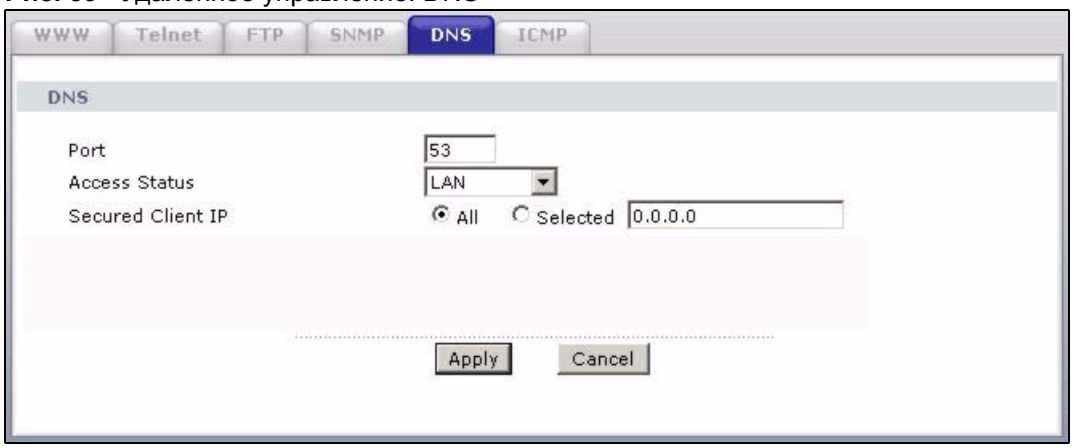
ПОЛЕ	ОПИСАНИЕ
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660RT2 при использовании этой службы. Выберите «All» (Все), чтобы разрешить любому компьютеру доступ к P660RT2 при использовании этой службы. Выберите «Selected» (Выбранный), чтобы разрешить доступ к P660RT2 только компьютеру с указанным IP-адресом при использовании этой службы.
SNMP Configuration (Настройка SNMP)	
Get Community (Пароль 'Get')	Введите пароль «Get», который является паролем для входящих запросов Get и GetNext от управляющей станции. По умолчанию установлен пароль «public» и разрешаются все запросы.
Set Community (Пароль Set)	Введите пароль «Set», который является паролем для входящих запросов Set от управляющей станции. По умолчанию установлен пароль «public» и разрешаются все запросы.
Trap (Прерывание)	
Community (Пароль)	Введите пароль 'Trap', посылаемый с каждым прерыванием на управляющую станцию SNMP. По умолчанию установлен пароль «public» и разрешаются все запросы.
Destination (получатель)	Укажите в этом поле IP-адрес станции, куда посылаются прерывания SNMP.
Apply (Применить)	Щелкните «Apply» (Применить) для сохранения сделанных настроек и выхода из этого окна.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

9.7 Настройка DNS

DNS (Система доменных имен) предназначена для отображения доменного имени на соответствующий ему IP-адрес и наоборот. Для получения дополнительной информации см. главу о локальных сетях.

Для изменения настроек DNS в P660RT2 щелкните «Advanced» (Дополнительно) > «Remote MGMT» (Удаленное управление) > «DNS». При этом откроется показанное ниже окно. Это окно используется для установки IP-адреса, с которого P660RT2 будет принимать запросы DNS, а также интерфейса, через который P660RT2 будет отправлять параметры DNS на эти запросы.

Рис. 59 Удаленное управление: DNS



В следующей таблице даны описания полей этого окна.

Табл. 38 Удаленное управление: DNS

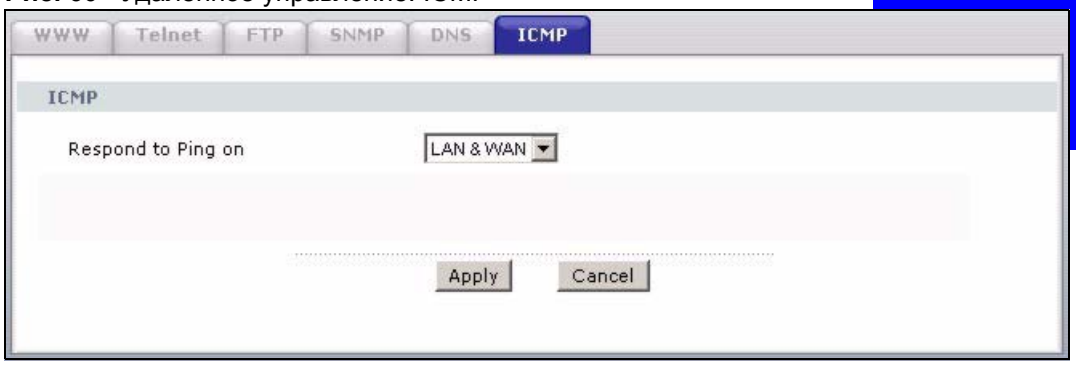
ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Номер порта службы DNS – 53.
Access Status (Статус доступа)	Выберите интерфейс(ы), через который компьютер сможет посылать P660RT2 запросы DNS.
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается посылать P660RT2 запросы DNS. Выберите «All» (Все), чтобы разрешить любому компьютеру посылать P660RT2 запросы DNS. Выберите «Selected» (Выбранный), чтобы разрешить P660RT2 посылать запросы DNS только компьютеру с указанным IP-адресом.
Apply (Применить)	Щелкните «Apply» (Применить) для сохранения сделанных настроек и выхода из этого окна.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

9.8 Настройка ICMP

Для изменения настроек безопасности в P660RT2 щелкните «Advanced» (Дополнительно) > «Remote MGMT» (Удаленное управление) > «ICMP». При этом откроется показанное ниже окно.

Если внешний пользователь попытается прозондировать неподдерживаемый порт P660RT2, ему будет автоматически отправлен ответный пакет ICMP. Это позволяет внешнему пользователю узнать о существовании модема P660RT2. Также P660RT2 поддерживает блокирование зондирования сети без отправки ответного пакета ICMP. Это позволяет скрыть существование P660RT2 от посторонних лиц при попытке эхо-тестирования неподдерживаемого порта.

Рис. 60 Удаленное управление: ICMP



В следующей таблице даны описания полей этого окна.

Табл. 39 Удаленное управление: ICMP

ПОЛЕ	ОПИСАНИЕ
ICMP	Протокол управляющих сообщений в сети Интернет (Internet Control Message Protocol) является протоколом управляющих сообщений и сообщений об ошибках между основным узлом и шлюзом в Интернет. ICMP использует дейтаграммы протокола Интернета (IP), но сообщения обрабатываются программным обеспечением TCP/IP, и невидимы для пользователей приложений.
Respond to PING on (Отвечать на PING-запросы)	Модем P660RT2 не отвечает на входящие запросы эхо-тестирования, если в поле «Disable» (Отключить) установлен флажок. Выберите «LAN» для ответа на входящие Ping-запросы из локальной сети. Выберите «WAN» для ответа на входящие Ping-запросы по глобальной сети. В противном случае выберите «LAN & WAN» для ответа на Ping-запросы как по локальной, так и глобальной сети.
Apply (Применить)	Щелкните Apply (Применить) для сохранения сделанных настроек и выхода из этого окна.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

Универсальная функция Plug and Play (UPnP)

В данной главе представлена информация о функции UPnP в Web-конфигураторе.

10.1 Описание универсальной функции Plug and Play

Универсальная функция Plug and Play (UPnP) – это распространенный открытый сетевой стандарт, использующий TCP/IP для обеспечения взаимодействия между устройствами в одноранговой сети. Устройство UPnP может динамически присоединяться к сети, получать IP-адрес, сообщать о своих функциях и собирать информацию о других устройствах сети. Также устройство может беспрепятственно и автоматически покидать сеть, если оно больше не используется.

Инструкции по настройке см. в Разд. 10.2.1 на с. 122.

10.1.1 Как узнать, используется ли UPnP?

Оборудование UPnP идентифицируется иконкой в папке «Network Connections» (Сетевые подключения) (Windows XP). Каждое совместимое с UPnP устройство, установленное в сети, появляется в виде отдельной иконки. Нажав на иконку устройства UPnP, вы получите доступ к информации и свойствам данного устройства.

10.1.2 NAT Transversal

Функция NAT Traversal с поддержкой UPnP автоматизирует процесс работы приложения через NAT. Сетевые устройства UPnP могут автоматически настраивать сетевую адресацию, объявлять о своем присутствии в сети другим устройствам UPnP и производить обмен простыми сообщениями о программных продуктах и службах. Функция NAT Traversal позволяет следующее:

- Динамическое отображение портов
- Распознавание общедоступных IP-адресов
- Назначение времени аренды для отображений

Windows Messenger является примером приложения, которое поддерживает NAT traversal и UPnP.

Для получения более подробной информации о NAT см. главу по трансляции сетевых адресов.

10.1.3 Предупреждения по использованию UPnP

Автоматический характер приложений NAT traversal при установке их собственных служб и открывании портов межсетевого экрана может привести к проблемам в отношении безопасности сети. В некоторых сетевых окружениях пользователи могут получить доступ к сетевой информации и конфигурации, а также к ее изменению.

Когда устройство UPnP подключается к сети, оно объявляет о своем присутствии с помощью многоадресной рассылки сообщения. В целях повышения безопасности P660RT2 разрешает многоадресную рассылку сообщений только по локальной сети.

Все устройства с включенной функцией UPnP могут свободно взаимодействовать друг с другом без дополнительной настройки. Отключите функцию UPnP, если ее не предпалагается использовать.

10.2 UPnP и ZyXEL

Корпорация ZyXEL получила сертификат от организации Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). Реализация UPnP корпорации ZyXEL поддерживает IGD 1.0 (Internet Gateway Device – Устройство Интернет-шлюза).

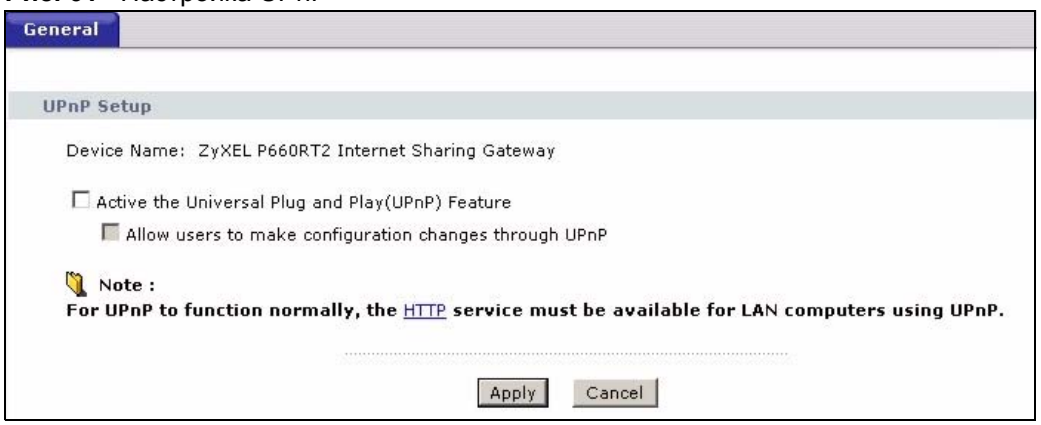
Примеры установки и использования UPnP см. в следующих разделах.

10.2.1 Настройка UPnP

Щелкните «Advanced» (Дополнительно) > «UPnP» для отображения окна, как показанного ниже. Это окно используется для настройки параметров функции Plug-and-Play P660RT2.

Более подробную информацию см. в Разд. 10.1 на с. 121.

Рис. 61 Настройка UPnP



В следующей таблице даны описания полей этого окна.

Табл. 40 Настройка UPnP

ПОЛЕ	ОПИСАНИЕ
Active the Universal Plug and Play (UPnP) Feature (Включить функцию UPnP)	Установите флажок для включения UPnP. Помните, что любой может с помощью приложения UPnP открыть окно регистрации Web-конфигуратора без ввода IP-адреса модема P660RT2 (хотя для доступа к Web-конфигуратору необходимо ввести пароль).
Allow users to make configuration changes through UPnP (Разрешить пользователям вносить изменения в конфигурацию через UPnP)	Установите здесь флажок, чтобы разрешить приложениям с включенной функцией UPnP автоматически выполнять настройку P660RT2 для того, чтобы они могли взаимодействовать через P660RT2. Например, с помощью обхода NAT приложения UPnP автоматически резервируют порт переадресации NAT, чтобы взаимодействовать с другим устройством UPnP. Это устраняет необходимость ручной настройки переадресации портов для приложений UPnP.
Apply (Применить)	Щелкните «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить) для возврата к предыдущим сохраненным настройкам.

10.3 Пример установки UPnP в Windows

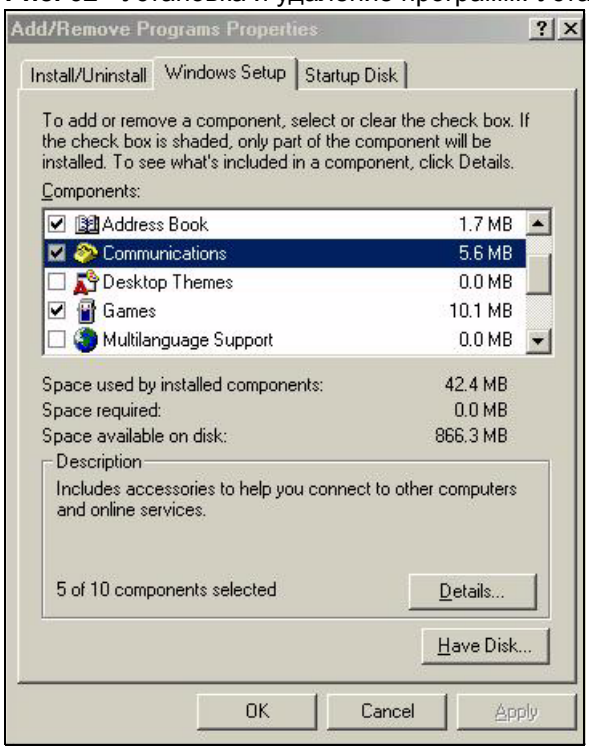
В данном разделе описывается установка UPnP в Windows Me и Windows XP.

10.3.1 Установка UPnP в Windows Me

Выполните следующие действия для установки UPnP в Windows Me.

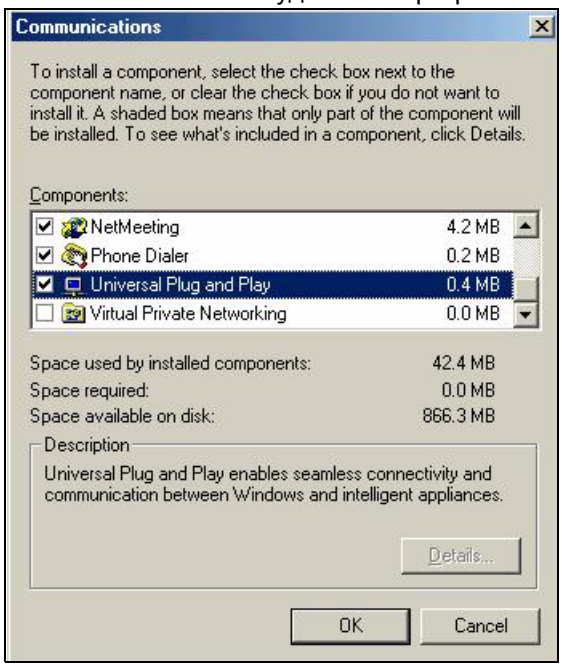
1. Нажмите «Start» (Пуск), «Control Panel» (Панель управления). Дважды щелкните «Add/Remove Programs» (Установка и удаление программ).
2. Щелкните по закладке «Windows Setup» (Установка Windows) и выберите «Communication» (Связь) в поле «Components» (Компоненты). Щелкните «Details» (Состав).

Рис. 62 Установка и удаление программ: Установка Windows: Связь



3 В окне «Communications» (Связь) в поле «Components» (Компоненты) установите флажок «Universal Plug and Play».

Рис. 63 Установка и удаление программ: Установка Windows: Связь: Компоненты



4 Нажмите «OK» для возврата в окно «Add/Remove Programs Properties» (Свойства: Установка и удаление программ) и нажмите «Next» (Далее).

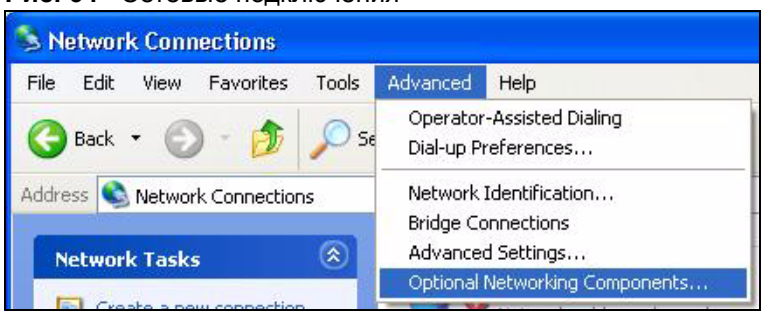
5 При появлении запроса перезагрузите компьютер.

10.3.2 Установка UPnP в Windows XP

Выполните следующие действия для установки UPnP в Windows XP.

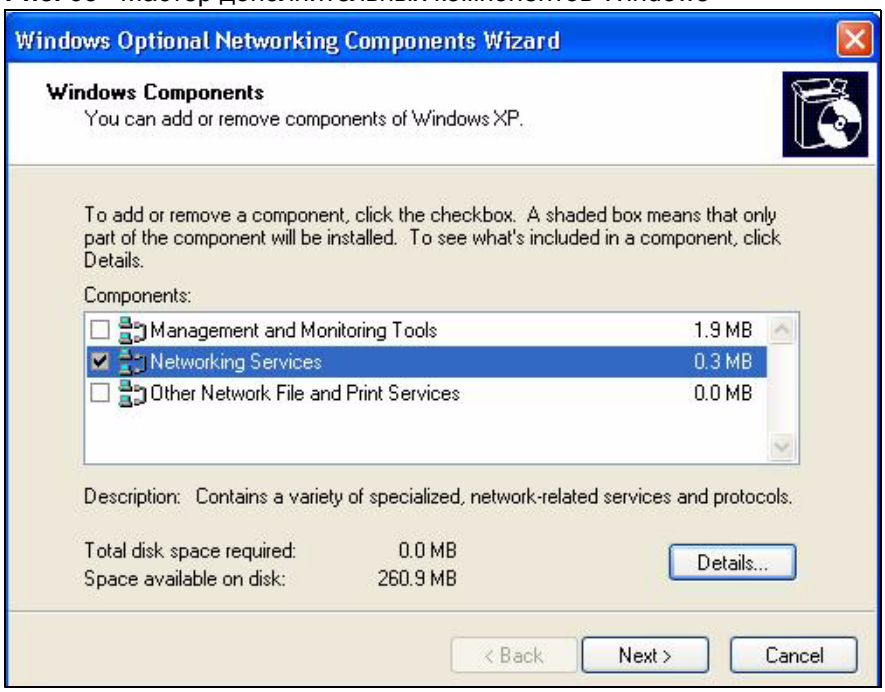
1. Щелкните «Start» (Пуск), «Control Panel» (Панель управления).
2. Дважды щелкните по иконке «Network Connections» (Сетевые подключения).
3. В окне «Network Connections» (Сетевые подключения) нажмите кнопку «Advanced» (Дополнительно) в главном меню и выберите «Optional Networking Components…» (Дополнительные сетевые компоненты...).

Рис. 64 Сетевые подключения



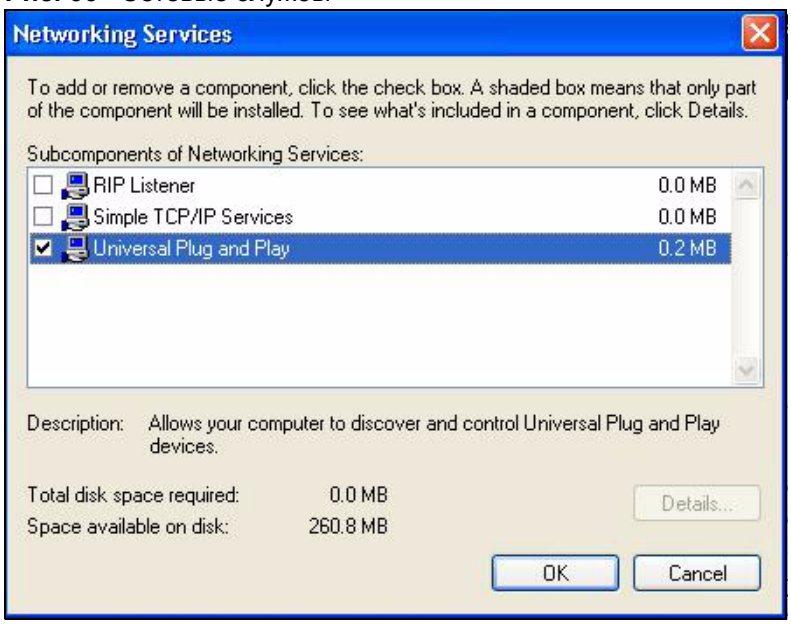
4. Появится окно «Windows Optional Networking Components Wizard» (Мастер дополнительных сетевых компонентов Windows). Выберите «Networking Services» (Сетевые службы) в поле «Components» (Компоненты) и нажмите «Details» (Состав).

Рис. 65 Мастер дополнительных компонентов Windows



5. В окне «Networking Services» (Сетевые службы) поставьте флажок «Universal Plug and Play».

Рис. 66 Сетевые службы



6 Щелкните «OK» для возврата в окно «Windows Optional Networking Component Wizard» (Мастер дополнительных сетевых компонентов Windows) и нажмите «Next» (Далее).

10.4 Пример использования UPnP в Windows XP

В этом разделе описывается использование функции UPnP в Windows XP. Функция UPnP уже должна быть установлена в Windows XP и включена в модеме P660RT2.

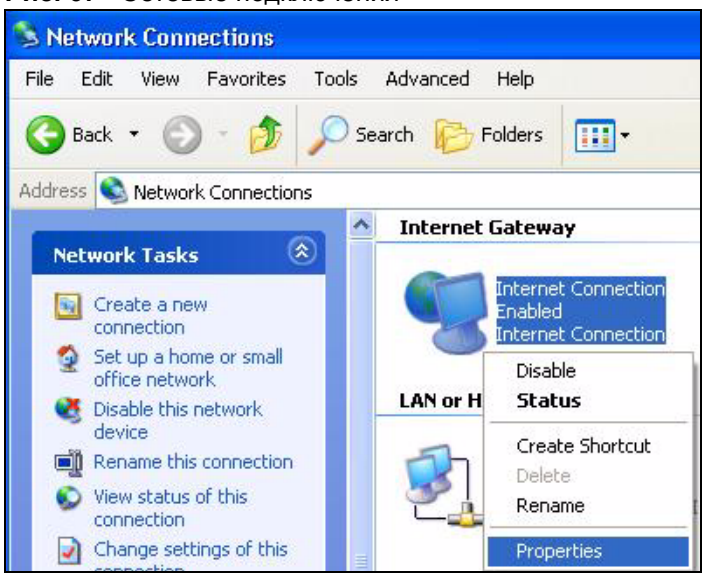
Убедитесь, что компьютер подключен к порту LAN модема P660RT2. Включите компьютер и P660RT2.

10.4.1 Автоматическое обнаружение сетевого устройства UPnP

1 Щелкните «Start» (Пуск), «Control Panel» (Панель управления). Дважды щелкните по иконке «Network Connections» (Сетевые подключения). В разделе «Internet Gateway» (Шлюз Интернет) появится иконка.

2 Щелкните правой кнопкой мыши по этой иконке и выберите «Properties» (Свойства).

Рис. 67 Сетевые подключения



3 В окне «Internet Connection Properties» (Свойства подключения к Интернет), нажмите «Settings» (Настройки) для просмотра автоматически созданных правил отображения портов.

Рис. 68 Свойства подключения к Интернет

4 Вы можете редактировать или удалять правила отображения портов, или щелкнуть по кнопке «Add» (Добавить), чтобы вручную добавить правило отображения портов.

Рис. 69 Свойства подключения к Интернет: Дополнительные настройки

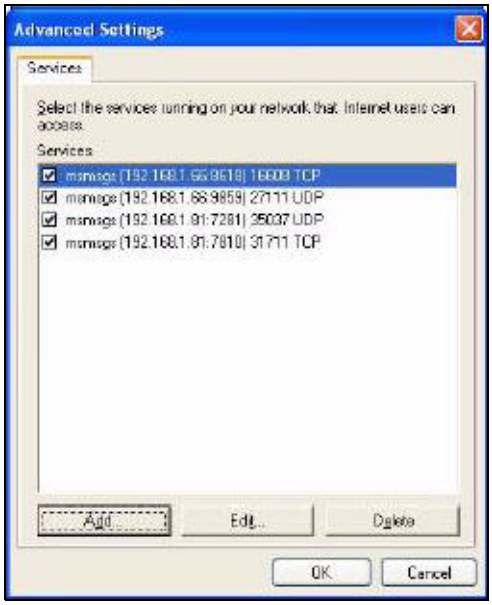
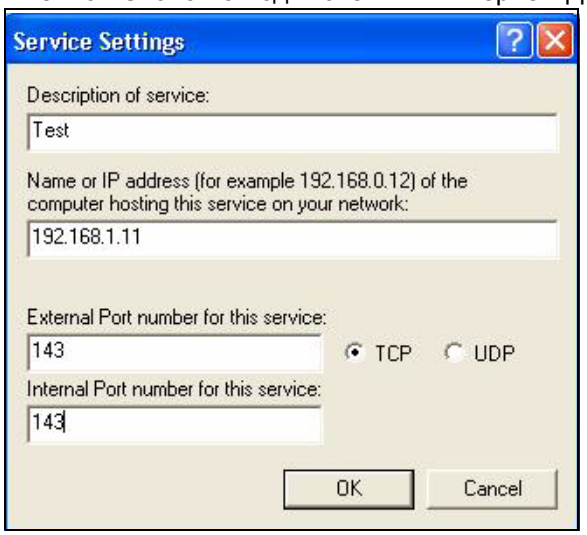


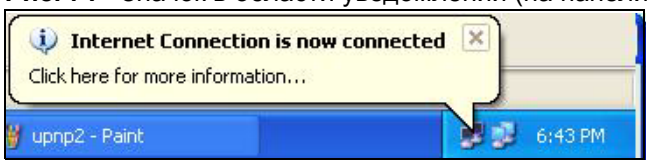
Рис. 70 Свойства подключения к Интернет: Дополнительные настройки: Добавить



При отключении устройства UPnP от компьютера все правила отображения портов автоматически удаляются.

5 Выберите «Show icon in notification area when connected» (При подключении вывести значок в области уведомлений) и нажмите «OK». На панели задач отображается значок.

Рис. 71 Значок в области уведомлений (на панели задач)



6 Дважды щелкните иконку для отображения текущего состояния подключения к Интернету.

Рис. 72 Состояние подключения к Интернет

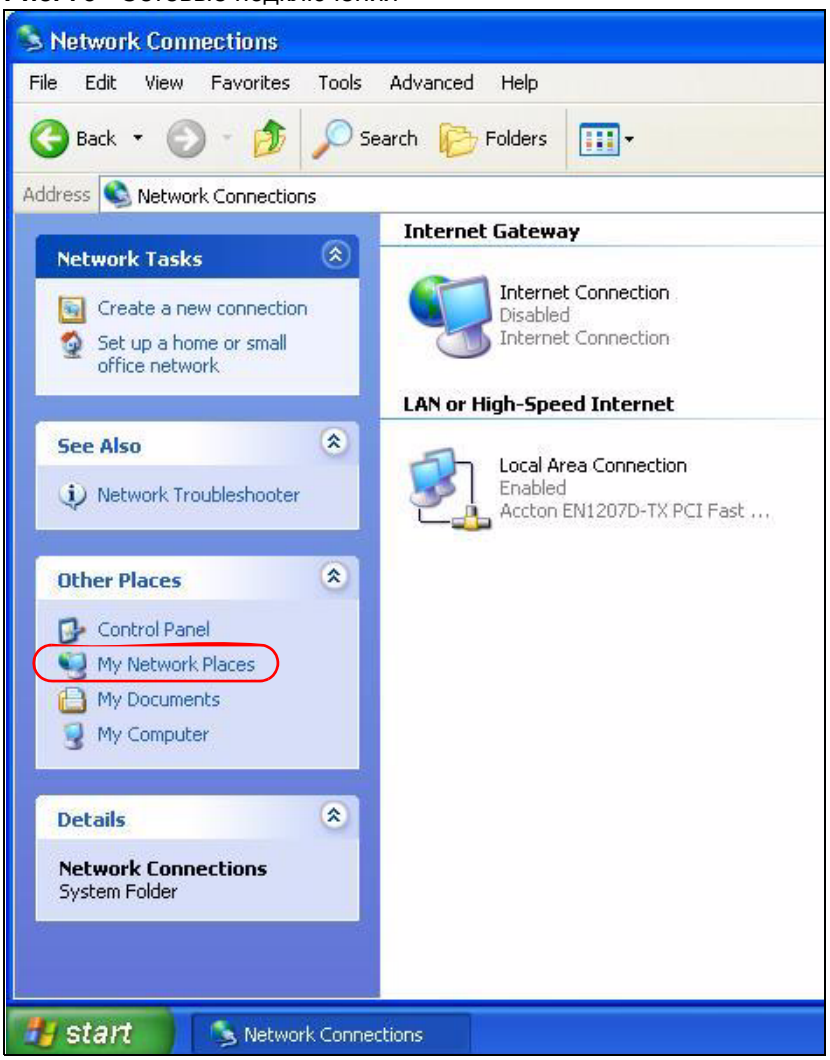
10.4.2 Простой доступ к Web-конфигуратору

С помощью UPnP вы можете получить доступ к программе настройки P660RT2 на основе Web технологии без предварительного выяснения IP-адреса P660RT2. Это может оказаться полезным, если вы не знаете IP-адрес P660RT2.

Выполните следующие действия для доступа к Web-конфигуратору.

1 Нажмите «Start» (Пуск), «Control Panel» (Панель управления).
2 Дважды щелкните по иконке «Network Connections» (Сетевые подключения).
3 Выберите «My Network Places» (Сетевое окружение) в разделе «Other Places» (Другие места).

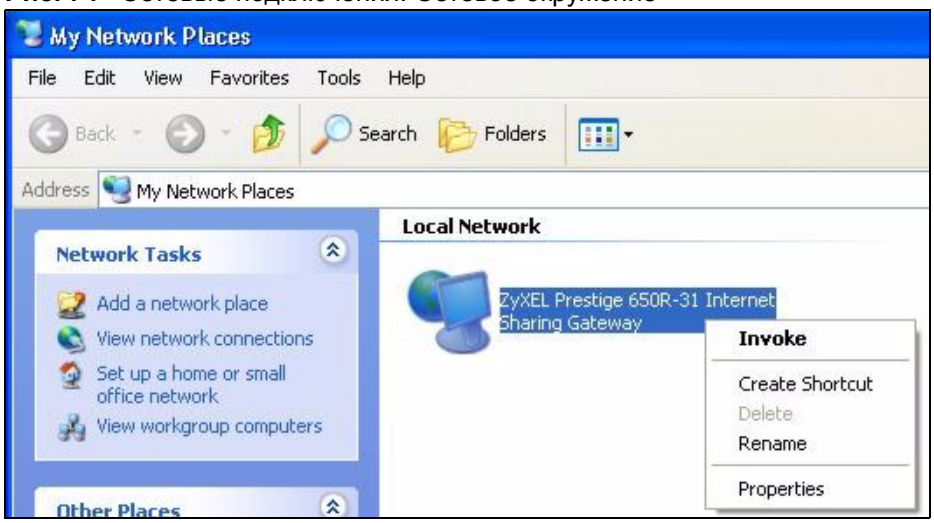
Рис. 73 Сетевые подключения



4 В разделе «Local Network» (Локальная сеть) для каждого устройства с включенной функцией UPnP отображается иконка с описанием.

5 Щелкните правой кнопкой мыши на иконке P660RT2 и выберите «Invoke» (Запустить). Появляется окно регистрации Web-конфигуратора.

Рис. 74 Сетевые подключения: Сетевое окружение



6 Щелкните правой кнопкой мыши на иконке P660RT2 и выберите «Properties» (Свойства). Появится окно свойств с основной информацией об устройстве P660RT2.

Рис. 75 Пример – Сетевые подключения: Сетевое окружение: Свойства

Часть III
Служебные программы и поиск/устранение неисправностей

Система(135)
Программные средства(141)
Диагностика(147)
Поиск и устранение неисправностей(149)

11

Система

Это окно используется для установки времени и даты в модеме P660RT2.

11.1 Настройка общих параметров

11.1.1 Настройка общих параметров и ввод системного имени

Окно «General Setup» (Общие параметры) содержит административную и общесистемную информацию. **Системное имя** используется для идентификации. Однако, поскольку некоторые Интернет-провайдеры проверяют это имя, следует вводить имя вашего компьютера.

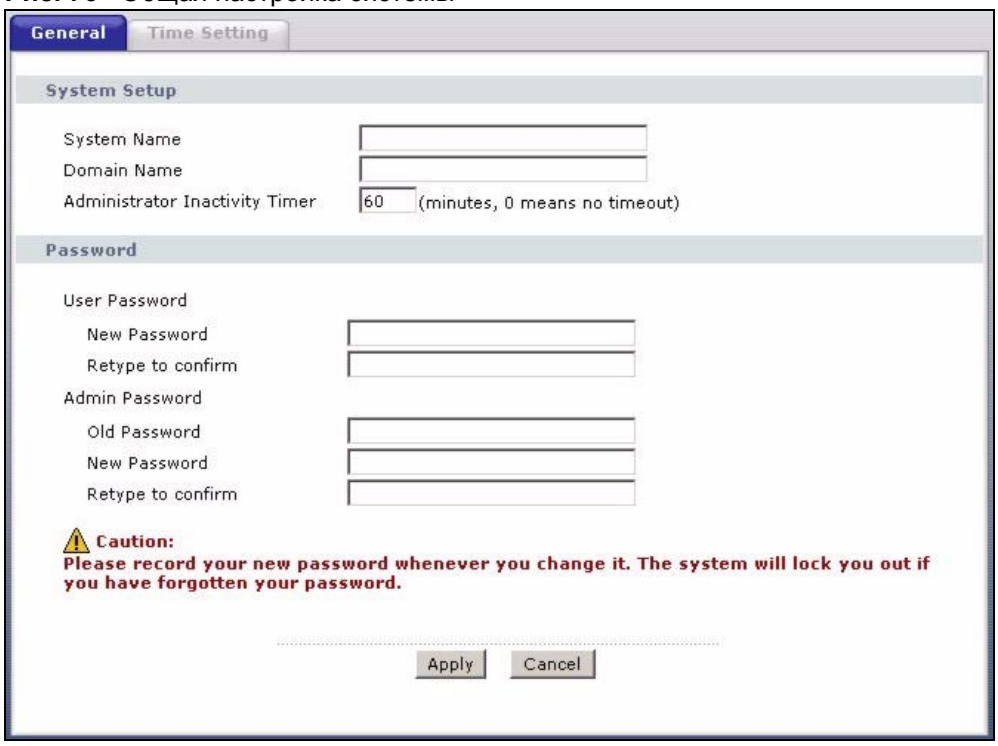
- В Windows 95/98 нажмите кнопку «Start» (Пуск), «Settings» (Настройка), «Control Panel» (Панель управления), «Network» (Сеть и удаленный доступ к сети). Щелкните по закладке «Identification» (Идентификация), запишите имя, установленное в поле «Computer Name» (Имя компьютера), и введите его в качестве системного имени.
- В Windows 2000 нажмите кнопку «Start» (Пуск), «Settings» (Настройка), «Control Panel» (Панель управления) и дважды щелкните «System» (Система). Выберите закладку «Network Identification» (Сетевая идентификация), а затем нажмите кнопку «Properties» (Свойства). Запишите имя, установленное в поле «Computer name» (Имя компьютера), и введите его в качестве системного имени.
- В Windows XP нажмите кнопку «Start» (Пуск), «My Computer» (Мой компьютер), «View system information» (Просмотр сведений о системе), а затем выберите закладку «Computer Name» (Имя компьютера). Запишите имя, установленное в поле «Full Computer Name» (Полное имя компьютера), и введите его в качестве системного имени P660RT2.

11.1.2 Настройка общих параметров

Запись «Domain Name» (Доменное имя) передается клиентам DHCP в локальной сети. Если оставить это поле пустым, будет использоваться доменное имя, полученное протоколом DHCP от Интернет-провайдера. В отличие от имени узла (системное имя), которое вы должны вводить на каждом отдельном компьютере, доменное имя может назначаться модемом P660RT2 с помощью DHCP.

Щелкните «Maintenance» (Сопровождение) > «System» (Система) для отображения окна «General» (Общие параметры).

Рис. 76 Общая настройка системы



В следующей таблице даны описания полей этого окна.

Табл. 41 Общая настройка системы

ПОЛЕ	ОПИСАНИЕ
General Setup (Настройка общих параметров)	
System Name (Системное имя)	Выбрать для системы идентифицирующее имя. В это поле рекомендуется ввести имя вашего компьютера «Computer name». Имя может включать до 30 алфавитно-цифровых символов. Пробелы внутри имени не допускаются. Допускаются тире "-" и знак подчеркивания "_".
Domain Name (Имя домена)	Введите в это поле доменное имя (если оно известно). Если это поле оставлено пустым, Интернет-провайдер может назначить доменное имя с помощью DHCP. Введенное доменное имя обладает более высоким приоритетом, чем доменное имя, назначенное Интернет-провайдером.
Administrator Inactivity Timer (Таймер простоя сеанса администрирования)	Введите время простоя в минутах, по истечении которого сеанс управления будет завершен. Значение по умолчанию 5 минут. Чтобы подключиться после завершения сеанса, необходимо снова зарегистрироваться и ввести пароль. Очень долгое время простоя увеличивает риск нарушения безопасности сети. Значение 0 означает, что сеанс управления не разрывается, независимо от времени простоя (не рекомендуется).
Password (Пароль)	
User Password (Пароль пользователя)	При регистрации с паролем пользователя можно выполнять только просмотр статуса P660RT2. По умолчанию установлен пароль **user**.

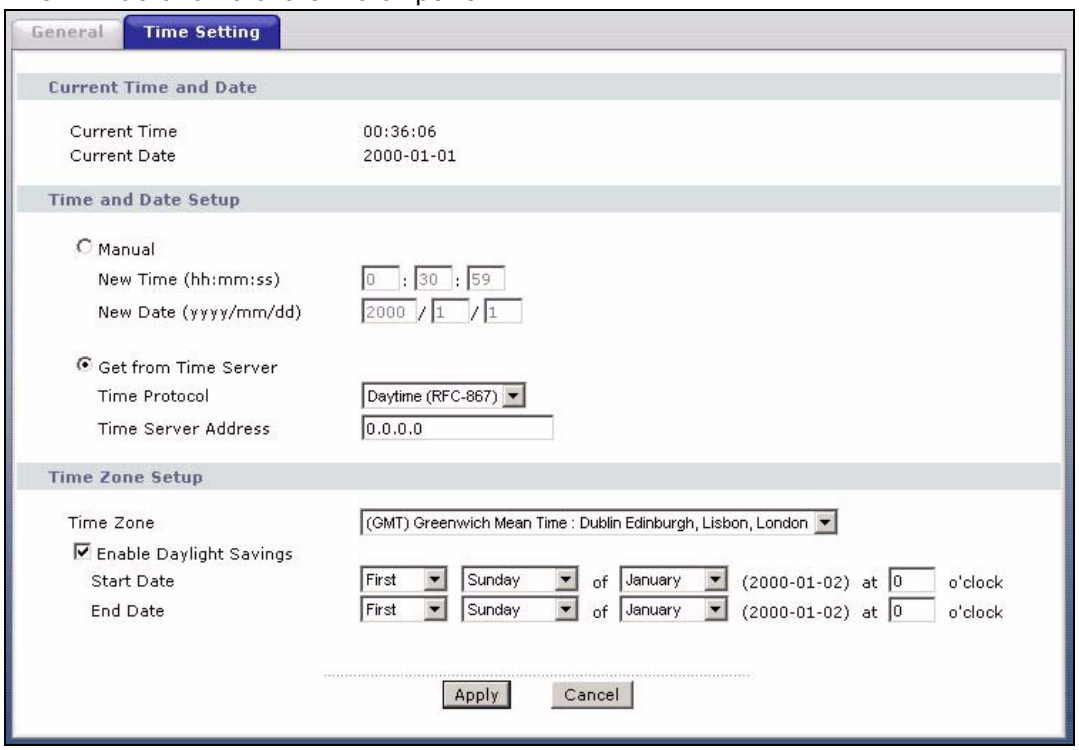
Табл. 41 Общая настройка системы

ПОЛЕ	ОПИСАНИЕ
New Password (новый пароль)	Введите новый пароль пользователя длиной до 30 символов. При вводе пароля вводимые символы заменяются на экране на символ *. После изменения пароля для доступа к P660RT2 необходимо использовать новый пароль.
Retype to Confirm (Повторный ввод для подтверждения)	Введите новый пароль еще раз для подтверждения.
Admin Password (Пароль администратора)	При регистрации с паролем администратора, кроме выполнения настроек с помощью Мастера, также можно выполнять настройку расширенных возможностей P660RT2.
Old Password (Старый пароль)	Введите пароль администратора по умолчанию (**1234**) или существующий пароль, который используется для доступа к системе при настройке расширенных возможностей.
New Password (новый пароль)	Введите новый пароль администратора длиной до 30 символов. При вводе пароля вводимые символы заменяются на экране на символ *. После изменения пароля для доступа к P660RT2 необходимо использовать новый пароль.
Retype to Confirm (Повторный ввод для подтверждения)	Введите новый пароль еще раз для подтверждения.
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

11.2 Установка времени

Для изменения даты и времени в P660RT2 нажмите кнопку «Maintenance» (Сопровождение) > «System» (Система) > «Time Setting» (Установка времени). При этом откроется показанное ниже окно. Это окно используется для установки времени в модеме P660RT2 в соответствии с вашим часовым поясом.

Рис. 77 Установка системного времени



В следующей таблице даны описания полей этого окна.

Табл. 42 Установка системного времени

ПОЛЕ	ОПИСАНИЕ
Current Time and Date (Текущее время и дата)	
Current Time (Текущее время)	В этом поле отображается время, установленное в модеме P660RT2. При каждой загрузке этой страницы модем P660RT2 синхронизирует время с сервером времени.
Current Date (Текущая дата)	В этом поле отображается дата в модеме P660RT2. При каждой загрузке этой страницы модем P660RT2 синхронизирует дату с сервером времени.
Time and Date Setup (Установка времени и даты)	
Manual (Вручную)	Выберите эту опцию для установки времени и даты вручную. При одновременной установке новых параметров даты и времени, часового пояса и перехода на летнее время, новые дата и время имеют приоритет, и параметры «Time Zone» (Часовой пояс) и «Daylight Saving» (Переход на летнее время) не влияют на них.

Табл. 42 Установка системного времени (продолжение)

ПОЛЕ	ОПИСАНИЕ
New Time (Новое время) (чч:мм:сс)	В этом поле отображается время, последний раз обновленное с помощью сервера времени или последний раз установленное вручную. При выборе в разделе «Time and Date Setup» (Установка времени и даты) режима «Manual» (Ручной) введите в это поле новое время и нажмите кнопку «Apply» (Применить).
New Date (Новая дата) (гггг/мм/дд)	В этом поле отображается дата, последний раз обновленная с помощью сервера времени или последний раз установленная вручную. При выборе в разделе «Time and Date Setup» (Установка времени и даты) режима «Manual» (Ручной), введите в это поле новую дату и нажмите кнопку «Apply» (Применить).
Get from Time Server (Получить от сервера времени)	Выберите эту опцию, чтобы P660RT2 синхронизировал время и дату с сервером, указанным в поле ниже.
Time Protocol (Протокол времени)	Выберите сервисный протокол, который используется сервером времени. Не все серверы времени поддерживают все протоколы, поэтому следует проконсультироваться с Интернет-провайдером или сетевым администратором, или попытаться определить работающий протокол методом проб и ошибок. Основные различия между ними заключаются в формате представления времени. Формат **Daytime (RFC 867)**- это день/месяц/год/часовой пояс сервера. Формат **Time (RFC 868)** представляет собой 4-байтовое целое число, означающее общее количество секунд, истекшее с 00:00:00, 01.01.1970. По умолчанию формат «NTP (RFC 1305)» аналогичен формату «Time (RFC 868)».
Time Server Address (Адрес сервера времени)	Введите IP-адрес или URL сервера времени длиной до 20 символов расширенного набора ASCII. Если нет уверенности в имеющейся информации, следует обратиться к Интернет-провайдеру или сетевому администратору.
Time Zone Setup (Установка часового пояса)	
Time Zone (Часовой пояс)	Выберите часовой пояс вашего местонахождения. Это поле устанавливает разницу между вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time – GMT).
Enable Daylight Savings (Включить переход на летнее время)	Летнее время — это период с поздней весны до ранней осени, когда во многих странах стрелки часов переводятся на час вперед, чтобы добавить час светлого времени суток. Установите флажок, если вы используете переход на летнее время.

Табл. 42 Установка системного времени (продолжение)

ПОЛЕ	ОПИСАНИЕ
Start Date (Дата начала)	Введите месяц и день, когда начинается летнее время, если выбран вариант «Daylight Savings» (Переход на летнее время). В поле «o'clock» (час.) используется 24 часовой формат. Далее приводится два примера: В большинстве частей Соединенных Штатов переход на летнее время начинается в первое воскресенье апреля. В каждой временной зоне Соединенных Штатов переход осуществляется в 2 часа ночи по местному времени. Таким образом, в Соединенных Штатах необходимо установить «First» (Первое), «Sunday» (Воскресенье), «April» (Апрель) и 2 в поле «o'clock» (часы). В странах Европейского Союза переход на летнее время начинается в последнее воскресенье марта. Во всех временных зонах Европейского Союза переход осуществляется в одно время – в 1 час ночи по Гринвичскому меридиану или универсальному скоординированному времени. Таким образом, в странах Европейского союза необходимо установить «Last» (Последнее), «Sunday» (Воскресенье), March (Март). Время, которое нужно ввести в поле «o'clock» (час.) зависит от вашей временной зоны. Например, в Германии необходимо установить 2, так как временная зона Германии находится на 1 час впереди зоны GMT или UTC (GMT+1).
End Date (Конечная дата)	Введите месяц и день, когда заканчивается летнее время, если выбран вариант «Enable Daylight Saving» (Включить переход на летнее время). В поле «o'clock» (час.) используется 24-часовой формат. Далее приводится два примера: В Соединенных Штатах летнее время заканчивается в последнее воскресенье октября. В каждой временной зоне Соединенных Штатов переход осуществляется в 2 часа ночи по местному времени. Таким образом, в Соединенных Штатах необходимо установить «Last» (Последнее), «Sunday» (Воскресенье), «October» (Октябрь) и 2 в поле «o'clock» (час.). В странах Европейского Союза летнее время заканчивается в последнее воскресенье октября. Во всех временных зонах Европейского Союза обратный переход осуществляется в одно время – в 1 час ночи по Гринвичскому меридиану или универсальному скоординированному времени. Таким образом, в странах Европейского Союза необходимо установить «Last» (Последнее), «Sunday» (Воскресенье), «October» (Октябрь). Время, которое нужно ввести в поле «o'clock» (час.) зависит от вашей временной зоны. Например, в Германии необходимо установить 2, так как временная зона Германии находится на 1 час впереди зоны GMT или UTC (GMT+1).
Apply (Применить)	Щелкните по кнопке «Apply» (Применить) для сохранения настроек P660RT2.
Cancel (Отменить)	Нажмите кнопку «Cancel» (Отменить), чтобы снова начать настройку в этом окне.

12

Программные средства

В этой главе рассказывается о загрузке новой микропрограммы, управлении конфигурацией и перезагрузке модема P660RT2.

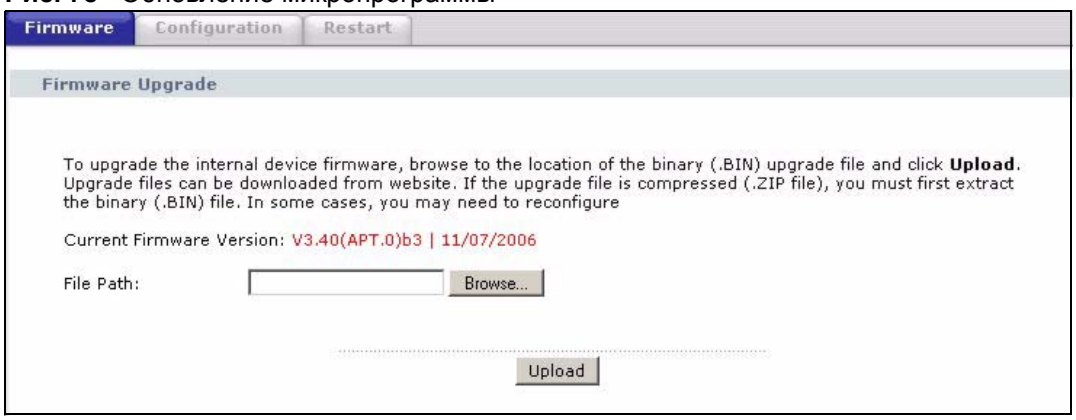
12.1 Обновление микропрограммы

Найдите программное обеспечение на сайте www.zyxel.ru в файле, в названии которого обычно используется название модели с расширением .bin, например, «P660RT2.bin». Для загрузки используется протокол HTTP (Hypertext Transfer Protocol – Протокол передачи гипертекста), загрузка может занять до 2-х минут времени. После успешной загрузки микропрограммы система перезапускается.

Необходимо использовать микропрограмму строго в соответствии с конкретной моделью устройства. См. наклейку на нижней панели устройства.

Щелкните «Maintenance» (Сопровождение) > «Tools» (Программные средства) для отображения окна «Firmware» (Микропрограмма). Следуйте указаниям в этом окне для загрузки микропрограммы в модем P660RT2.

Рис. 78 Обновление микропрограммы



В следующей таблице даны описания полей этого окна.

Табл. 43 Обновление микропрограммы

ПОЛЕ	ОПИСАНИЕ
Current Firmware Version (Текущая версия микропрограммы)	Здесь отображается текущая версия и дата создания микропрограммы.
File Path (Путь к файлу)	Введите путь к файлу, который вы хотите загрузить, или нажмите кнопку «Browse...» (Обзор...), чтобы указать местонахождение файла.
Browse... (Обзор...)	Щелкните по кнопке «Browse...» (Обзор...), чтобы указать местонахождение файла с расширением .bin, который требуется загрузить. Архивированные файлы (.zip) необходимо распаковать, прежде чем выполнять загрузку.
Upload (Загрузить)	Нажмите кнопку «Upload» (Загрузить) для запуска процесса загрузки. Процесс загрузки может занять до 2 минут.

НЕЛЬЗЯ выключать питание P660RT2 во время загрузки микропрограммы!

После появления окна «Firmware Upload in Progress» (Выполняется загрузка микропрограммы), подождите 2 минуты, прежде чем снова входить в программу P660RT2.

Рис. 79 Выполняется загрузка микропрограммы

P660RT2 автоматически перезапускается, что вызывает временное отключение устройства от сети. В некоторых операционных системах может появиться следующая иконка на рабочем столе.

Рис. 80 Временное отключение сети

По истечении 2 минут, снова подключитесь к модему и проверьте версию новой микропрограммы в окне «System Status» (Состояние системы).

Если загрузку не удалось завершить успешно, появляется следующее окно. Нажмите кнопку «Return» (Возврат) для возврата к окну «Firmware» (Микропрограмма).

Рис. 81 Сообщение об ошибке

12.2 Окно конфигурации

Щелкните «Maintenance» (Сопровождение) > «Tools» (Программные средства) > «Configuration» (Конфигурация). В этом окне отображается информация о заводских настройках по умолчанию, резервном сохранении и восстановлении конфигурации.

Рис. 82 Configuration (Конфигурация)

12.2.1 Резервное сохранение конфигурации

Резервное сохранение конфигурации позволяет сохранить текущую конфигурацию P660RT2 в файле на компьютере. Если настройка P660RT2 выполнена, и устройство работает нормально, то перед внесением каких-либо изменений настоятельно рекомендуется создать резервную копию файла конфигурации. Файл с резервной копией конфигурации пригодится в случае, если Вам придется вернуться к предыдущим настройкам.

Для сохранения текущей конфигурации P660RT2 на компьютере щелкните «Backup» (Резервное сохранение).

12.2.2 Восстановление конфигурации

Функция восстановления конфигурации позволяет загрузить с компьютера в P660RT2 новый или предварительно сохраненный файл конфигурации.

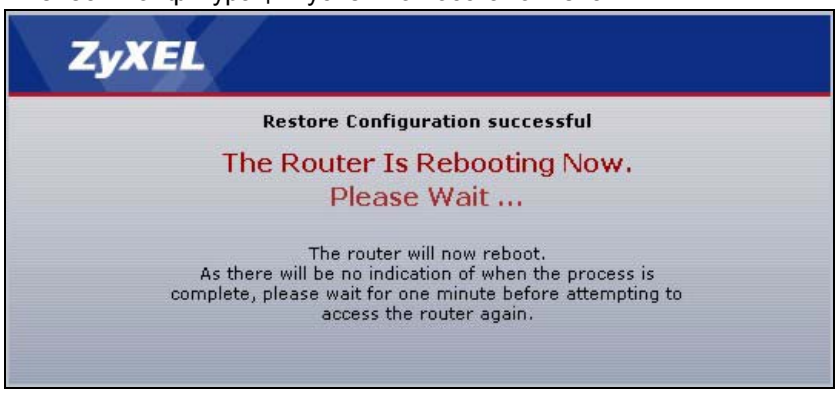
Табл. 44 Сопровождение: Восстановление конфигурации

ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите в этом поле путь к файлу, который Вы хотите загрузить или нажмите **Browse** ..., чтобы найти его.
Browse... (Обзор...)	Нажмите «Browse...» (Обзор...), чтобы найти файл для загрузки. Не забудьте распаковать сжатые файлы (.ZIP), прежде чем загружать их.
Upload (Загрузить)	Нажмите кнопку «Upload» (Загрузить) для запуска процесса загрузки.

НЕЛЬЗЯ выключать питание P660RT2 во время загрузки файла конфигурации!

После появления окна «Restore Configuration successful» (Конфигурация успешно восстановлена), необходимо подождать одну минуту, прежде чем снова регистрироваться в P660RT2.

Рис. 83 Конфигурация успешно восстановлена



P660RT2 автоматически перезапускается, что вызывает временное отключение устройства от сети. В некоторых операционных системах может появиться следующая иконка на рабочем столе.

Рис. 84 Временное отключение сети

При загрузке файла конфигурации по умолчанию необходимо изменить IP-адрес компьютера, чтобы он находился в той же подсети, что и IP-адрес P660RT2 по умолчанию (192.168.1.1). Подробнее об установке IP-адреса компьютера см. в соответствующем приложении.

Если загрузку не удалось завершить успешно, появляется следующее окно. Нажмите кнопку «Return» (Возврат) для возврата к окну «Configuration» (Конфигурация).

Рис. 85 Ошибка восстановления конфигурации

12.2.3 Восстановление заводских настроек по умолчанию

При нажатии кнопки «RESET» (Сброс) в этом разделе сбрасываются все измененные пользователем параметры, и настройки P660RT2 возвращаются к заводским настройкам по умолчанию.

Возвращение настроек P660RT2 к заводским настройкам по умолчанию также можно выполнить, нажав кнопку «RESET» (Сброс) на задней панели устройства. Дополнительную информацию о кнопке «RESET» (Сброс) см. в главе описания Web-конфигуратора.

12.3 Перезапуск

Это окно позволяет выполнить перезагрузку P660RT2 без выключения электропитания.

Щелкните «Maintenance» (Сопровождение) > «Tools» (Программные средства) > «Restart» (Перезапуск). Щелкните по кнопке «Restart» (Перезапуск) P660RT2 для перезагрузки. Эта операция не влияет на конфигурацию P660RT2.

Рис. 86 Окно перезапуска

13

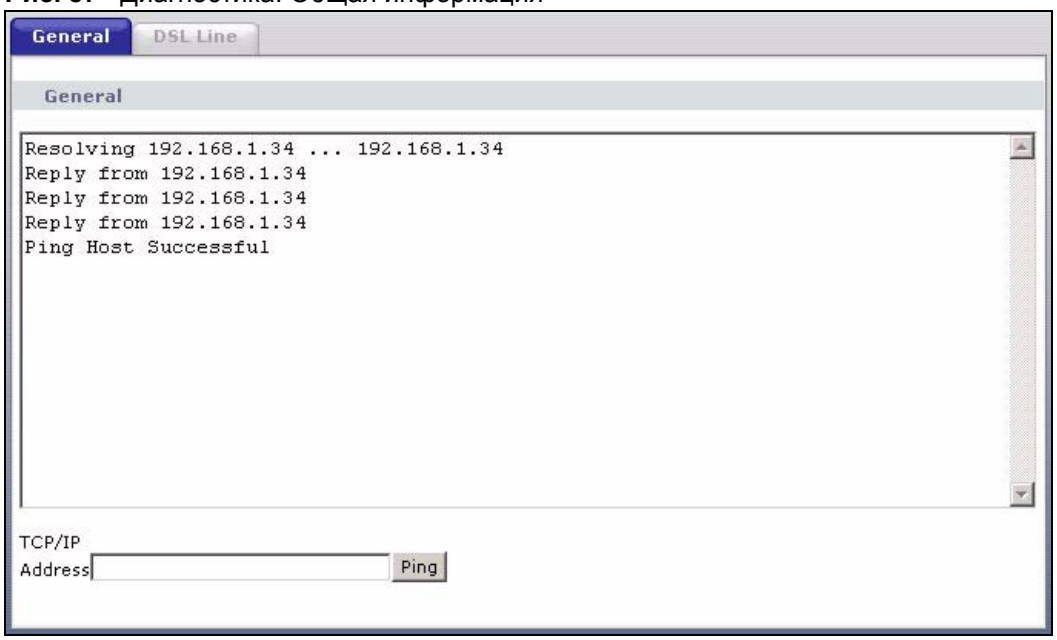
Диагностика

Информация в этих окнах представлена в режиме только для чтения и предназначена, чтобы помочь определить неисправность P660RT2.

13.1 Общая диагностика

Щелкните «Maintenance» (Сопровождение) > «Diagnostic» (Диагностика) для отображения окна, показанного ниже.

Рис. 87 Диагностика: Общая информация



В следующей таблице даны описания полей этого окна.

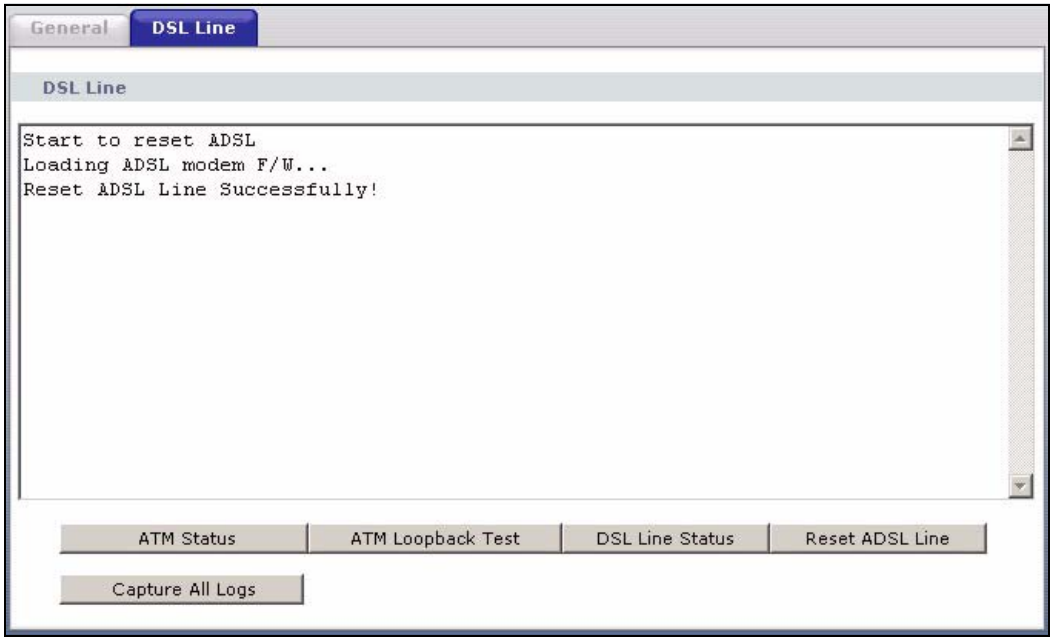
Табл. 45 Диагностика: Общая информация

ПОЛЕ	ОПИСАНИЕ
TCP/IP Address (Адрес TCP/IP)	Введите IP-адрес компьютера, который необходимо протестировать с помощью команды "ping", чтобы проверить соединение.
Ping (Эхо-тестирование)	Щелкните по этой кнопке для тестирования устройства с введенным IP-адресом с помощью команды «ping».

13.2 Диагностика линии DSL

Щелкните «Maintenance» (Сопровождение) > «Diagnostic» (Диагностика) > «DSL Line» (Линия DSL) для отображения окна, показанного ниже.

Рис. 88 Диагностика: Линия DSL



В следующей таблице даны описания полей этого окна.

Табл. 46 Диагностика: Линия DSL

ПОЛЕ	ОПИСАНИЕ
ATM Status (Состояние ATM)	Щелкните по этой кнопке для просмотра статуса ATM.
ATM Loopback Test (Тест петля ATM)	Щелкните по этой кнопке для запуска теста петля ATM. Прежде чем начать выполнение теста, убедитесь, что вы настроили хотя бы один канал PVC с соответствующими VPI/VCI. P660RT2 посылает пакет OAM F5 на коммутатор DSLAM/ATM, после чего он возвращается обратно в P660RT2. Тест петля ATM используется для поиска и устранения неисправностей в сети с DSLAM и ATM.
DSL Line Status (Статус линии DSL)	Щелкните по этой кнопке для просмотра линейных рабочих величин и линейного побитового распределения порта DSL.
Reset ADSL Line (Сброс линии ADSL)	Нажмите эту кнопку, чтобы заново инициализировать ADSL линию. Тогда в большом текстовом поле сверху будет отображаться прохождение и результаты этой операции, например: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
Capture All Logs (Показать все регистрационные записи)	Щелкните по этой кнопке для отображения всех регистрационных записей, сгенерированных линией DSL.

14

Поиск и устранение неисправностей

В этой главе рассказывается об устранении возмозможных неисправностей, которые могут появиться при работе с модемом. Возможные неисправности можно разделить на следующие категории:

- Питание, подключение оборудования и светодиоды
- Доступ и регистрация в P660RT2
- Доступ в Интернет

14.1 Питание, подключение оборудования и светодиоды

? Модем P660RT2 не включается. Ни один из светодиодов не включается.

1. Убедитесь, что P660RT2 включен.
2. Убедитесь, что используется адаптер или кабель питания из комплекта поставки P660RT2.
3. Убедитесь, что адаптер или кабель питания подключен к P660RT2 и к соответствующему источнику питания. Убедитесь, что источник питания включен.
4. Выключите и снова включите P660RT2.
5. Если неисправность не устраняется, свяжитесь с поставщиком оборудования.

? Один из светодиодов работает неправильно.

1. Убедитесь, что вы знаете, как светодиод должен работь в нормальном режиме. См. Разд. 1.5 на с. 27.
2. Проверьте подключение оборудования. См. Краткое руководство.
3. Убедитесь, что кабели не повреждены. Для замены поврежденных кабелей свяжитесь с поставщиком оборудования.
4. Выключите и снова включите P660RT2.

5 Если неисправность не устраняется, свяжитесь с поставщиком оборудования.

14.2 Доступ и регистрация в P660RT2

Потеряна информация об IP-адресе P660RT2.

1 IP-адрес, установленный изготовителем по умолчанию – **192.168.1.1**.
2 Если IP-адрес был изменен и затем информация об этом утеряна, можно посмотреть IP-адрес P660RT2, установленный для шлюза по умолчанию на компьютере. Чтобы выполнить это на компьютере под управлением Windows, нажмите кнопку «Start» (Пуск) > «Run» (Выполнить), введите команду **cmd** и затем **ipconfig**. IP-адрес «Default Gateway» (Шлюз по умолчанию) может являться IP-адресом модема P660RT2 (это зависит от конкретной сети). Введите этот IP-адрес в Интернет браузере.
3 Если это не поможет, выполните сброс устройства к заводским настройкам по умолчанию. См. Разд. 14.4 на с. 153.

Утерян пароль.

1 Пароль администратора по умолчанию – **1234**.
2 Если это не поможет, выполните сброс устройства к заводским настройкам по умолчанию. См. Разд. 14.4 на с. 153.

Не отображается окно Web-конфигуратора Login (Регистрация) или отсутствует доступ в систему.

1 Убедитесь, что используется правильный IP-адрес.
   - IP-адрес, установленный изготовителем по умолчанию – 192.168.1.1.
   - Если IP-адрес был изменен, убедитесь, что используется новый IP-адрес.
   - Если IP-адрес был изменен и затем утерян, см. рекомендации по поиску и устранению неисправностей в Потеряна информация об IP-адресе P660RT2.
2 Проверьте подключение оборудования и убедитесь, что светодиоды работают в нормальном режиме. См. Краткое руководство и Разд. 1.5 на с. 27.
3 Убедитесь, что в Интернет-браузере включена поддержка всплывающих окон, а также JavaScripts Java. См. Прил. E на с. 183.
4 Если функция Any IP (Любой IP) (Разд. 5.3.4 на с. 77) отключена, проверьте, что компьютер находится в тойже подсети, что и P660RT2. (Пропустите этот шаг, если

известно, что между компьютером и модемом P660RT2 имеются маршрутизаторы.)

5 Выполните сброс устройства к заводским настройкам по умолчанию и попробуйте получить доступ к P660RT2 с IP-адресом по умолчанию. См. Разд. 14.4 на с. 153.

6 Если неисправность не устраняется, обратитесь к сетевому администратороу или поставщику, или выполните дополнительные рекомендации.

Дополнительные рекомендации

- Попробуйте получить доступ к P660RT2 с использованием другой службы, например, Telnet. Если доступ к P660RT2 существует, проверьте параметры удаленного управления P660RT2, выполняемого с помощью HTTP.

Окно Login (Регистрация) отображается, но невозможно выполнить вход в систему P660RT2.

1 Проверьте, что имя пользователя и пароль введены правильно. Для регистрации с правами администратора введите имя пользователя **admin** и пароль по умолчанию **1234**. Символы в эти поля вводятся с учетом регистра, следовательно, проверьте, что [Caps Lock] выключена.

2 Нельзя получить доступ к Web-конфигуратору, если другой пользователь подключился к P660RT2 через Telnet. Подключитесь к P660RT2 позднее или попросите зарегистрированного пользователя выполнить выход из системы.

3 Выключите и снова включите P660RT2.

4 Отключите и снова подключите к P660RT2 адаптер или кабель питания.

5 Если это не поможет, выполните сброс устройства к заводским настройкам по умолчанию. См. Разд. 14.4 на с. 153.

Невозможно подключиться к P660RT2 через Telnet.

См. рекомендации по поиску и устранению неисправностей в разделе Не отображается окно Web-конфигуратора Login (Регистрация) или отсутствует доступ в систему. Рекомендации по настройке браузера сюда не относятся.

Невозможно выполнить загрузку/скачивание файла конфигурации с помощью FTP. / Не удается загрузить новую версию микропрограммы с помощью FTP.

См. рекомендации по поиску и устранению неисправностей в Не отображается окно Web-конфигуратора Login (Регистрация) или отсутствует доступ в систему. Рекомендации по настройке браузера сюда не относятся.

14.3 Доступ в Интернет

Невозможно получить доступ в Интернет.

1. Проверьте подключение оборудования и проверьте, что светодиоды работают в нормальном режиме. См. Краткое руководство и Разд. 1.5 на с. 27.
2. Проверьте, что введены правильно параметры учетной записи, предоставленные Интерне-провайдером. Символы в эти поля вводятся с учетом регистра, следовательно, проверьте, что [Caps Lock] выключена.
3. Отключите все кабели от устройства и еще раз выполните инструкции Краткого руководства.
4. Если неисправность не устраняется, обратитесь к Интернет-Провайдеру.

Невозможно получить доступ в Интернет. Доступ в Интернет настроен через P660RT2, но подключение к Интернету больше не работает.

1. Проверьте подключение оборудования и проверьте, что светодиоды работают в нормальном режиме. См. Краткое руководство и Разд. 1.5 на с. 27.
2. Выключите и снова включите P660RT2.
3. Если неисправность не устраняется, обратитесь к Интернет-Провайдеру.

Подключение к Интернету работает медленно или нестабильно.

1. Возможно, что локальная сеть перегружена. Посмотрите на светодиоды и проверьте их работу по Разд. 1.5 на с. 27. Если Модем P660RT2 посылает и передает большие объемы информации, закройте программы, которые используют Интернет, особенно равноправные приложения.
2. Выключите и снова включите P660RT2.
3. Если неисправность не устраняется, обратитесь к сетевому администратору или поставщику.

14.4 Сброс настроек модема P660RT2 к заводским установкам

Если вы забыли пароль или не можете получить доступ к Web-конфигуратору, необходимо нажать на кнопку «RESET» на задней панели P660RT2 для загрузки файла конфигурации, установленного изготовителем по умолчанию. Это означает, что прежняя конфигурация будет полностью потеряна, и пароль будет сброшен на значение по умолчанию «1234».

14.4.1 Использование кнопки сброса настроек

1. Убедитесь, что светодиод «POWER» (Питание) горит (не мигает).
2. Нажмите и удерживайте кнопку «RESET» (СБРОС) в течение 10 секунд или до тех пор, пока светодиод «POWER» (Питание) не начнет мигать, затем отпустите ее. Когда светодиод «POWER» (Питание) начинает мигать, это означает, что настройки по умолчанию восстановлены и происходит перезапуск P660RT2.

Часть IV
Приложения и алфавитный указатель

Технические характеристики(157)
Инструкции по настенному монтажу(161)
Разделители частот и микрофильтры(163)
Настройка IP-адреса компьютера(167)
Всплывающие окна, сценарии и разрешения Java(183)
IP-адреса и организация подсетей(191)
Конфликты при назначении IP-адресов(201)
Службы Интернет(205)
Интерпретатор команд(209)
Правовая информация(215)
Сервисная служба(219)

A

Технические характеристики

См. также общий обзор основных функций в главе "Введение".

Таблицы характеристик

Табл. 47 Устройство

IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Пароль по умолчанию	администратор: 1234 пользователь: user
Диапазон DHCP	от 192.168.1.33 до 192.168.1.64
Размеры (Д x Ш x В)	111 мм (Д) × 106,5 мим (Ш) × 35 мм (В)
Питание	9 В DC (постоянный ток), 1А
Порт Ethernet	порт Ethernet 10/100 Мбит/с с разъемом RJ-45 и автоопределением MDI/MDI-X
Рабочая температура	0º C ~ 40º C
Температура хранения	-20 ºC ~ 60 ºC
Рабочая влажность	20 % ~ 85 %
Влажность при хранении	20% ~ 90%
Расстояние между центрами отверстий на задней панели устройства.	75 мм
Размер винтов для настенного крепления	M3*10

Табл. 48 Встроенное программное обеспечение

Стандарты ADSL	Многорежимный стандарт (ANSI T1.413, выпуск 2; G.dmt(G.992.1); G.lite(G992.2)) f#. ADSL2 G.dmt.bis (G.992.3). ADSL2 G.lite.bis (G.992.4). ADSL2+ (G.992.5). Annex L/M (только при работе в режиме Annex A) SRA (Seamless Rate Adaptation – Плавная регулировка скорости передачи). Адаптация с автоматическим выбором скорости передачи. Физическое подключение ADSL ATM AAL5 (5-й уровень адаптации ATM). Подключение по нескольким протоколам через AAL5 (RFC2684/1483). PPP через ATM AAL5 (RFC 2364). PPP по Ethernet (RFC 2516). Инкапсуляция RFC 1483 через ATM. Инкапсулированная маршрутизация MAC (инкапсуляция ENET). Мультиплексирование на базе VC и LLC. До 8 постоянных виртуальных каналов (PVC). I.610 F4/F5 OAM.
Поддержка других протоколов.	PPP (Point-to-Point Protocol – Протокол «точка-точка») – протокол канального уровня. Прозрачный межсетевой мост для неподдерживаемых протоколов сетевого уровня. Сервер/Клиент/Ретранслятор DHCP. RIP I/RIP II. ICMP. SNMP v1 и v2c с поддержкой MIB II (RFC 1213). Многоадресная рассылка IP IGMP v1 и v2. Прокси-сервер IGMP. UPnP.
Управление	Встроенный Web-конфигуратор. CLI (Command Line Interpreter – Интерпретатор командной строки). Удаленное управление по протоколу Telnet или Web. Возможность управления по протоколу SNMP. FTP/TFTP для загрузки микропрограммного обеспечения, архивирования и восстановления конфигурации. Встроенные средства диагностики для флэш-памяти (FLASH), каналов ADSL, ОЗУ (RAM) и порта локальной сети (LAN). MAP — “Multimedia Auto Provisioner” (учебное пособие по установке и автоматический конфигуратор мультимедийных средств).
NAT/SUA (Трансляция сетевых адресов/Учетная запись одиночного пользователя)	Переадресация портов. Сеансы 1024 NAT. Мультимедийные приложения. PPPOE под NAT/SUA.
Статическая маршрутизация.	16 IP и 4 моста.
Прочие функции	Any IP (Любой IP). Перенаправление трафика. Динамическая система доменных имен (DYNDNS). Псевдоним IP.

Табл. 49 Характеристики встроенного программного обеспечения

Обновление микропрограммы	Загрузите новую версию микропрограммы (если есть) с Web-сайта ZyXEL и с помощью Web-конфигуратора, средства FTP или TFTP загрузите ее в модем P660RT2. Примечание: необходимо загружать микропрограмму строго в соответствии с конкретной моделью устройства.
Резервное сохранение и восстановление конфигурации	Сделайте копию конфигурации P660RT2. Эту копию можно загрузить в P660RT2 позже, если потребуется вернуться к предыдущей конфигурации.
Трансляция сетевых адресов (NAT)	Каждый компьютер в сети должен иметь уникальный IP-адрес. Используйте функцию NAT для преобразования общедоступного IP-адреса(ов) в несколько частных IP-адресов для компьютеров вашей сети.
Несколько PVC (Permanent Virtual Circuits – постоянный виртуальный канал))	Модем P660RT2 поддерживает до 8 постоянных виртуальных каналов.
Переадресация портов	Если в сети есть сервер (например, Web-сервер или сервер электронной почты), с помощью этой функции можно разрешить доступ к нему пользователям из Интернета.
Перенаправление трафика	Функция перенаправления трафика автоматически направляет трафик WAN к резервному шлюзу LAN, если P660RT2 не может установить соединение с Интернетом, выполняя, таким образом, функции дополнительного резервирования в случае невозможности подключения к WAN обычным образом.
DHCP (Протокол динамической настройки узла)	С помощью этой функции модем P660RT2 назначает IP-адреса, шлюз IP по умолчанию и серверы DNS компьютерам локальной сети.
Поддержка динамических DNS	Поддержка динамической DNS (Domain Name System – система доменных имен) позволяет использовать фиксированный URL, например, www.zyxel.com с динамическим IP-адресом. Для использования этой услуги необходимо зарегистрироваться у провайдера услуг динамической DNS.
Многоадресная рассылка IP	Многоадресная рассылка IP используется для отправки трафика определенной группе компьютеров. Модем P660RT2 поддерживает версии 1 и 2 протокола IGMP (Internet Group Management Protocol - протокол управления группами в сети Интернет), который используется для присоединения к группам многоадресной рассылки (см. RFC 2236).
Псевдоним IP	Псевдоним IP позволяет разделить физическую сеть на логические подсети на одном интерфейсе Ethernet, при этом P660RT2 действует как шлюз для каждой подсети.
Маршрутизация на базе стратегии IP (IPPR)	Как правило, маршрутизация производится только на основе адреса получателя, поэтому маршрутизатор выбирает самый короткий путь для пересылки пакета. Политика маршрутизации IP (IP Policy Routing — IPPR) обеспечивает механизм замены схемы маршрутизации по умолчанию и позволяет изменить алгоритм прохождения пакетов на основе политики, определяемой сетевым администратором.

Табл. 49 Характеристики встроенного программного обеспечения

Time and Date (Время и дата)	Можно синхронизировать текущее время и дату с внешним сервером времени при включении питания P660RT2. Время также можно установить вручную. Дата и время используются в регистрационных журналах.
PPPoE	PPPoE имитирует коммутируемое соединение для доступа в Интернет.
Универсальная функция «Plug and Play» (UPnP)	Устройство UPnP может динамически присоединяться к сети, получать IP-адрес, сообщать о своих функциях и собирать информацию о других устройствах сети.
Удаленное управление	Удаленное управление позволяет с помощью выбранной службы (например, HTTP или FTP) с компьютера в сети (LAN или WAN) подключиться к P660RT2.

B

Инструкции по настенному монтажу

Для установки модема P660RT2 на стену выполните следующее:

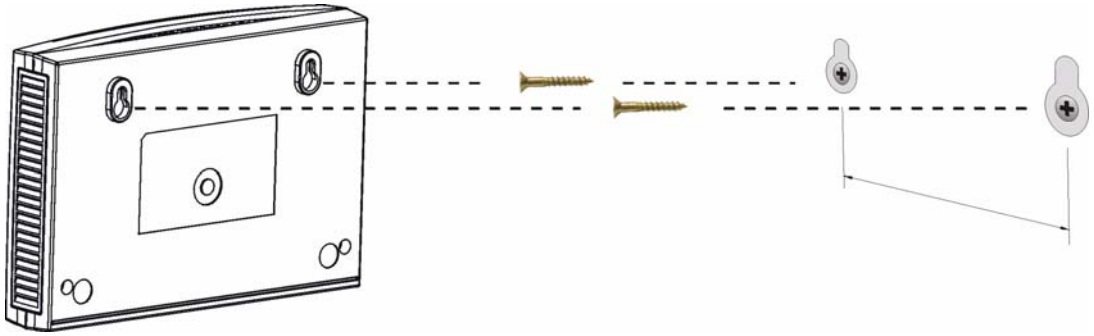
В Прил. A на с. 157 указан размер винтов и расстояние между центрами отверстий.

1. Найдите на стене свободное место, расположенное на достаточной высоте. Стена должна быть прочной.
2. Просверлите два отверстия под саморезы. Расстояние между центрами отверстий должно соответствовать указанному в приложении «Технические характеристики изделия».

При сверлении не повредите проходящие внутри стены трубы и скрытую проводку.

3. Саморезы вкручивайте не полностью. Оставьте небольшой зазор (около 5 мм) между головками саморезов и стеной.
4. Убедитесь, что саморезы надежно закреплены в стене. Они должны выдерживать вес модема P660RT2 и соединительных проводов.
5. Совместите отверстия на задней панели модема P660RT2 с саморезами в стене. Повесьте модем P660RT2 на саморезы.

Рис. 89 Пример настенного монтажа



C

Разделители частот и микрофильтры

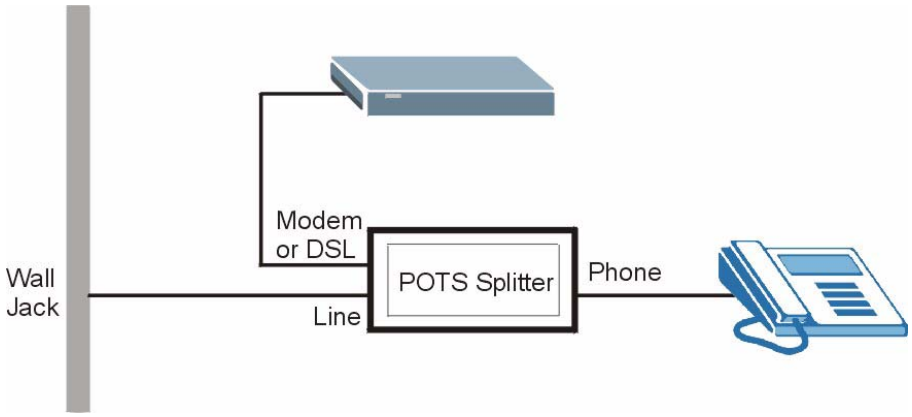
В этом приложении описывается установка сплиттера для подключения телефонного аппарата и телефонного микрофильтра.

Подключение телефонного сплиттера

При использовании полноскоростного стандарта ADSL (стандарт G.dmt) можно подключить телефонный сплиттер, обеспечивающий разделение телефонных сигналов и сигналов ADSL. Это позволяет одновременно использовать одну телефонную линию для звонков и доступа в Интернет. Кроме того, сплиттер устраняет помехи, вносимые телефонными аппаратами.

Сплиттер устанавливается в точке подвода телефонной линии, как показано на следующем рисунке.

Рис. 90 Подключение телефонного сплиттера



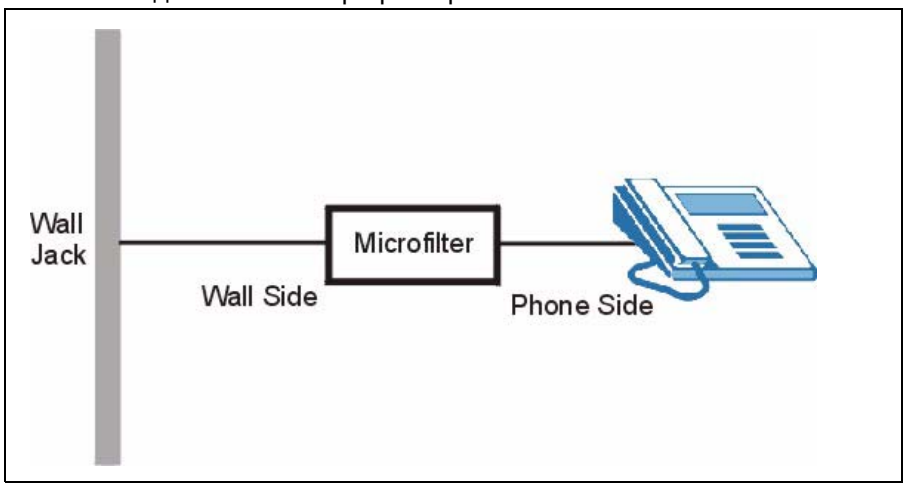
1. Переведите переключатель на сплиттере в положение “Annex A”
1. Подключите разъем с маркировкой "Phone" к телефону.
2. Подключите разъем с маркировкой "Modem" или "DSL" к модему P660RT2.
3. Подключите разъем с маркировкой "Line" к настенной телефонной розетке.

Телефонные микрофильтры

Передача голосовых сигналов телефона происходит в более низком диапазоне частот (0 - 4 кГц), в то время как передача сигналов ADSL - в более высоком широкополосном диапазоне (более 4 кГц). Микрофильтр действует как фильтр нижних частот для телефона, что обеспечивает отсутствие влияния сигналов ADSL на передачу телефонных сигналов. Телефонный микрофильтр поставляется отдельно.

1. Найдите и отключите все телефоны.
2. Подключите кабель от телефонной розетки к разъему “wall side” микрофильтра.
3. Подключите разъем «phone» микрофильтра к телефону, как показано на следующем рисунке.
4. После подключения кабелей проверьте, работает ли телефон. Если телефон не работает, отключите микрофильтр и обратитесь в местную телефонную компанию или к поставщику микрофильтра.

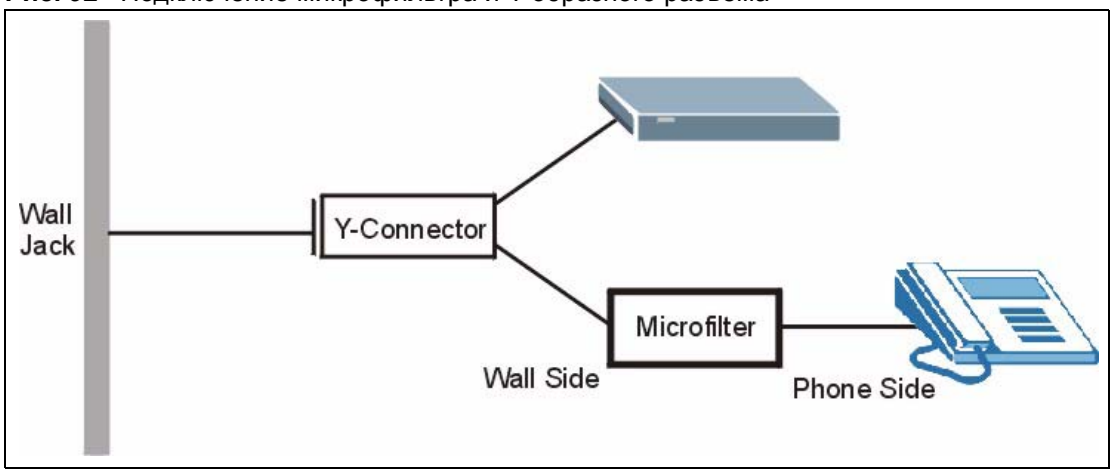
Рис. 91 Подключение микрофильтра



Также можно использовать Y-образный разъем с микрофильтром, чтобы подключить модем и телефон к одной телефонной розетке без использования телефонного разделителя частот.

1. Подключите телефонный кабель от настенной розетки к Y-образному разъему со стороны, где имеется один вывод.
2. Подключите один кабель от Y-образного разъема со стороны с двумя выводами к разъему «LINE» микрофильтра.
3. Подключите другой кабель от конца Y-образного разъема с двумя выводами к P660RT2.
4. Подключите разъем «phone» микрофильтра к телефону, как показано на следующем рисунке.

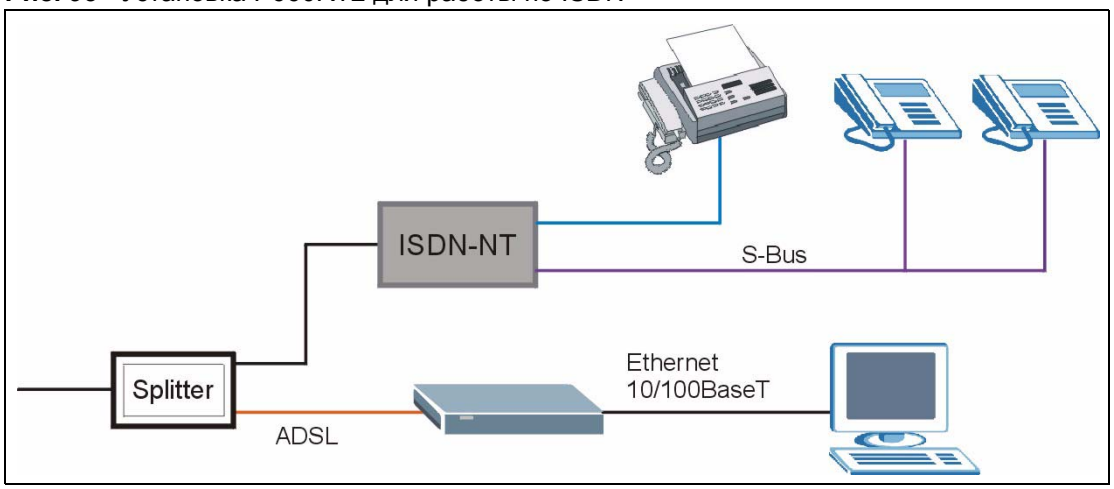
Рис. 92 Подключение микрофильтра и Y-образного разъема



Установка P660RT2 для работы по ISDN или с охранно-пожарной сигнализацией

Этот раздел предназначен только для тех, кто использует модем P660RT2 с ADSL в сети ISDN или на линии с установленной охранно-пожарной сигнализацией. Ниже приводится пример установки P660RT2 для работы по ISDN.

Рис. 93 Установка P660RT2 для работы по ISDN



1 Переведите переключатель на сплиттере в положение “Annex B”

1 Подключите разъем с маркировкой "Phone" к терминалу ISDN или охранно-можарной сигнализации

2 Подключите разъем с маркировкой "Modem" или "DSL" к модему P660RT2.

3 Подключите разъем с маркировкой "Line" к настенной телефонной розетке.

D

Настройка IP-адреса компьютера

На всех компьютерах должны быть установлены сетевые платы Ethernet 10 или 100 Мбит/с и протоколы TCP/IP.

Операционные системы Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 и выше, а также все версии систем UNIX/LINUX уже содержат программные компоненты, необходимые для инсталляции и использования стека протоколов TCP/IP на вашем компьютере. При использовании ОС Windows 3.1 необходимо приобрести пакет прикладных программ TCP/IP другого производителя.

Протокол TCP/IP обычно уже установлен на компьютерах с операционной системой Windows NT/2000/XP, Macintosh OS 7 и более поздними версиями.

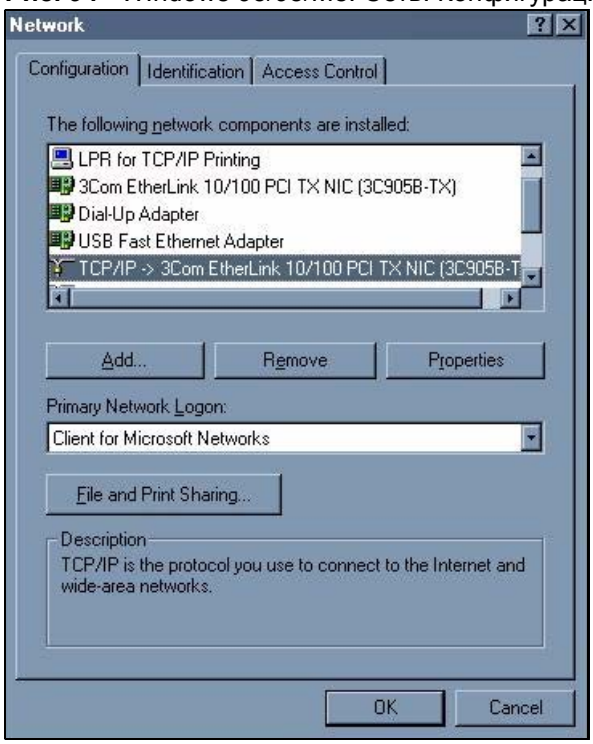
После инсталляции соответствующих компонентов TCP/IP сконфигурируйте параметры TCP/IP для подключения к сети.

Если вы назначаете IP-адреса вручную, вместо использования динамических адресов, убедитесь, что ваши компьютеры имеют IP-адреса, относящиеся к той же подсети, что и порт LAN P660RT2.

Windows 95/98/Me

Нажмите кнопку «Start» (Пуск), «Settings» (Настройка), «Control Panel» (Панель управления) и дважды щелкните по иконке «Network» (Сеть), чтобы открыть окно «Network» (Сеть).

Рис. 94 WIndows 95/98/Me: Сеть: Конфигурация



Установка компонентов

В окне «Network» (Сеть) на закладке «Configuration» (Конфигурация) отображается список установленных компонентов. Вам потребуется сетевая карта, протокол TCP/IP и клиент для сетей Microsoft.

Если необходимо установить сетевую карту:

1. В окне «Network» (Сеть) нажмите кнопку «Add» (Добавить).
2. Выберите «Adapter» (Сетевая карта) и нажмите кнопку «Add» (Добавить).
3. Выберите производителя и модель вашей сетевой карты и нажмите кнопку «OK».

Если необходимо установить протокол TCP/IP:

1. В окне «Network» (Сеть) нажмите кнопку «Add» (Добавить).
2. Выберите «Protocol» (Протокол) и нажмите «Add» (Добавить).
3. Выберите «Microsoft» из списка производителей.
4. Выберите «TCP/IP» из списка сетевых протоколов и нажмите кнопку «OK».

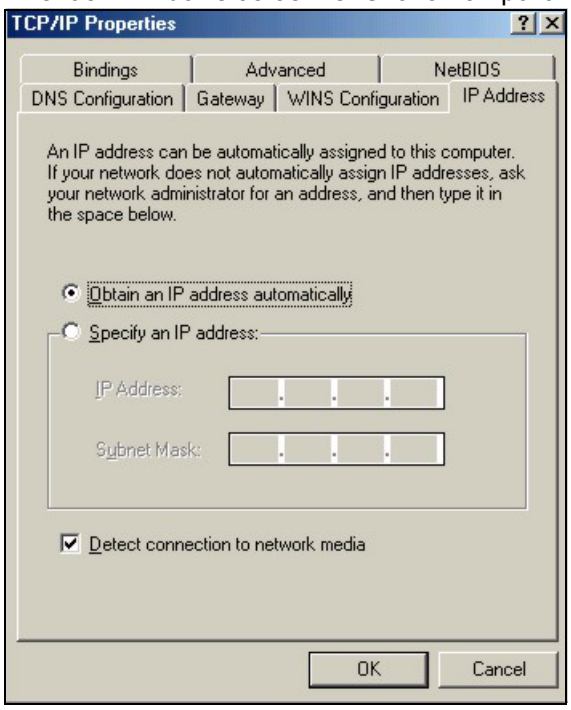
Если необходимо установить «Client for Microsoft Networks» (Клиент для сетей Microsoft):

1. Щелкните по кнопке «Add» (Добавить).
2. Выберите «Client» (Клиент) и нажмите кнопку «Add» (Добавить).
3. Выберите «Microsoft» из списка производителей.
4. Выберите «Client for Microsoft Networks» (Клиент для сетей Microsoft) из списка сетевых клиентов и нажмите кнопку «OK».
5. Перезагрузите компьютер, чтобы сделанные изменения вступили в силу.

Настройка

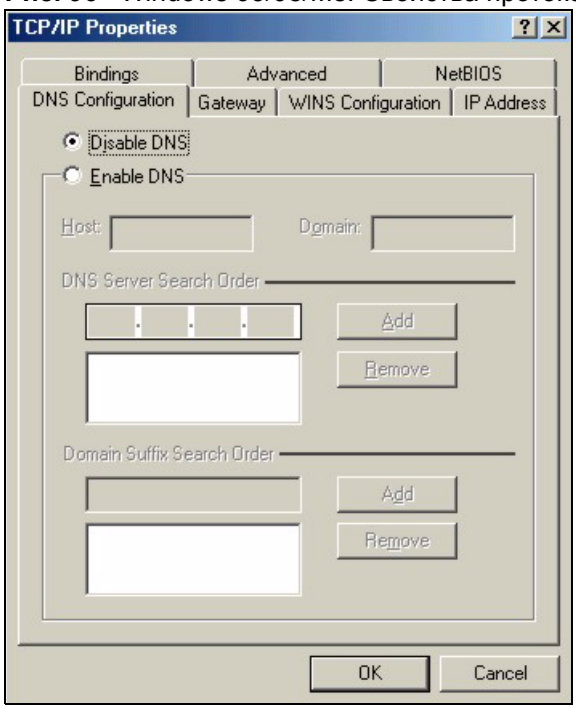
1. В окне «Network» (Сеть) выберите закладку «Configuration» (Конфигурация), затем выберите запись TCP/IP для вашей сетевой карты и нажмите кнопку «Properties» (Свойства)
2. Выберите закладку «IP Address» (IP-адрес).
   - Если используется динамический IP-адрес, выберите «Obtain an IP address automatically» (Получить IP-адрес автоматически).
   - Если используется статический IP-адрес, выберите «Specify an IP address» (Указать IP-адрес явным образом) и заполните поля «IP Address» (IP-адрес) и «Subnet Mask» (Маска подсети).

Рис. 95 Windows 95/98/Me: Свойства протокола TCP/IP: IP-адрес



3. Выберите закладку «DNS Configuration» (Конфигурация DNS).
   - Если у вас нет данных по конфигурации DNS, выберите «Disable DNS» (Отключить DNS).
   - Если вы располагаете информацией о конфигурации DNS, выберите «Enable DNS» (Включить DNS) и заполните поля, расположенные ниже (в заполнении всех полей может не быть необходимости).

Рис. 96 Windows 95/98/Me: Свойства протокола TCP/IP: Конфигурация DNS



4 Выберите закладку «Gateway» (Шлюз).
   - Если вы не знаете IP-адрес шлюза, удалите все установленные ранее шлюзы.
   - Если у вас есть IP-адрес шлюза, введите его в поле «New gateway» (Новый шлюз) и нажмите кнопку «Add» (Добавить).
5 Щелкните «OK», чтобы сохранить сделанные изменения и закрыть окно «TCP/IP Properties» (Свойства протокола TCP/IP).
6 Щелкните «OK», чтобы закрыть окно «Network» (Сеть). При появлении запроса вставьте в дисковод компакт диск Windows.
7 Включите P660RT2 и перезагрузите компьютер при появлении запроса.

Проверка настроек

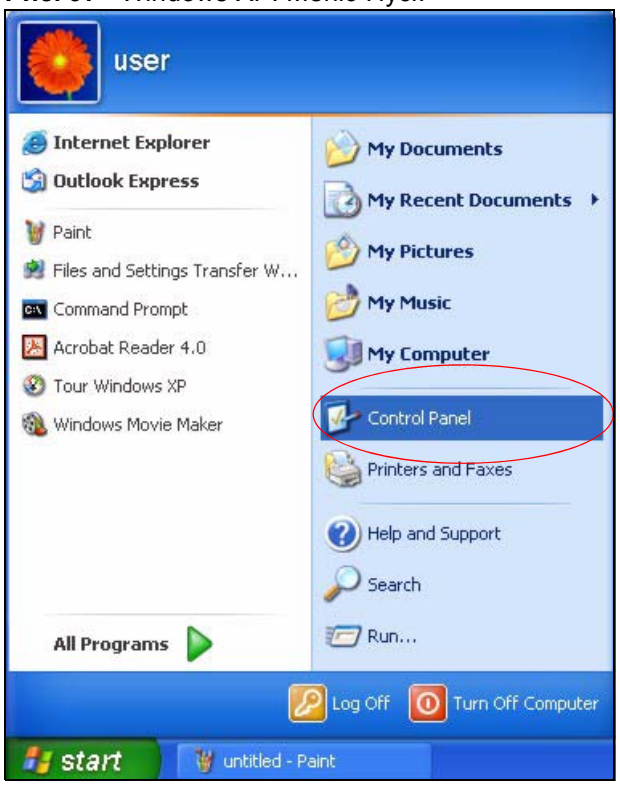
1 Щелкните «Start» (Пуск) и затем «Run» (Выполнить).
2 В окне «Run» (Выполнить) введите "winipcfg" и нажмите кнопку «OK» для отображения окна «IP Configuration» (Настройка IP).
3 Выберите свою сетевую карту. Вы должны увидеть IP-адрес, маску подсети и шлюз по умолчанию вашего компьютера.

Windows 2000/NT/XP

В следующих рисунках используется тема графического интерфейса Windows XP по умолчанию.

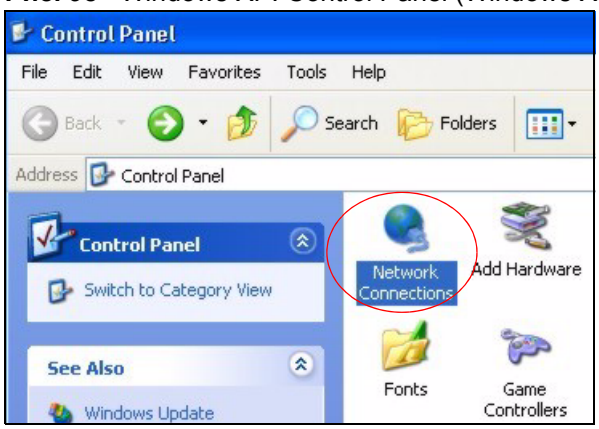
1 Щелкните «start» (пуск) («Start» (Пуск) в Windows 2000/NT), «Settings» (Настройка), «Control Panel» (Панель управления).

Рис. 97 Windows XP: Меню Пуск



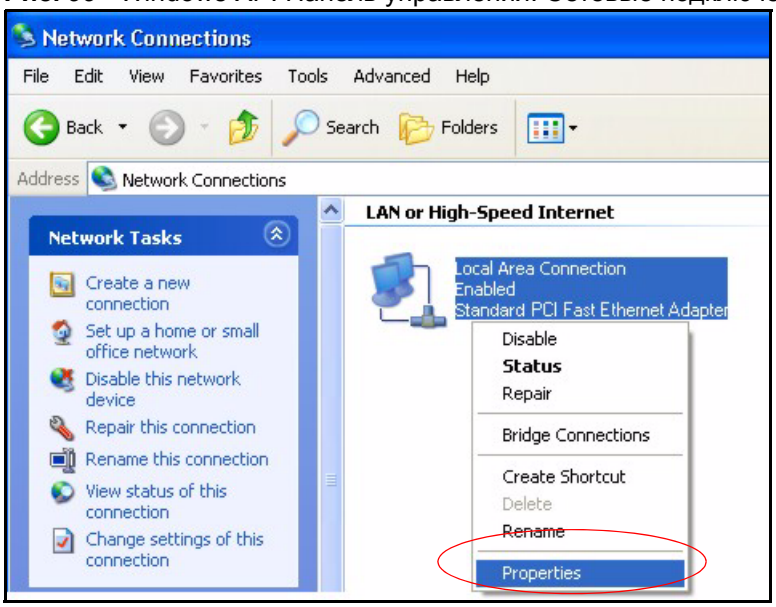
2 В панели управления дважды щелкните «Network Connections» (Сетевые подключения) (или «Network and Dial-up Connections» (Сеть и удаленный доступ к сети) в Windows 2000/NT).

Рис. 98 Windows XP: Control Panel (Windows XP: Панель управления



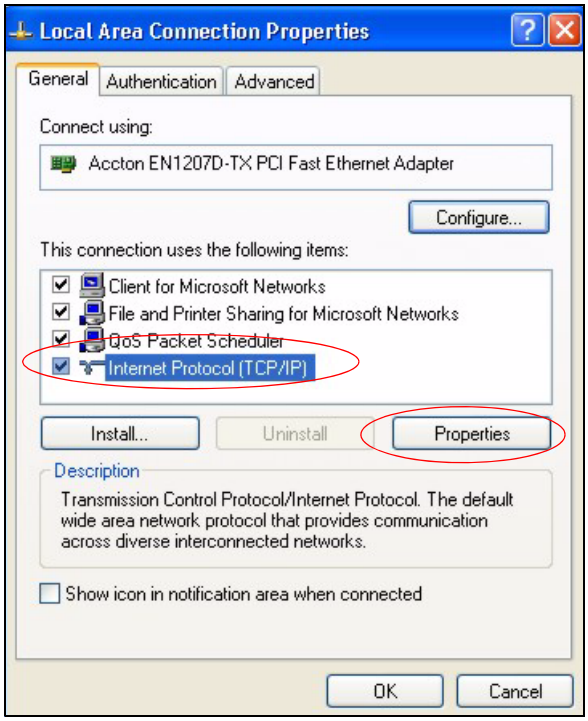
3 Щелкните правой кнопкой мыши «Local Area Connection» (Подключение по локальной сети) и выберите «Properties» (Свойства).

Рис. 99 Windows XP: Панель управления: Сетевые подключения: Свойства



4 На закладке «General» (Общие) в WinXP выберите «Internet Protocol (TCP/IP)» (Протокол Интернета (TCP/IP)) и щелкните «Properties» (Свойства).

Рис. 100 Windows XP: Подключение по локальной сети: Свойства

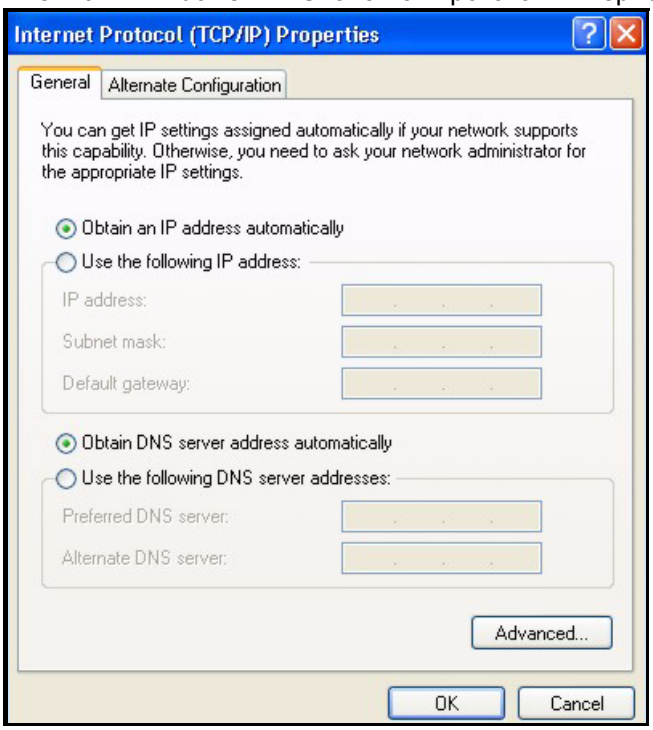


5 Появляется окно «Internet Protocol TCP/IP Properties» (Свойства: Протокол Интернета (TCP/IP)) (закладка «General» (Общие) в Windows XP).

- Если вы используете динамический IP-адрес, выберите «Obtain an IP address automatically» (Получить IP-адрес автоматически).

- Если вы имеете статический IP-адрес, выберите «Use the following IP Address» (Использовать следующий IP-адрес) и заполните поля «IP address» (IP-адрес), «Subnet mask» (Маска подсети) и «Default gateway» (Основной шлюз).
- Щелкните по кнопке «Advanced» (Дополнительно).

Рис. 101 Windows XP: Свойства: Протокол Интернета (TCP/IP)



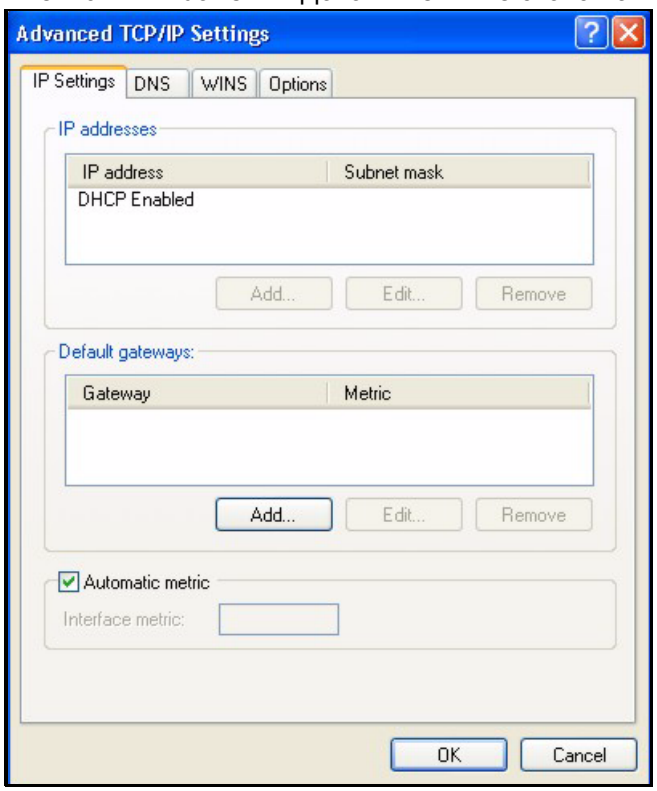
6 Если Вы не знаете IP-адрес шлюза, удалите все предварительно настроенные шлюзы на закладке «IP Settings» (Параметры IP) и нажмите «OK».

Для настройки дополнительных IP-адресов выполните следующие действия:

- На закладке «IP Settings» (Параметры IP) в поле для IP-адресов нажмите «Add» (Добавить).
- В окне «TCP/IP Address» (Адрес TCP/IP), введите IP-адрес в поле «IP address» (IP-адрес) и маску подсети в поле «Subnet mask» (Маска подсети), затем нажмите кнопку «Add» (Добавить).
- Повторите описанные выше действия для каждого IP-адреса, который необходимо добавить.
- Настройте дополнительные шлюзы по умолчанию на закладке «IP Settings» (Параметры IP), щелкнув по кнопке «Add» (Добавить) в разделе «Default gateways» (Основные шлюзы).
- В окне «TCP/IP Gateway Address» (Адрес шлюза TCP/IP), введите IP-адрес шлюза по умолчанию в поле «Gateway» (Шлюз). Для ручной настройки метрики по умолчанию (количества транзитных пунктов при передаче), снимите флажок «Automatic metric» (Автоматическая метрика) и введите значение в поле «Metric» (Метрика).
- Щелкните по кнопке «Add» (Добавить).
- Повторите предыдущие три действия для всех шлюзов, которые необходимо добавить.

- Щелкните «OK» после завершения настройки.

Рис. 102 Windows XP: Дополнительные свойства TCP/IP

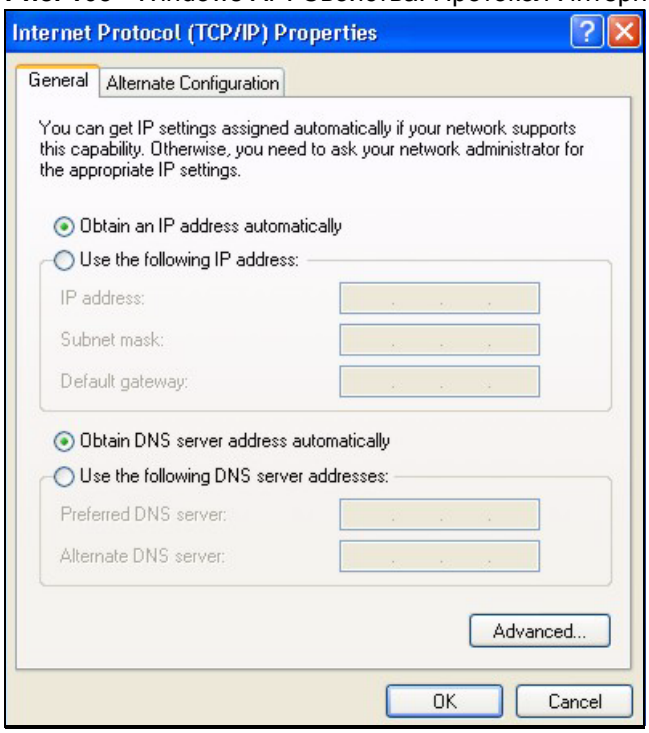


7 В окне «Internet Protocol TCP/IP Properties» (Свойства: Протокол Интернета (TCP/IP)) на закладке «General» (Общие) в Windows XP:

- Выберите «Obtain DNS server automatically» (Получить адрес DNS-сервера автоматически), если вы не знаете IP-адрес(а) сервера(ов) DNS.
- Если вы знаете IP-адрес(а) сервера(ов) DNS, выберите «Use the following DNS server addresses» (Использовать следующие адреса серверов DNS), и введите адреса в поля «Preferred DNS server» (Предпочитаемый DNS-сервер) и «Alternate DNS server» (Альтернативный DNS-сервер).

  Если серверы DNS уже установлены, щелкните по кнопке «Advanced» (Дополнительно), а затем на закладке «DNS» для их упорядочивания.

Рис. 103 Windows XP: Свойства: Протокол Интернета (TCP/IP)



8 Щелкните «OK», чтобы закрыть окно «Internet Protocol (TCP/IP) Properties» (Свойства: Протокол Интернета (TCP/IP)).

9 Щелкните «Close» (Закрыть) («OK» в Windows 2000/NT), чтобы закрыть окно «Local Area Connection Properties» (Свойства подключения по локальной сети).

10 Закройте окно «Network Connections» (Сетевые подключения) («Network and Dial-up Connections» (Сеть и удаленный доступ к сети) в Windows 2000/NT).

11 Включите P660RT2 и перезагрузите компьютер при появлении запроса.

Проверка настроек

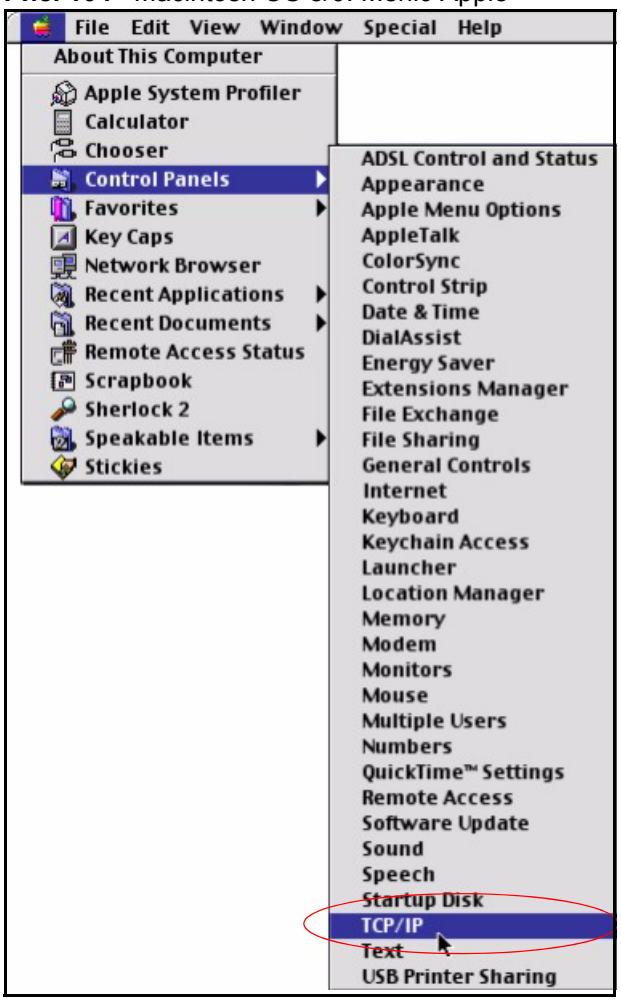
1 Щелкните «Start» (Пуск), «All Programs» (Все программы), «Accessories» (Стандартные) и «Command Prompt» (Командная строка).

2 В окне «Command Prompt» (Командная строка) введите команду "ipconfig" и нажмите клавишу [ENTER]. Также можно открыть окно «Network Connections» (Сетевые подключения), щелкнуть правой кнопкой мыши на сетевом подключении, выбрать «Status» (Состояние) и затем щелкнуть по закладке «Support» (Поддержка).

Macintosh OS 8/9

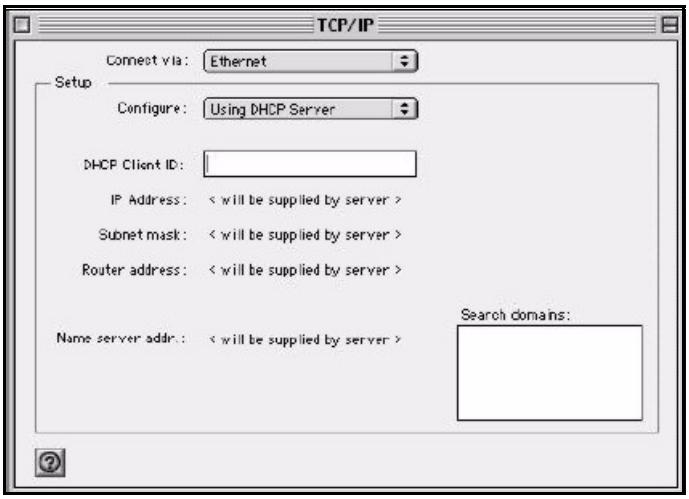
1 Нажмите кнопку меню Apple, выберите «Control Panel» (Панель управления), а затем дважды щелкните «TCP/IP», чтобы открыть «TCP/IP Control Panel» (Панель управления TCP/IP).

Рис. 104 Macintosh OS 8/9: Меню Apple



2 Выберите «Ethernet built-in» (Встроенный сетевой контроллер) из списка «Connect via» (Подключение через...).

Рис. 105 Macintosh OS 8/9: TCP/IP



3 Для настройки динамических параметров выберите «Using DHCP» (Использовать сервер DHCP) в списке «Configure:» (Настроить:).

4 Для настройки статических параметров выполните следующие действия:
   - В разделе «Configure» (Настроить), выберите «Manually» (Настроить вручную).
   - Введите IP-адрес в поле «IP Address» (IP-адрес).
   - Введите маску подсети в поле «Subnet mask» (Маска подсети).
   - Введите IP-адрес P660RT2 в окне «Router address» (Адрес маршрутизатора).
5 Закройте окно «TCP/IP Control Panel» (Панель управления TCP/IP).
6 При появлении запроса нажмите «Save» (Сохранить) для сохранения изменений в конфигурации.
7 Включите P660RT2 и перезагрузите компьютер при появлении запроса.

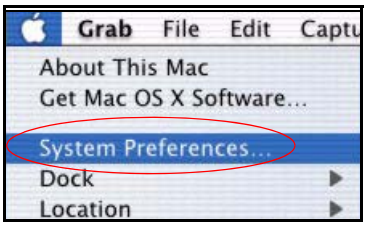
Проверка настроек

Проверьте свойства TCP/IP в окне «TCP/IP Control Panel» (Панель управления TCP/IP).

Macintosh OS X

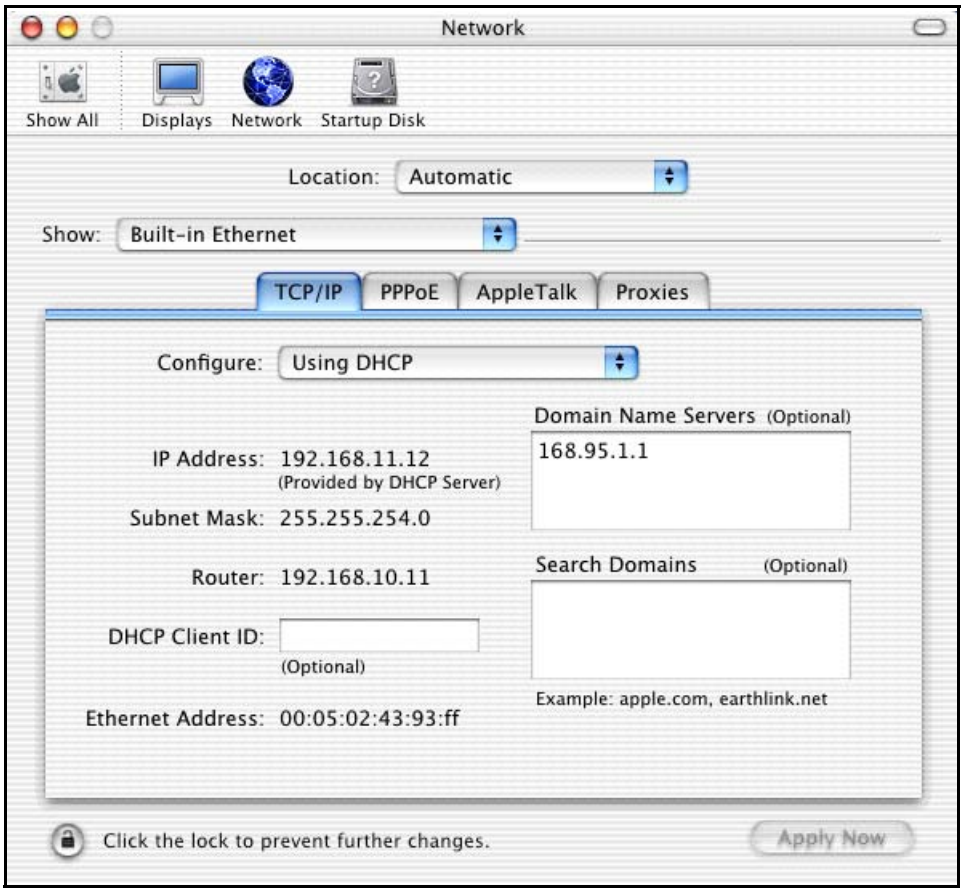
1 Нажмите кнопку меню Apple и затем «System Preferences» (Настройки системы), чтобы открыть окно «System Preferences» (Настройки системы).

Рис. 106 Macintosh OS X: Меню Apple



2 Нажмите «Network» (Сеть) на панели иконок.
   - Выберите «Automatic» (Автоматически) в списке «Location» (Местонахождение).
   - Выберите «Built-in Ethernet» (Встроенный сетевой контроллер) из списка «Show» (Показать).
   - Выберите закладку «TCP/IP».
3 Для настройки динамических параметров выберите «Using DHCP» (Использовать DHCP) в списке «Configure» (Настроить).

Рис. 107 Macintosh OS X: Сеть



4 Для настройки статических параметров выполните следующие действия:
   - В разделе «Configure» (Настроить), выберите «Manually» (Настроить вручную).
   - Введите IP-адрес в поле «IP Address» (IP-адрес).
   - Введите маску подсети в поле «Subnet mask» (Маска подсети).
   - Введите IP-адрес P660RT2 в окне «Router address» (Адрес маршрутизатора).
5 Щелкните «Apply Now» (Применить) и закройте окно.
6 Включите P660RT2 и перезагрузите компьютер при появлении запроса.

Проверка настроек

Проверьте свойства TCP/IP в окне **«Network» (Сеть)**.

Linux

В этом разделе описана настройка TCP/IP Вашего компьютера в Red Hat Linux 9.0. Порядок настройки, диалоговые окна и размещение файлов могут различаться в зависимости от версии Linux.

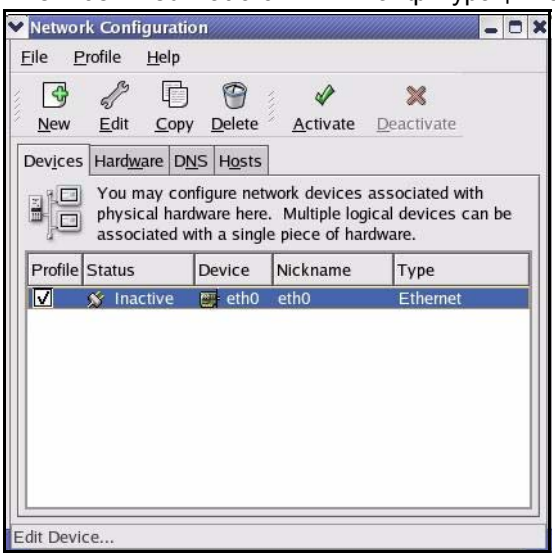
Вы должны быть зарегистрированы в системе в качестве корневого администратора.

Использование графического интерфейса KDE

Для настройки IP-адреса Вашего компьютера с помощью KDE проделайте следующее.

1 Нажмите кнопку «Red Hat» (в нижнем левом углу экрана), выберите «System Setting» (Настройка системы) и «Network» (Сеть).

Рис. 108 Red Hat 9.0: KDE: Конфигурация сети: Устройства



2 Дважды щелкните по профилю сетевой карты, которую Вы хотите настроить. При этом откроется окно «Ethernet Device — General» (Устройство Ethernet — Общие).

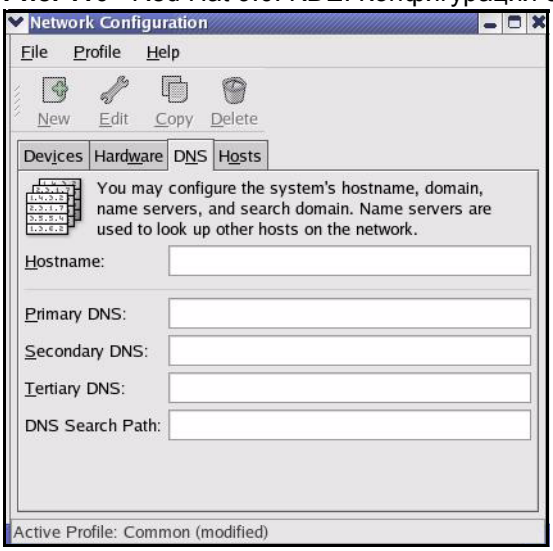
Рис. 109 Red Hat 9.0: KDE: Устройство Ethernet: Общие

- Если у Вас динамический IP-адрес, нажмите «Automatically obtain IP address settings with» (Автоматическое получение IP-адреса через...) и из предложенного списка выберите «DHCP».
- Если у Вас статический IP-адрес, нажмите «Statically set IP Addresses» (Статическое присвоение IP-адреса) и заполните поля «IP address» (IP-адрес), «Subnet mask» (Маска подсети) и «Default gateway» (Шлюз по умолчанию).

3 Нажмите «OK» для сохранения изменений и закройте окно «Ethernet Device — General» (Устройство Ethernet — Общие).

4 Если Вы знаете IP-адрес(а) сервера(ов) DNS, выберите вкладку «DNS» в окне «Network Configuration» (Конфигурация сети). Введите данные серверов DNS в имеющиеся поля.

Рис. 110 Red Hat 9.0: KDE: Конфигурация сети: DNS



5 Выберите закладку «Devices» (Устройства).

6 Щелкните по кнопке «Activate» (Активировать) для вступления изменений в силу. Появится следующее окно. Нажмите «Yes» (Да) для сохранения изменений во всех окнах.

Рис. 111 Red Hat 9.0: KDE: Конфигурация сети: Включить

7 По завершении перезагрузки сетевой карты убедитесь, что «Status» (Статус) = «Active» (Активен) в окне «Network Configuration» (Конфигурация сети).

Использование файлов конфигурации

Для редактирования файлов сетевой конфигурации и настройки IP-адреса Вашего компьютера выполните следующие действия:

1 Предположим, что Ваш компьютер оборудован только одной сетевой картой. Найдите файл конфигурации `ifconfig-eth0` (где `eth0` — имя карты Ethernet). Откройте его с помощью любого текстового редактора.

- Если у Вас динамический IP-адрес, то введите **dhcp** в поле "`BOOTPROTO=`". Пример показан на следующем рисунке.

Рис. 112 Red Hat 9.0: Настройка динамического IP-адреса в файле «ifconfig-eth0»

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- Если у Вас статический IP-адрес, то введите **static** в поле "`BOOTPROTO=`". Введите "`IPADDR=`", затем IP-адрес (в десятичном виде с разделительными точками), "`NETMASK=`" и затем маску подсети. В приведенном ниже примере показан статический IP-адрес = 192.168.1.10 и маска подсети = 255.255.255.0.

Рис. 113 Red Hat 9.0: Настройка статического IP-адреса в файле «ifconfig-eth0»

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 Если Вы знаете IP-адрес(а) Вашего сервера DNS, то введите информацию о сервере DNS в файл `resolv.conf` в каталоге "`/etc`". В следующем примере показан ввод двух IP-адресов сервера DNS.

Рис. 114 Red Hat 9.0: Установка параметров DNS в файле «resolv.conf»

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 После того как Вы отредактируете и сохраните файлы конфигурации, необходимо перезагрузить сетевую карту. Введите "`./network restart`" в каталоге "`/etc/rc.d/init.d`". Пример показан на следующем рисунке.

Рис. 115 Red Hat 9.0: Перезапуск карты Ethernet

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

Проверка настроек

Чтобы проверить настройки TCP/IP, введите `ifconfig` в окне терминала.

Рис. 116 Red Hat 9.0: Проверка свойств протокола TCP/IP

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

E

Всплывающие окна, сценарии и разрешения Java

Чтобы воспользоваться web-конфигуратором, необходимо активировать следующие опции:

- Исходящие от модема всплывающие окна в Интернет-браузере.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (по умолчанию активированы).

Здесь использованы снимки окон Internet Explorer 6.0. Окна в других версиях Internet Explorer могут отличаться.

Блокирование всплывающих окон в Internet Explorer

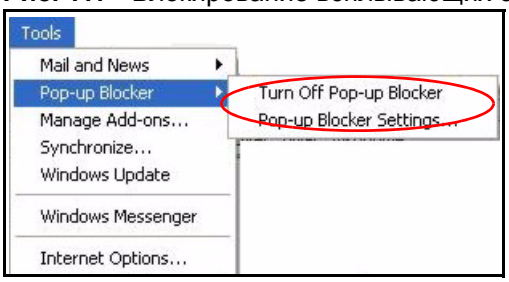
Чтобы зарегистрироваться на Вашем устройстве, Вам возможно придется отключить блокирование всплывающих окон.

Либо отключите блокирование всплывающих окон (в Windows XP SP 2 оно по умолчанию включено), либо разрешите его и создайте исключение для IP-адреса Вашего устройства.

Отключение блокирования всплывающих окон

1 Откройте Internet Explorer, выберите «Tools» (Сервис), «Pop-up Blocker» (Блокирование всплывающих окон) и затем «Turn Off Pop-up Blocker» (Выключить блокирование всплывающих окон).

Рис. 117 Блокирование всплывающих окон



Вы также можете проверить, отключено ли блокирование всплывающих окон в разделе «Pop-up Blocker» (Блокирование всплывающих окон) на закладке «Privacy» (Конфиденциальность).

1. Откройте Internet Explorer, выберите «Tools» (Сервис), «Internet Options» (Свойства обозревателя), «Privacy» (Конфиденциальность).
2. Снимите флажок «Block pop-ups» (Блокировать всплывающие окна) в разделе «Pop-up Blocker» (Блокирование всплывающих окон). Это отключит блокирование всплывающих окон.

Рис. 118 Свойства обозревателя: Конфиденциальность

3. Нажмите кнопку «Apply» (Применить), чтобы сохранить настройки.

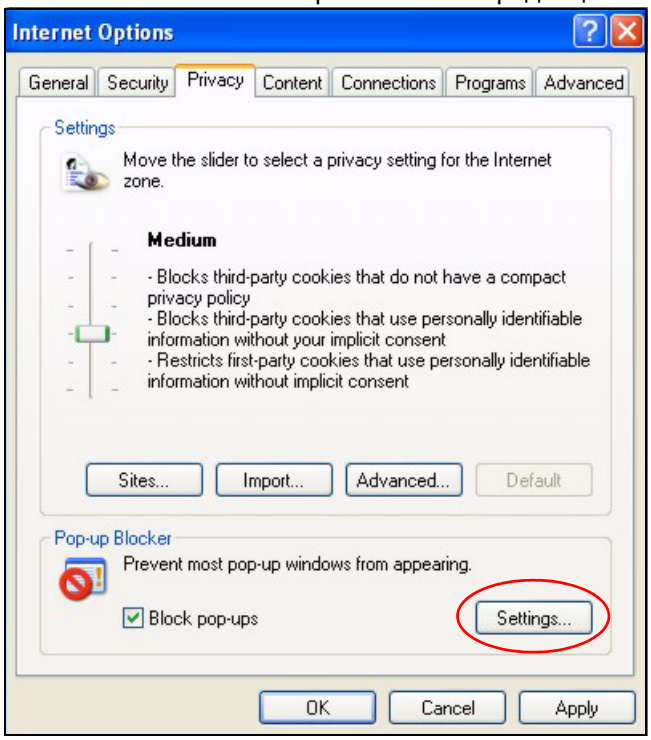
Включение блокировки всплывающих окон с исключениями

Если же Вы хотите, чтобы всплывающие окна были разрешены лишь на Вашем устройстве, то можно сделать следующее.

1. Откройте Internet Explorer, выберите «Tools» (Сервис), «Internet Options» (Свойства обозревателя) и затем закладку «Privacy» (Конфиденциальность).

2 Выберите «Settings…» (Параметры...) – откроется окно «Pop-up Blocker Settings» (Параметры блокирования всплывающих окон).

Рис. 119 Свойства обозревателя: Конфиденциальность



3 Введите IP-адрес вашего устройства (web-страницу, которую вы не хотите блокировать) с префиксом «http://». Например, введите http://192.168.167.1

4 Щелкните «Add» (Добавить) для переноса IP-адреса в список «Allowed sites» (Разрешенные веб-узлы).

Рис. 120 Параметры блокирования всплывающих окон

5 Для возврата на закладку «Privacy» (Конфиденциальность) нажмите кнопку «Close» (Закрыть).

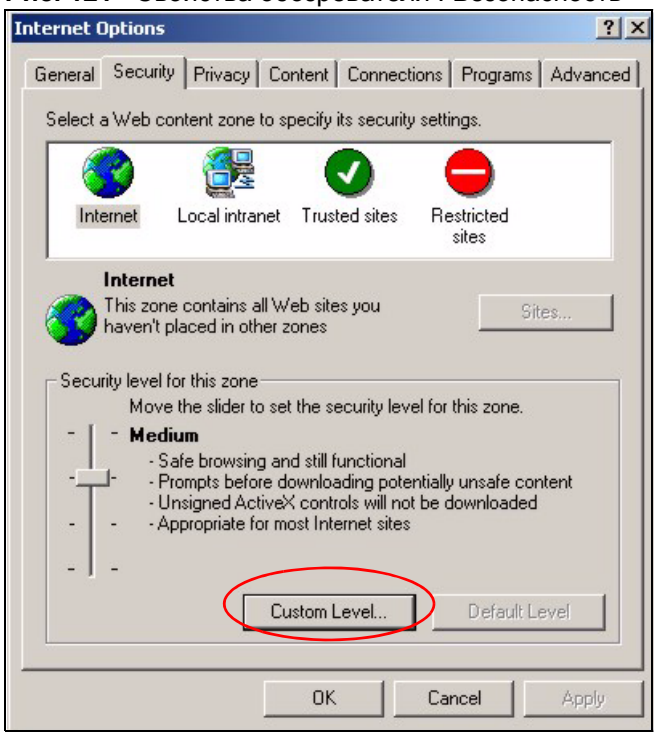
6 Нажмите кнопку «Apply» (Применить), чтобы сохранить настройки.

Сценарии Java (JavaScripts)

Если страницы web-конфигуратора отображаются в Internet Explorer некорректно, проверьте, разрешено ли использование сценариев Java.

1 Откройте Internet Explorer, выберите «Tools» (Сервис), «Internet Options» (Свойства обозревателя) и затем закладку «Security» (Безопасность).

Рис. 121 Свойства обозревателя : Безопасность



2 Нажмите кнопку «Custom Level...» (Другой...).

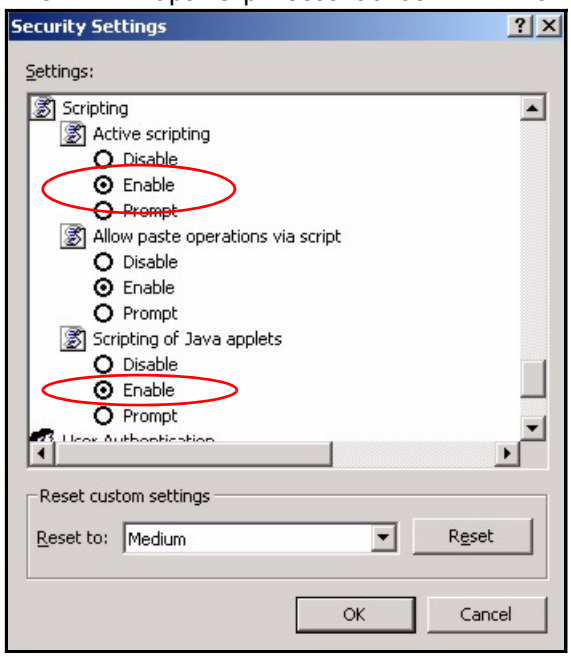
3 Пролистайте до раздела «Scripting» (Сценарии).

4 В разделе «Active scripting» (Активные сценарии) должно быть установлено «Enable» (Разрешить) (значение по умолчанию).

5 В разделе «Scripting of Java applets» (Выполнять сценарии приложений Java) также должно быть установлено «Enable» (Разрешить) (значение по умолчанию).

6 Нажмите «OK», чтобы закрыть окно.

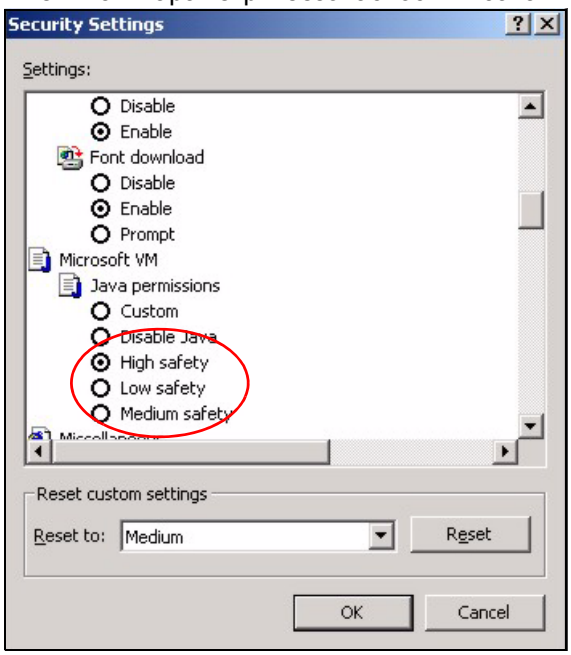
Рис. 122 Параметры безопасности – Выполнение сценариев приложений Java



Разрешения Java

1. Откройте Internet Explorer, выберите «Tools» (Сервис), «Internet Options» (Свойства обозревателя) и затем закладку «Security» (Безопасность).
2. Нажмите кнопку «Custom Level...» (Другой...).
3. Пролистайте до раздела «Microsoft VM».
4. В разделе «Java permissions» (Разрешения Java) выберите уровень безопасности.
5. Нажмите «OK», чтобы закрыть окно.

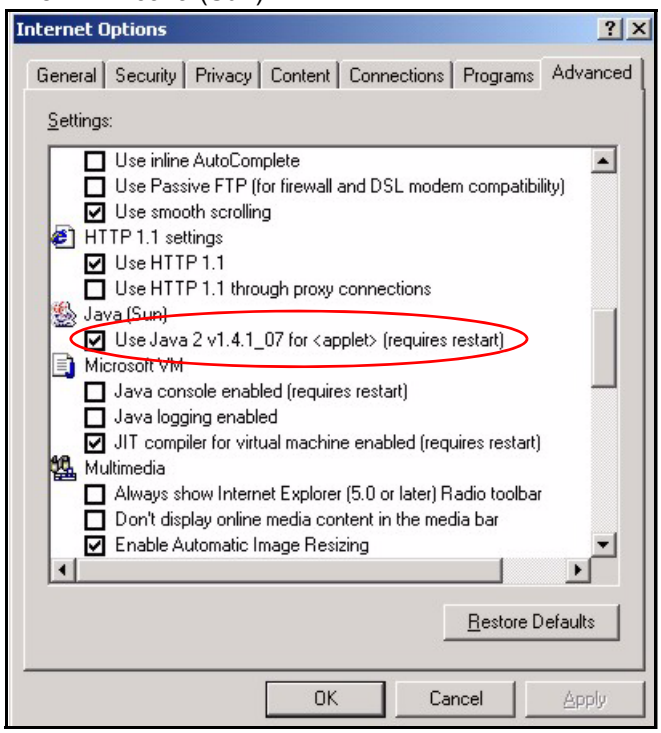
Рис. 123 Параметры безопасности – Java



JAVA (Sun)

1. Откройте Internet Explorer, выберите «Tools» (Сервис), «Internet Options» (Свойства обозревателя) и затем закладку «Advanced» (Дополнительно).
2. Убедитесь, в разделе «Java (Sun)» установлено «Use Java 2 for <applet>» (Использовать Java 2 для приложения).
3. Нажмите «OK», чтобы закрыть окно.

Рис. 124 Java (Sun)



F

IP-адреса и организация подсетей

В этом приложении представлена информация об IP-адресах, и масках подсети.

IP-адрес определяет конкретное устройство в сети. Каждому сетевому устройство (включая компьютеры, серверы, маршрутизаторы, принтеры и т.д.) для обмена информацией по сети требуется IP-адрес. Такие сетевые устройства также называют узлами.

Маска подсети определяет максимальное количество узлов в сети. Также маски подсети используются для разделения сети на несколько подсетей.

Описание IP-адресов

Одна часть IP-адреса является номером сети, а другая часть – номером узла. Так же, как все дома, находящиеся на одной улице, имеют общее название улицы, все узлы в локальной сети имеют общий номер сети. Так же, как каждый дом имеет индивидуальный номер, каждый узет в сети имеет уникальный идентификационный номер - идентификатор узла. Номер сети используется маршрутизаторами при отправке пакетов в соответствующую сеть, а идентификатор узла определяет конкретное устройство в этой сети для доставки этих пакетов.

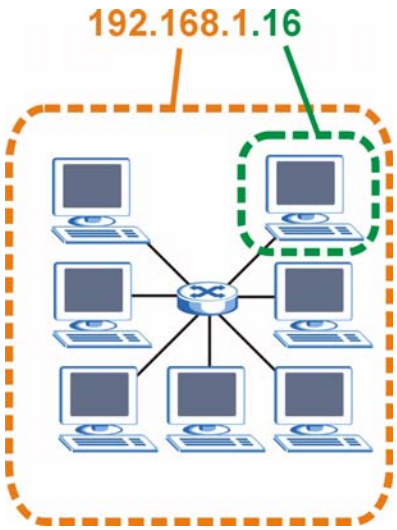
Структура

IP-адрес состоит их четырех частей, записанных в десятичном виде с разделительными точками, например: 192.168.1.1. Каждая из четырех частей называется байтом. Байт – это восьмизначное двоичное число (например, число 11000000 в десятичном представлении равно 192).

Следовательно, каждый байт имеет диапазон возможных значений от 00000000 до 11111111 в двоичном формате, или от 0 до 255 в десятичном.

На следующем рисунке показан пример IP-адреса, в котором три первых байта (192.168.1) являются номером сети, а четвертый байт (16) является идентификатором узла.

Рис. 125 Номер сети и идентификатор узла



Какая часть IP-адреса является номером сети и как идентификатор узла меняется в соответствии с маской подсети.

Маска подсети

С помощью маски подсети можно определить, какие биты являются частью номера сети, а какие – частью идентификатора узла (используя операцию логического «И»). Термин “подсеть” это сокращенное название для “физически независимого сегмента сети”.

Маска подсети состоит из 32 битов. Если бит маски подсети имеет значение “1”, это значит, что соответствующий бит IP-адреса является частью номера сети. Если бит маски подсети имеет значение 0, это значит, что соответствующий бит IP-адреса является частью идентификатора узла.

В следующем примере показаны маска подсети, определяющая номер сети (жирным шрифтом), и идентификатор узла для IP-адреса 192.168.1.2.

Табл. 50 Пример номера сети и идентификатора узла в IP-адресе

	1-Й БАЙТ: (192)	**2-Й БАЙТ: (168)**	**3-Й БАЙТ: (1)**	**4-Й БАЙТ: (2)**
IP-адрес (в двоичной форме)	11000000	10101000	00000001	00000010
Маска подсети (в двоичной форме)	**11111111**	**11111111**	**11111111**	00000000
IPX	**11000000**	**10101000**	**00000001**	
Идентификатор узла				00000010

По договоренности маска подсети всегда состоит из непрерывной последовательности единиц в начале маски (слева), за которой следует непрерывная последовательность нулей общей длиной в 32 бита.

Маски подсети определяют какую часть в адресе составляет номер сети (т.е. биты со значением “1”). Например, “8-битная маска” означает, что первые 8 битов маски являются единицами, а оставшиеся 24 бита – нулями.

Маски подсети записываются в десятичном виде с разделительными точками, так же, как и IP-адреса. В следующем примере показаны 8-битные, 16-битные, 24-битные и 29-бит маски подсети в двоичном и десятичном виде.

Табл. 51 Маска подсети

	ДВОИЧНАЯ ФОРМА				В ДЕСЯТИЧНОМ ВИДЕ
	1-Й БАЙТ:	2-Й БАЙТ:	3-Й БАЙТ:	4-Й БАЙТ:	
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Размер сети определяет максимально возможное число узлов, которое может находиться в сети. Чем больше число битов в номере сети, тем меньше число битов, остающихся для идентификатора узла.

IP-адрес, в котором идентификатор узла состоит только из нулей, является IP-адресом сети (например, 192.168.1.0 с 24-битной маской подсети). IP-адрес, в котором идентификатор узла состоит только из единиц, является широковещательным адресом для этой сети (например, 192.168.1.255 с 24-битной маской подсети).

Поскольку эти два IP-адреса нельзя использовать для отдельных узлов, максимально возможное число узлов в сети рассчитывается следующим образом:

Табл. 52 Максимальное число узлов

МАСКА ПОДСЕТИ		РАЗМЕР ИДЕНТИФИКАТОРА УЗЛА В АДРЕСЕ		МАКСИМАЛЬНОЕ ЧИСЛО УЗЛОВ
8 бита	255.0.0.0	24 бита	$2^{24} – 2$	16777214
16 бита	255.255.0.0	16 бита	$2^{16} – 2$	65534
24 бита	255.255.255.0	8 бита	$2^{8} – 2$	254
29 бита	255.255.255.248	3 бита	$2^{3} – 2$	6

Записи маски подсети

Поскольку маска всегда состоит из непрерывной последовательности сначала единиц и затем непрерывной последовательности нулей общей длиной 32 бита, можно просто указывать количество единиц вместо того, чтобы определять значение каждого байта. Это обычно обозначается путем записи после адреса символа “/” и количества бит с единицами.

Например, запись 192.1.1.0 /25 равносильна зпаиси 192.1.1.0 с маской подсети 255.255.255.128.

В следующей таблице показаны несколько масок подсети с использованием обоих видов записи.

Табл. 53 Альтернативные варианты записи маски подсети

МАСКА ПОДСЕТИ	АЛЬТЕРНАТИВНАЯ ЗАПИСЬ	ПОСЛЕДНИЙ БАЙТ (В ДВОИЧНОЙ ФОРМЕ)	ПОСЛЕДНИЙ БАЙТ (В ДЕСЯТИЧНОЙ ФОРМЕ)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

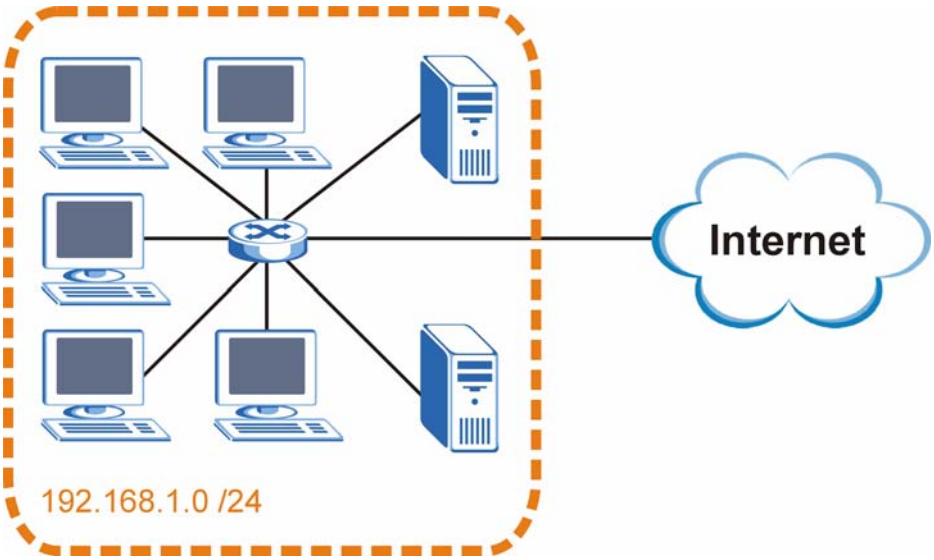
Организация подсетей

Маски подсети также используются для разделения сети на несколько подсетей. В следующем примере сетевой администратор 2 подсети, чтобы изолировать группу серверов от остальной сети компании в целях безопасности.

В этом примере адрес сети компании – 192.168.1.0. Первые 3 байта адреса (192.168.1) являются номером сети, а оставшийся байт является идентификатором узла, следовательно, макимальное число узлов в этой сети равно $2^8 – 2$ или 254.

На следующем рисунке показана сеть компании до разделения на подсети.

Рис. 126 Пример организации подсетей: до разделения на подсети

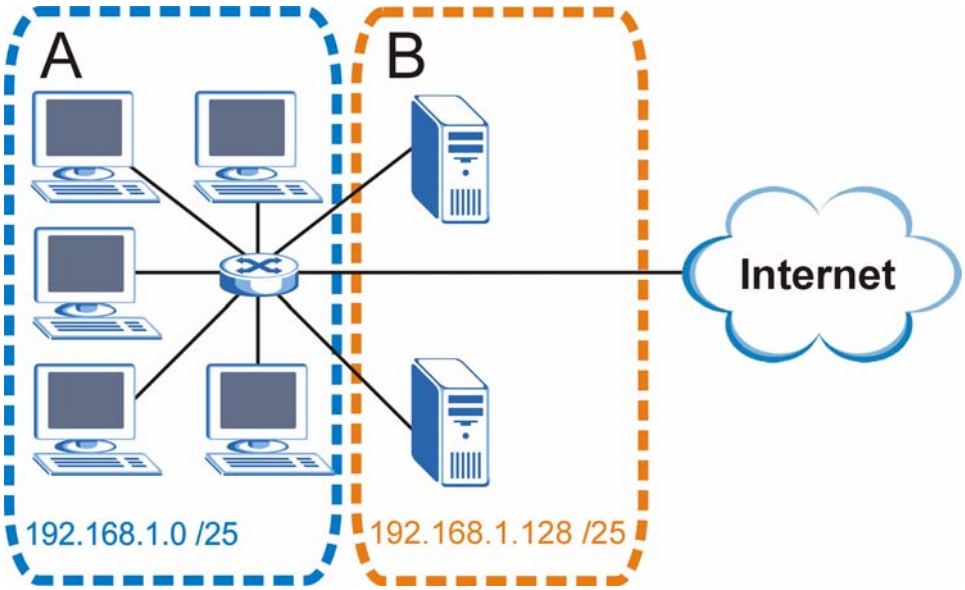


Можно “занять” один бит идентификатора узла для разделения сети 192.168.1.0 на две отдельные подсети. Маска подсети состоит теперь из 25 битов (255.255.255.128 или /25).

«Заимствованный» бит идентификатора узла может принимать значения 0 или 1, давая, таким образом, две подсети; 192.168.1.0 /25 и 192.168.1.128 /25.

На следующем рисунке показана сеть компании после разделения на подсети. Теперь организовано две подсети, **A** и **B**.

Рис. 127 Пример организации подсетей: после разделения на подсети



При 25-битной маске подсети в идентификаторе узла остается 7 битов, следовательно, максимальное число узлов в каждой подсети равно $2^7 - 2$ или 126 (идентификатор узла, состоящий только из нулей является адресом самой подсети, а состоящий только из единиц – широковещательным адресом этой подсети).

Адрес 192.168.1.0 с маской 255.255.255.128 определяет подсеть **A**, а 192.168.1.127 с маской 255.255.255.128 является ее широковещательным адресом. Следовательно, самый младший IP-адрес, который может быть назначен действительному узлу для подсети **A** – 192.168.1.1, а старший – 192.168.1.126.

Подобным образом рассчитывается диапазон идентификаторов узлов для подсети **B**: от 192.168.1.129 до 192.168.1.254.

Пример: Четыре подсети

В предыдущем примере продемонстрировано использование 25-битной маски подсети для разделения 24-битного адреса на две подсети. Аналогично для разделения 24-битного адреса на четыре подсети, потребуется «заимствовать» два бита из идентификатора узла для получения четырех возможных комбинаций: 00, 01, 10 и 11. Маска подсети имеет 26 бит (11111111.11111111.11111111.**11**000000) или 255.255.255.192.

Каждая подсеть имеет 6 битов для идентификатора узла, при этом получается 2^6 — 2 или 62 узла в каждой подсети (все нули в индентификаторе узла обозначают саму подсеть, все единицы являются широковещательным адресом этой подсети).

Табл. 54 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес (в десятичной форме)	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**00**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.0	Минимальный идентификатор узла: 192.168.1.1	
Адрес широковещательной рассылки: 192.168.1.63	Максимальный идентификатор узла: 192.168.1.62	

Табл. 55 Подсеть 2

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	64
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**01**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.64	Минимальный идентификатор узла: 192.168.1.65	
Адрес широковещательной рассылки: 192.168.1.127	Максимальный идентификатор узла: 192.168.1.126	

Табл. 56 Подсеть 3

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	128
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**10**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.128	Минимальный идентификатор узла: 192.168.1.129	
Адрес широковещательной рассылки: 192.168.1.191	Максимальный идентификатор узла: 192.168.1.190	

Табл. 57 Подсеть 4

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	192
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**11**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.192	Минимальный идентификатор узла: 192.168.1.193	
Адрес широковещательной рассылки: 192.168.1.255	Максимальный идентификатор узла: 192.168.1.254	

Пример: Восемь подсетей

Аналогично используется 27-битная маска для создания 8 подсетей (000, 001, 010, 011, 100, 101110111).

В следующей таблице приведены значения битов последнего байта IP-адреса для каждой подсети.

Табл. 58 Восемь подсетей

ПОДСЕТЬ	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКОВЕЩАТЕЛЬНЫЙ АДРЕС
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Проектирование подсетей

В следующей таблице представлена сводка для проектирования подсетей в сети с 24-битным номером сети.

Табл. 59 Проектирование подсетей в сети с 24-битным номером сети

КОЛИЧЕСТВО “ЗАИМСТВОВАННЫХ” БИТОВ ИДЕНТИФИКАТОРА УЗЛА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО УЗЛОВ В КАЖДОЙ ПОДСЕТИ
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

В следующей таблице представлена сводка для проектирования подсетей в сети с 16-битным номером сети.

Табл. 60 Проектирование подсетей в сети с 16-битным номером сети

КОЛИЧЕСТВО “ЗАИМСТВОВАННЫХ” БИТОВ ИДЕНТИФИКАТОРА УЗЛА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО УЗЛОВ В КАЖДОЙ ПОДСЕТИ
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Настройка IP-адресов

Номер сети зависит от конкретной ситуации. Если Интернет-провайдер или сетевой администратор назначают блок зарегистрированных IP-адресов, то они также дадут инструкции по выбору IP-адреса и маске подсети.

Если Интернет-провайдер не предоставляет этих данных в явной форме, то вероятнее всего он назначает динамический IP-адрес при установлении соединения. В этом случае рекомендуется установить IP-адрес в диапазоне от 192.168.0.0 до 192.168.255.0. Агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало этот диапазон специально для частного использования. Если явно не предписано использовать другие адреса, не следует использовать номера за пределами этого диапазона. Необходимо также включить функцию «NAT» (Network Address Translation – трансляция сетевых адресов) в P660RT2.

Выбрав номер сети, выберите для P660RT2 IP-адрес, который легко запоминается, например, 192.168.1.1, но убедитесь, что никакое другое устройство в вашей сети не использует этот IP-адрес.

Маска подсети определяет сетевую часть IP-адреса. P660RT2 автоматически рассчитывает маску подсети для заданного IP-адреса. Нельзя изменять маску подсети, вычисленную P660RT2, без прямых указаний.

IP-адреса для частных сетей

Каждая машина в Интернете должна иметь свой уникальный адрес. Если сеть изолирована от Интернета, например, соединяет между собой локальные сети двух филиалов, можно без проблем назначать узлам произвольные IP-адреса. Тем не менее, Агенство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало следующие три блока IP-адресов специально для частных сетей:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

IP-адрес может быть получен от IANA, от Интернет-провайдера или может быть назначен частной сетью. Если ваша организация относительно небольшая, и доступ в Интернет осуществляется через Интернет-провайдера, Интернет-провайдер может предоставить адреса Интернета для ваших локальных сетей. С другой стороны, если организация является частью большой компании, следует проконсультироваться с сетевым администратором по поводу назначения IP-адресов.

Независимо от конкретной ситуации не стоит назначать произвольные IP-адреса; лучше следовать приведенным выше указаниям. Для получения более подробной информации по назначению адресов см. RFC 1597, *Address Allocation for Private Internets* и RFC 1466, *Guidelines for Management of IP Address Space.*

G

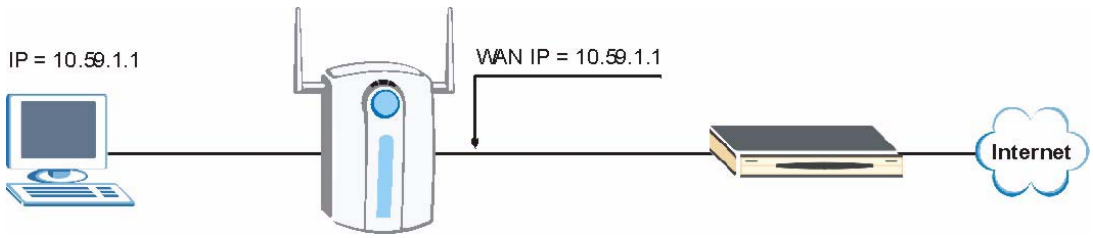
Конфликты при назначении IP-адресов

В этом приложении описываются ситуации возникновения конфликтов IP-адресов. Абоненты с одинаковыми IP-адресами не смогут получить доступ в Интернет.

Случай A: В модеме P660RT2 используются одинаковые IP-адреса в глобальной и локальной сети

На следующем рисунке представлен пример, где в P660RT2 используется IP-адрес порта WAN, идентичный IP-адресу компьютера в локальной сети.

Рис. 128 Конфликт IP-адресов: Случай A

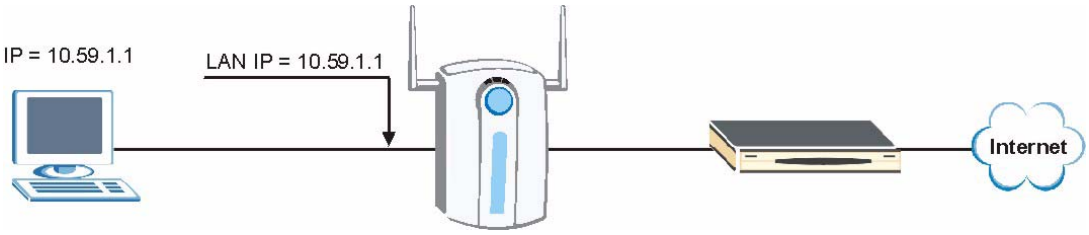


Нелбходимо настроить P660RT2 на использование различных глобального и локального IP-адресов, находящихся в различных подсетях, если включен сервер DHCP в P660RT2. Например, установите IP-адрес в глобальной сети 192.59.1.1, а IP-адрес в локальной сети – 10.59.1.1. То есть, для P660RT2 рекомендуется использовать общедоступный IP-адрес в глобальной сети.

Случай B: IP-адрес порта LAN P660RT2 совпадает с IP-адресом клиента DHCP

На следующем рисунке P660RT2 выступает в качестве сервера DHCP. Модем P660RT2 назначает клиенту DHCP такой же IP-адрес, как и IP-адрес порта LAN, к которому подключен этот клиент.

Рис. 129 Конфликт IP-адресов: Случай B

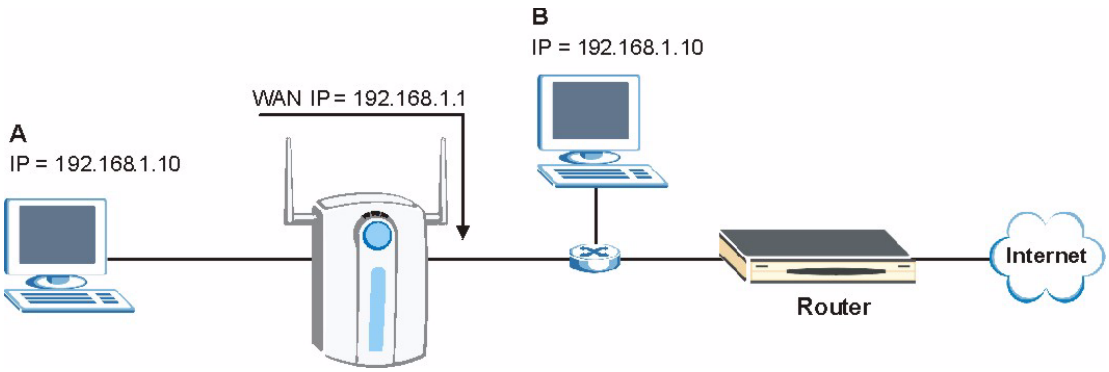


Для разрешения этой проблемы убедитесь, что IP-адрес порта LAN P660RT2 не находится в диапазоне непрерывных IP-адресов DHCP.

Случай C: IP-адрес компьютера совпадает с IP-адресом сетевого устройства

На следующем рисунке представлен пример, где IP-адрес клиентского компьютера совпадает с IP-адресом сетевого устройства, не подключенного к P660RT2

Рис. 130 Конфликт IP-адресов: Случай C



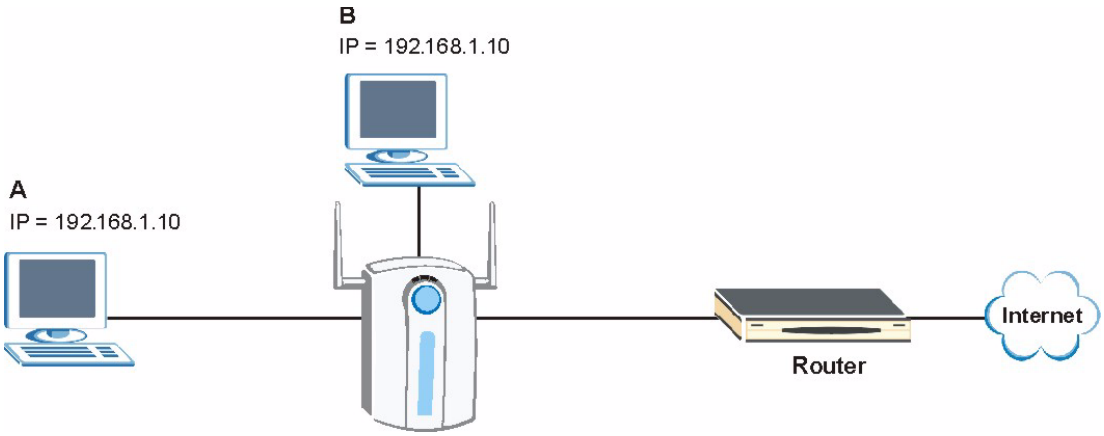
Нелбходимо настроить P660RT2 на использование различных глобального и локального IP-адресов, находящихся в различных подсетях, если включен сервер DHCP в P660RT2. Например, установите IP-адрес в глобальной сети 192.59.1.1, а IP-адрес в локальной сети – 10.59.1.1. То есть, для P660RT2 рекомендуется использовать общедоступный IP-адрес в глобальной сети.

Случай D: Два или более компьютеров имеют одинаковые IP-адреса.

С помощью преобразования всех частных IP-адресов в IP-адрес глобальной сети, P660RT2 позволяет компьютерам с различными сетевыми конфигурациями получить доступ в Интернет Однако существуют ситуации, когда два или более абонентов используют одинаковый частный IP-адрес. Это может произойти в том случае, если компьютер настроен на использование статического (фиксированного) IP-адреса, идентичного IP-адресу, который сервер DHCP P660RT2 назначает другому компьютеру, являющемуся клиентом DHCP.

В этом случае абоненты не смогут получить доступ в Интернет.

Рис. 131 Конфликт IP-адресов: Случай D



Эта проблема может быть решена при помощи установки коммутатора VLAN или настройкой компьютеров на получение динамических IP-адресов.

H

Службы Интернет

В следующей таблице приводятся распространенные службы и связанные с ними протоколы и номера портов. Для получения полного списка номеров портов, номеров типа/кода ICMP и служб, посетите web-сайт IANA (Internet Assigned Number Authority – Агентство по назначению имен и уникальных параметров протоколов Интернет).

- **Имя**: короткое описательное имя службы. Можно использовать это имя или создать другое.
- **Протокол**: тип протокола протокол IP, используемый для данной службы. Если используется **TCP/UDP**, то служба использует одинаковый с TCP и UDP номер порта. Если используется «USER-DEFINED» (определяется пользователем), параметр «Port(s)» Порт(ы) является номером протокола IP, не номером порта.
- **Порт(ы)**: значение зависит от параметра **Протокол**. Дополнительную информацию по номерам портов можно получить в RFC 1700.
  - Если значение **Протокола** – **TCP**, **UDP**, или **TCP/UDP**, то это номер порта IP.
  - Если значение **Протокола** – **USER**, то это номер протокола IP.
- **Описание**: краткое описание приложений, которые используют данную службу, или ситуацией, в которых используется данная служба.

Табл. 61 Наиболее часто используемые службы

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	определяется пользователем	51	Эту службу использует протокол туннелирования IPSEC AH (Заголовк аутентификации).
AIM/New-ICQ	TCP	5190	Служба Internet Messenger AOL. Она также использует порт прослушивания для ICQ.
AUTH	TCP	113	Протокол аутентификации, используется некоторыми серверами.
BGP	TCP	179	Протокол BGP (пограничный межсетевой протокол).
BOOTP_CLIENT	udp	68	Клиент DHCP.
BOOTP_SERVER	udp	67	Сервер DHCP.
CU-SEEME	TCP udp	7648 24032	Популярное решение для видеоконференцсвязи от White Pines Software.
DNS	TCP/UDP	53	Сервер имен доменов – служба, определяющая соответствие web-имен (например, www.zyxel.com) и номеров IP.

Табл. 61 Наиболее часто используемые службы (продолжение)

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
ESP (IPSEC_TUNNEL)	определяется пользователем	50	Эту службу использует протокол туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).
FINGER	TCP	79	Finger – команда для UNIX или Интернет, используемая для проверки нахождения пользователя в сети.
FTP	TCP TCP	20 21	Протокол передачи файлов, программа для быстрой передачи файлов, в том числе файлов большого размера, которые невозможно пересылать средствами электронной почты.
H.323	TCP	1720	Протокол для Net Meeting.
HTTP	TCP	80	Протокол передачи гипертекста - протокол клиент/сервер для "Всемирной паутины".
HTTPS	TCP	443	HTTPS - это надежный сеанс связи http, часто используемый в электронной коммерции.
ICMP	определяется пользователем	1	Internet Control Message Protocol (Протокол межсетевых управляющих сообщений) часто используется в целях диагностики и маршрутизации.
ICQ	udp	4000	Популярная система интерактивного общения в Интернет.
IGMP (многоадресная рассылка)	определяется пользователем	2	Internet Group Multicast Protocol (Широковещательный протокол взаимодействия групп в сети Интернет) используется для отпраки пакетов определенным группам узлов.
IKE	udp	500	Алгоритм обмена ключами в Интернет, используется для распределения и управления ключами.
IRC	TCP/UDP	6667	Еще одна программа интерактивного общения в Интернет.
MSN Messenger	TCP	1863	Протокол для передачи сообщений в сетях Microsoft.
NEW-ICQ	TCP	5190	Программа для обмена текстовыми сообщениями между абонентами сети Internet в реальном времени.
NEWS	TCP	144	Протокол для групп новостей.
NFS	udp	2049	Сетевая файловая система – NFS, распределенная файловая служба клиент/сервер, обеспечивающая прозрачное совместное использование файлов в сети.
NNTP	TCP	119	Network News Transport Protocol (Сетевой протокол передачи новостей) – система доставки для групп новостей USENET.

Табл. 61 Наиболее часто используемые службы (продолжение)

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
PING	определяется пользователем	1	Packet INternet Groper (Программа для отправки пакетов Интернет) – протокол отправки эхо-запроса ICMP для проверки доступности удаленного узла.
POP3	TCP	110	Почтовый протокол версии 3, позволяет клиентскому компьютеру получать электронную почту с сервера POP3, используя временное соединение (TCP/IP или другое).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol (Протокол тунелирования "точка-точка") обеспечивает безопасную передачу данных в общедоступных сетях. Это канал управления.
PPTP_TUNNEL (GRE)	определяется пользователем	47	PPTP (Point-to-Point Tunneling Protocol – Протокол тунелирования "точка-точка") обеспечивает безопасную передачу данных в общедоступных сетях. Это канал передачи данных.
RCMD	TCP	512	Удаленное управление командной строкой.
REAL_AUDIO	TCP	7070	Система прямого воспроизведения звука, обеспечивает передачу аудиопотоков в сети в реальном времени.
REXEC	TCP	514	Daemon-служба удаленного выполнения команд.
RLOGIN	TCP	513	Удаленная регистрация.
RTELNET	TCP	107	Удаленный доступ через Telnet.
RTSP	TCP/UDP	554	Протокол (Real Time Streaming – Протокол воспроизведения в реальном времени) - это удаленное управление для мультимедиа в Интернете.
SFTP	TCP	115	Простой протокол передачи файлов.
SMTP	TCP	25	Simple Mail Transfer Protocol (Простой протокол электронной почты) – стандартный протокол обмена сообщениями для сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой.
Протокол SNMP	TCP/UDP	161	Simple Network Management Program (Простой протокол управления сетью).
SNMP-TRAPS	TCP/UDP	162	Прерывания для совместного использования с SNMP (RFC:1215).

Табл. 61 Наиболее часто используемые службы (продолжение)

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
SQL-NET	TCP	1521	Structured Query Language (Язык структурированных запросов) представляет собой интерфейс для доступа к данным на различных типах систем баз данных, включая универсальные вычислительные машины, системы средней производительности, системы UNIX и сетевые серверы.
SSH	TCP/UDP	22	Программа для обеспечения безопасной удаленной регистрации.
STRM WORKS	udp	1558	Протокол передачи данных.
SYSLOG	udp	514	Syslog (Системный журнал) позволяет отправлять системные журналы на сервер UNIX.
TACACS	udp	49	Login Host Protocol (Протокол регистрации узла), используется для TACACS (Terminal Access Controller Access Control System – Система управления доступом на основе контроллера доступа к терминалу).
Сетевой теледоступ (Telnet)	TCP	23	Telnet - это протокол регистрации и эмуляции терминала, общий для среды Интернета и UNIX. Он работает в сетях TCP/IP. Его основная функция - разрешить пользователям регистрацию на удаленном узле.
TFTP	udp	69	Trivial File Transfer Protocol (Упрощенный протокол передачи файлов) – это протокол передачи файлов в Интернет, подобный FTP, но использующий UDP (Протокол передачи дейтаграмм пользователя), а не TCP (Протокол управления передачей).
VDOLIVE	TCP	7000	Еще одна программа для видеоконференций.

I

Интерпретатор команд

Ниже приводятся инструкции по работе с интерпретатором команд. Более подробную информацию об этих командах можно найти на компакт-диске, входящем в комплект поставки или на web-сайте zyxel.com.

Использование не описанных в документации команд или неправильная настройка могут повредить устройство или полностью вывести его из строя.

Доступ через Telnet

Чтобы подключиться к P660RT2 с помощью Telnet, выполните следующие действия:

1. Убедитесь, что компьютер физически подключен к одному из портов LAN.
2. Убедитесь, что IP-адрес компьютера и IP-адрес коммутатора принадлежат одной подсети. В Windows нажмите кнопку «Start» (Пуск) (как правило, в левом нижнем углу), «Run» (Выполнить), затем введите `telnet 192.168.1.1` (IP-адрес для управления по умолчанию) и нажмите кнопку «OK».
3. На экране появится окно регистрации. Введите пароль администратора (пароль по умолчанию – «1234»).

Синтаксис команд

- Ключевые слова команд выделены шрифтом `courier new`.
- Вводить ключевые слова команды следует в точности как показано ниже, без сокращений.
- Обязательные поля команды заключаются в угловые скобки <>.
- Необязательные поля команды заключаются в квадратные скобки `[]`.
- Символ `|` означает "или".

  Например:

  sys filter netbios config <type> <on|off>

  означает, что необходимо указать тип фильтра NetBIOS и включить либо отключить его.

Использование команд

Для отображения списка доступных команд введите `help` или `?` в командной строке. Команду всегда следует вводить полностью. Введите `exit` для завершения сеанса.

Примеры команд

В этом разделе представлено несколько примеров команд, которые используются в P660RT2. Эти примеры предназначены только для справки. Команды, доступные в конкретной модели P660RT2 могут отличаться от приведенных здесь. Более подробно см. в других приложениях. Команда "routing"

Синтаксис: `ip nat routing [0:LAN] [0:no|1:yes]`

С помощью этой команды можно настроить P660RT2 на маршрутизацию трафика, не соответствующего правилу NAT, через конкретный интерфейс. Примером такой ситуации может служить наличие серверов с общедоступными IP-адресами, которые подключены к локальной сети.

В следующем примере такая команда настраивает P660RT2 на маршрутизацию трафика, не соответствующего правилу NAT, через интерфейс LAN.

Рис. 132 Пример команды "routing"

```
ras> ip nat routing 2 0
Маршрутизация будет выполняться при NAT, даже если ни одно
правило NAT не соблюдается.
-----------------------------------------------
         LAN: yes
```

Режим работы ARP и команды "ARP ackGratuitous"

модем P660RT2 не принимает информацию в ответе ARP, если прежде P660RT2 не посылал соответствующий запрос. Это помогает предотвратить обновление таблицы ARP в P660RT2 неправильными отображениями IP-адресов на MAC-адреса вследствие использования ложного ARP. Неправильное отображение IP-адреса на MAC-адрес в таблице ARP P660RT2 приводит к тому, что P660RT2 посылает пакеты чужому устройству.

Команды для использования и игнорирования намеренных запросов ARP

Узел может посылать запрос ARP для разрешения своего IP-адреса. Такаой запрос называется намеренным запросом ARP. В пакете используется собственный IP-адрес узла в качестве IP-адреса источника и IP-адреса назначения. В пакете используется широковещательный адрес Ethernet (FF:FF:FF:FF:FF:FF) в качестве MAC-адреса назначения. Это используется для определения, есть ли в сети узел, который имеет такой же IP-адрес, как и у узла, отправителя запроса. Другие узлы в сети также могут обновить отображение IP-адреса на MAC-адрес этого узла в свей таблице ARP.

Команды `ip arp ackGratuitous` устанавливают, как модем P660RT2 обрабатывает намеренные запросы ARP.

- Команда `ip arp ackGratuitous active no` действует так, что P660RT2 игнорирует намеренные запросы ARP.
- Команда `ip arp ackGratuitous active yes` действует так, что P660RT2 отвечает на намеренные запросы ARP.

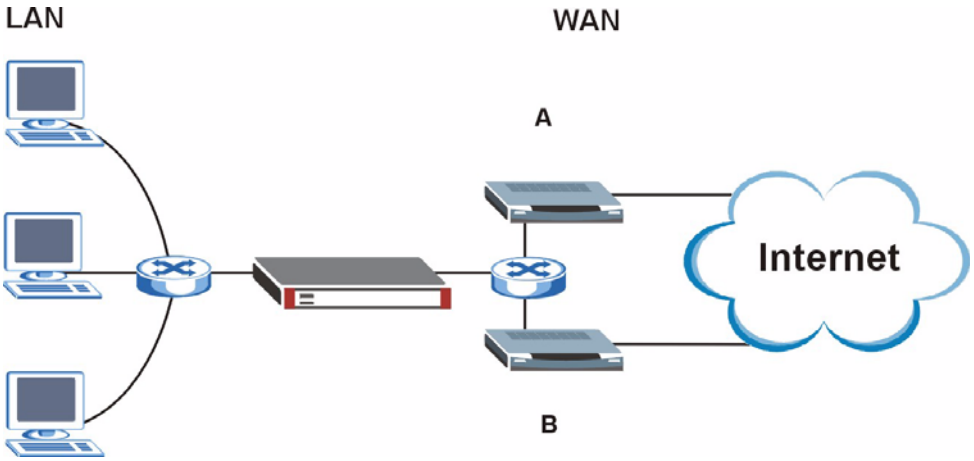
  Например, если стандартный шлюз выходит из строя, резервный шлюз посылает намеренный запрос ARP. Если в этом запросе содержится IP-адрес, которого еще нет в таблице ARP P660RT2, то P660RT2 посылает запрос ARP, чтобы определить, узел, использующий этот IP-адрес. После того, как P660RT2 получит ответ от резервного шлюза, он добавит новую запись в свою таблицу ARP.

  Если в таблице ARP P660RT2 уже содержится запись с таким IP-адресом, ответ P660RT2 зависит от параметров команды `ip arp ackGratuitous forceUpdate`.

  - Команда `ip arp ackGratuitous forceUpdate on` используется, чтобы P660RT2 обновлял MAC-адрес в записи ARP.
  - Команда `ip arp ackGratuitous forceUpdate` off используется, чтобы P660RT2 не обновлял MAC-адрес в записи ARP.

Резервный шлюз (как показано на следующем рисунке) служит примером, когда требуется включить принудительное обновление при намеренных запросах ARP. Однажды шлюз A выходит из строя, и резервный шлюз (B) включается в работу с использованием того же статического IP-адреса, как был у шлюза A. Шлюз B передает широковещательный намеренный запрос ARP, чтобы узнать, какой узел использует этот IP-адрес. Если команда "ackGratuitous" включает принудительное обновление, P660RT2 принимает намеренный запрос ARP и обновляет свою таблицу ARP. В этом случае в P660RT2 содержится правильная запись ARP для шлюза, и устройство посылает пакеты через резервный шлюз. Если команда ackGratuitous отключает принудительное обновление, P660RT2 не обновляет запись ARP для шлюза и не может отправлять пакеты через шлюз B.

Рис. 133 Backup Gateway (Резервный шлюз)



При обновлении записей ARP повышается риск атак с имитацией законного пользователя. Рекомендуется включать принудительное обновление с помощью комады "ackGratuitous", только если это необходимо, как в предыдущем примере с резервным шлюзом. Включение принудительного обновления является гораздо более опасным, чем отключение, так как P660RT2 обновляет таблицу ARP даже при существующей записи.

Настройка длины ключа для фазы 2 шифрования IPSec AES

Синтаксис: `ipsec ipsecConfig encryKeyLen <0:128 | 1:192 | 2:256>`

По умолчанию в P660RT2 используется ключ шифрования AES длиной 128 бит для фазы 2 туннелей IPSec. Эта команда используется для изменения существующего правила VPN с целью использовать большую длину ключа шифрования AES.

См. следующий пример. Существует правило VPN, где используется AES для шифрования фазы 2 и требуется, чтобы в нем использовалось шифрование 192 бит.

- Команда в первой строке используется, чтобы начать редактирование правила VPN.
- Команда во второй строке устанавливает в правиле VPN использование AES 192 бита для фазы 2 шифрования.
- Команда в третьей строке отображает результаты.

Рис. 134 Пример команды "routing"

```
ras> ipsec ipsecEdit 1
ras> ipsec ipsecConfig encryKeyLen 1
ras> ipsec ipsecDisplay
---------- IPSec Setup ----------
Index #= 1     Active= No    Multi Pro = No    Protocol= 0 Global SW= 0xA
Bound IKE 9999   NailUp = No   Netbios = No   Name= test

ControlPing = No  LogControlPing = No  Control ping address = 0.0.0.0
Local:  Addr Type= SINGLE      Port Start= 0         End= N/A
        IP Addr Start= 0.0.0.0              Mask= N/A
Remote: Addr Type= SINGLE      Port Start= 0         End= N/A
        IP Addr Start= 0.0.0.0              Mask= N/A
Enable Replay Detection= No    Key Management= IKE
Phase 2 - Active Protocol= ESP
          Encryption Algorithm= AES    Authentication Algorithm= SHA1
          Encryption Key Length = 192
          SA Life Time (Seconds)= 28800
          Encapsulation= Tunnel   Perfect Forward Secrecy (PFS)= None
ras>
```

J

Правовая информация

Авторское право

Авторское право © 2006. Издано ZyXEL Communications Corporation.

Содержимое данного издания не может быть воспроизведено целиком или частично, переписано, помещено в систему поиска информации, переведено на любой язык или передано в любой форме при помощи любых средств, электронным, механическим, магнитным, оптическим, химическим, путем фотокопирования, вручную или любым другим способом, без предварительного письменного разрешения ZyXEL Communications Corporation.

Издано ZyXEL Communications Corporation. Все права защищены.

Непризнание иска

Корпорация ZyXEL не принимает на себя ни в какой форме ответственность за применение или использование любого изделия или программного обеспечения, описанного в данном руководстве пользователя. Корпорация ZyXEL также не предоставляет никаких лицензий на свои патентные права, а также на патентные права третьих сторон. Кроме того, корпорация ZyXEL сохраняет за собой право вносить изменения в любые описываемые в данном документе изделия без дополнительного уведомления. Информация в этом руководстве также может быть изменена без специального уведомления.

Торговая марка

ZyNOS (ZyXEL Network Operating System — Сетевая операционная система ZyXEL) является зарегистрированной торговой маркой ZyXEL Communications, Inc. Торговые марки, упомянутые в данном издании, используются только в целях идентификации и являются собственностью своих законных владельцев.

Сертификация

Заключение FCC по помехам

Данное устройство соответствует Части 15 Правил FCC. Работа оборудования отвечает следующим двум условиям:

- Данное устройство не может являться причиной недопустимых помех.
- Данное устройство должно быть устойчивым к помехам, включая помехи, которые могут вызвать нежелательные действия.

Данное оборудование было протестировано и признано соответствующим ограничениям для цифровых приборов Класса B согласно Правилам FCC, Часть 15. Данные ограничения разработаны для обеспечения разумной защиты против недопустимых помех при коммерческом использовании. В данном устройстве генерируется и используется высокочастотное излучение, которое может стать причиной недопустимых помех при радиосвязи, при неправильной установке и использовании устройства. Корпорация ZyXEL не дает гарантии, что помехи будут отсутствовать при установке устройства в специфических условиях.

Если данное устройство является причиной недопустимых помех при приеме теле/радиопередач, что можно определить путем выключения и включения устройства, то пользователь может попробовать снизить уровень помех с помощью следующих мер:

1. Переориентировать или переместить приемную антенну.
2. Увеличить расстояние между оборудованием и приемным устройством.
3. Подключить устройство и приемник к розеткам различным контуров сети электропитания.
4. Обратиться за помощью к дилеру или опытному теле- или радиотехнику.

Замечания

Изменения или модификации, не одобренные явным образом стороной, ответственной за соблюдение соответствия, могут стать причиной лишения пользователя права работать с оборудованием.

Данное цифровое устройство класса B соответствует канадскому стандарту ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Просмотр сертификатов

1. Перейдите по ссылке http://www.zyxel.com.
2. Выберите свое изделие на домашней странице ZyXEL и перейдите на страницу, посвященную этому изделию.
3. Выберите на этой странице нужный сертификат для просмотра.

Ограниченная гарантия корпорации ZyXEL

Корпорация ZyXEL гарантирует легальному конечному пользователю (покупателю), что данное изделие не имеет и в течение периода до двух лет со дня покупки не будет иметь дефектов, связанных с использованными материалами и производственным браком. В течение гарантийного периода и по подтверждении покупки, если изделие имеет признаки неисправности, связанные с производственным браком и/или использованными материалами, корпорация ZyXEL будет, по своему выбору, ремонтировать или заменять дефектные изделия или комплектующие без оплаты деталей или стоимости работы, а также всего того, что окажется необходимым для восстановления надлежащего режима работы изделия или комплектующих. Любая замена может включать как новые, так и восстановленные функционально эквивалентные изделия аналогичной или более высокой стоимости; выбор в данном

случае остается за корпорацией ZyXEL. Данные гарантийные обязательства не распространяются на случаи, когда изделие было вскрыто, модифицировано, использовано не по назначению, повреждено в результате форс-мажорных обстоятельств или неправильных условий эксплуатации.

Примечание

Покупатель, согласно данным гарантийным обязательствам, может рассчитывать только на ремонт или замену. Данные гарантийные обязательства заменяют собой все прочие гарантийные обязательства, явные или неявные, включая любые неявные гарантийные обязательства в отношении годности для продажи или решения конкретных целей и задач. Корпорация ZyXEL не несет никакой ответственности перед покупателем за косвенные убытки любого олда.

Для получения обслуживания по данным гарантийным обязательствам следует связаться с Сервисным центром ZyXEL; информация о номере разрешения на возврат (RMA) содержится в Гарантийном талоне на данное оборудование. Изделия должны быть возвращены с предварительно оплаченным почтовым сбором. Рекомендуется застраховать каждое устройство на период пересылки. Изделия, возвращенные без документов, подтверждающих факт покупки или с просроченной гарантией, будут отремонтированы или заменены (по усмотрению корпорации ZyXEL), и клиенту будет выставлен счет на оплату работ и деталей. Все отремонтированные или замененные изделия будут отправлены корпорацией ZyXEL по соответствующему обратному адресу с оплаченным почтовым сбором. Данные гарантийные обязательства предоставляют определенные законом права, а также дополнительные права, которые могут быть различными в разных странах.

Регистрация

Зарегистрируйте ваше изделие в режиме он-лайн для получения по электронной почте сообщений об обновлениях микропрограммного обеспечения и информации об изделиях на сайте www.zyxel.com (глобальный), или на сайте www.us.zyxel.com (для Северной Америки).

K

Сервисная служба

При обращении в Сервисную службу будьте готовы предоставить следующую информацию:

Обязательные сведения

- Модель изделия и серийный номер.
- Гарантийные обязательства.
- Дата приобретения устройства.
- Краткое описание неисправности, а также действий, предпринятых по ее устранению.

Головной офис корпорации (По всему миру)

- E-mail службы поддержки: support@zyxel.com.tw
- E-mail отдела продаж: sales@zyxel.com.tw
- Телефон: +886-3-578-3942
- Факс: +886-3-578-2439
- Web-сайт: www.zyxel.com, www.europe.zyxel.com
- FTP-сайт: ftp.zyxel.com, ftp.europe.zyxel.com
- Обычная почта: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa RICA

- E-mail службы поддержки: soporte@zyxel.co.cr
- E-mail отдела продаж: sales@zyxel.co.cr
- Телефон: +506-2017878
- Факс: +506-2015098
- Web-сайт: www.zyxel.co.cr
- FTP-сайт: ftp.zyxel.co.cr
- Обычная почта: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Чешская Республика

- E-Mail: info@cz.zyxel.com
- Телефон: +420-241-091-350
- Факс: +420-241-091-359
- Web-сайт: www.zyxel.cz

- Обычная почта: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Дания

- E-mail службы поддержки: support@zyxel.dk
- E-mail отдела продаж: sales@zyxel.dk
- Телефон: +45-39-55-07-00
- Факс: +45-39-55-07-07
- Web-сайт: www.zyxel.dk
- Обычная почта: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Финляндия

- E-mail службы поддержки: support@zyxel.fi
- E-mail отдела продаж: sales@zyxel.fi
- Телефон: +358-9-4780-8411
- Факс: +358-9-4780 8448
- Web-сайт: www.zyxel.fi
- Обычная почта: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

Франция

- E-Mail: info@zyxel.fr
- Телефон: +33-4-72-52-97-97
- Факс: +33-4-72-52-19-20
- Web-сайт: www.zyxel.fr
- Обычная почта: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Германия

- E-mail службы поддержки: support@zyxel.de
- E-mail отдела продаж: sales@zyxel.de
- Телефон: +49-2405-6909-0
- Факс: +49-2405-6909-99
- Web-сайт: www.zyxel.de
- Обычная почта: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Венгрия

- E-mail службы поддержки: support@zyxel.hu
- E-mail отдела продаж: info@zyxel.hu
- Телефон: +36-1-3361649
- Факс: +36-1-3259100
- Web-сайт: www.zyxel.hu
- Обычная почта: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Казахстан

- Служба поддержки: http://zyxel.kz/support
- E-mail отдела продаж: sales@zyxel.kz
- Телефон: +7-3272-590-698
- Факс: +7-3272-590-689
- Web-сайт: www.zyxel.kz
- Обычная почта: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

Северная Америка

- E-mail службы поддержки: support@zyxel.com
- E-mail отдела продаж: sales@zyxel.com
- Телефон: +1-800-255-4101, +1-714-632-0882
- Факс: +1-714-632-0858
- Web-сайт: www.us.zyxel.com
- FTP-сайт: ftp.us.zyxel.com
- Обычная почта: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Норвегия

- E-mail службы поддержки: support@zyxel.no
- E-mail отдела продаж: sales@zyxel.no
- Телефон: +47-22-80-61-80
- Факс: +47-22-80-61-81
- Web-сайт: www.zyxel.no
- Обычная почта: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Польша

- E-Mail: info@pl.zyxel.com
- Телефон: +48 (22) 333 8250
- Факс: +48 (22) 333 8251
- Web-сайт: www.pl.zyxel.com
- Обычная почта: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Россия

- Служба поддержки: http://zyxel.ru/support
- E-mail отдела продаж: sales@zyxel.ru
- Телефон техподдержки 8-800-200-8929
- Телефон: +7-095-542-89-29
- Факс: +7-095-542-89-25
- Web-сайт: www.zyxel.ru
- Обычная почта: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Испания

- E-mail службы поддержки: support@zyxel.es
- E-mail отдела продаж: sales@zyxel.es
- Телефон: +34-902-195-420
- Факс: +34-913-005-345
- Web-сайт: www.zyxel.es
- Обычная почта: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Швеция

- E-mail службы поддержки: support@zyxel.se
- E-mail отдела продаж: sales@zyxel.se
- Телефон: +46-31-744-7700
- Факс: +46-31-744-7701
- Web-сайт: www.zyxel.se
- Обычная почта: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Украина

- E-mail службы поддержки: support@ua.zyxel.com
- E-mail отдела продаж: sales@ua.zyxel.com
- Телефон: +380-44-247-69-78
- Факс: +380-44-494-49-32
- Web-сайт: www.ua.zyxel.com
- Обычная почта: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

Великобритания

- E-mail службы поддержки: support@zyxel.co.uk
- E-mail отдела продаж: sales@zyxel.co.uk
- Телефон: +44-1344 303044, 08707 555779 (UK only)
- Факс: +44-1344 303034
- Web-сайт: www.zyxel.co.uk
- FTP-сайт: ftp.zyxel.co.uk
- Обычная почта: ZyXEL Communications UK, Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

Вместо “+” наберите код международной телефонной связи.

Алфавитный указатель

A

Авторское право 215
Агенство по назначению имен и уникальных параметров протоколов Интернет
см. IANA 199
Агентство по назначению имен и уникальных параметров протоколов Интернет, см. IANA 75
ALG
включение SIP/FTP/H.323 92
ALG (Application Layer Gateway - встроенный программный шлюз для приложений) 91
Альтернативные варианты записи маски подсети 194
Any IP (Любой IP).
Any IP и NAT 78
Application Layer Gateway (ALG - встроенный программный шлюз для приложений) 91

B

База управляющей информации (MIB) 115

C

Варианты использования 25
Виртуальный канал (VC) 54
Восстановление конфигурации 144
Время простоя 110
Встроенная справка 32

D

Гарантия 216
примечание 217
DHCP 74, 75, 105, 135
конфигурация 74
DNS 74
DNS и удаленное управление 117

E

Диагностика 147
Динамическая система доменных имен (DYNDNS) 105
Доменное имя 135
Доменное имя и клиенты DHCP 135
Доступ в Интернет 25, 41
Мастер настройки 41

F

FTP 26, 109, 113
и NAT 92
и удаленное управление 113

H

Заводские настройки по умолчанию 145
Заключение Федеральной Комиссии по связи (FCC) по помехам 215
HTTP
и удаленное управление 109
HTTP (Протокол передачи гипертекста) 141

I

IANA 75, 199
Идентификатор виртуального канала (VCI) 55
Идентификатор виртуального пути (VPI) 55
IGMP
версии 77
и многоадресная рассылка 77
IGMP (Internet Group Multicast Protocol/Протокол многоадресной рассылки) 76
Изменение пароля при входе 31
Имя пользователя 106
Инициализировать заново линию ADSL
диагностика
линия ADSL 148

Инкапсуляция 53, 55
инкапсуляция ENET ENCAP 53
протокол "точка-точка" поверх Ethernet (PPPoE) 53
PPPoA 54
RFC 1483 54
Интерфейс Web-конфигуратора 32
IP
адрес 75
адрес в локальной сети по умолчанию 29
диапазон адресов 82
и статический маршрут 101
назначение адреса 55
назначение адреса при ENET ENCAP 56
назначение адреса при PPPoA 56
назначение адреса при PPPoE 56
назначение адреса при RFC 1483 56
пул адресов 74
IP-адрес 93
и NAT 94
сервер по умолчанию 93
NAT 94
IP-адрес в локальной сети по умолчанию 29

K

Кнопка перезапуска 153
Командный интерфейс 26
Контактная информация 219
Конфигурация
резервное сохранение 144
восстановление 144
Краткое руководство
подключение оборудования 29

L

LAN (ЛВС)
DHCP 74
TCP/IP 75
Линия DSL, инициализировать заново 148
Любой IP
как работает 77, 78
настройка 81

M

Максимальный размер пакета (MBS) 57, 63, 69
Маршрутизация на базе стратегии IP (IPPR) 159
Маска подсети 75, 192
Маски DYNDNS 105
Метрика 56
Метрика, стоимость передачи 56
MIB (Management Information Base – База управляющей информации) 115
Микропрограмма 141
загрузка 141
обновление 141
ошибка загрузки 143
Многоадресная рассылка 76
Многопротокольная инкапсуляция 54
Монтаж
настенное крепление 161
Мультиплексирование 54, 55
на базе LLC 54
на базе VC 54
Мультиплексирование на базе VC 55

N

Настенное крепление 161
Настройка диапазона IP 74
Настройка общих параметров 135
Настройки по умолчанию 145
NAT 75, 91, 93, 199
режим 91
и серверы 90
как работает 88
конфигурация 91
правило отображения адресов 99
приложение 89
пример 93
назначение трансляции сетевых адресов 88
определения 87
характеристики 158
типы отображения 89
NAT Transversal 121
Незаданная скорость передачи (UBR) 63, 68
Непризнание иска 215

O

Технические характеристики
у 157
Ограничения на FTP 109
Ограничения на TFTP 109
Ограничения на удаленное управление 109

Управление устройством
с использованием Telnet См. командный
Организация подсетей 194

P

Пароль
изменение при входе 31
Переменная скорость передачи (VBR) 63, 68
Перенаправление трафика 69, 70, 71, 159
пример 69
Пиковая скорость ячеек (PCR) 57, 63, 68
Поддерживаемая скорость ячеек (SCR) 57, 63, 68
Поддерживаемые протоколы 158
Подсеть 191
Полупостоянное соединение 56
Постоянная скорость передачи (CBR) 63, 68
PPPoA 55
PPPoE 53
преимущества 53
Протокол "Точка-точка" поверх уровня 5 адаптации ATM (AAL5) 54
Протокол маршрутизации канального уровня с инкапсуляцией MAC (ENET ENCAP) 53
протокол обмена информацией о маршрутизации
также см. RIP 76
Протокол разрешения адресов (ARP) 78
Протокол SNMP 26, 114
агент 114
базы управляющей информации (MIB) 115
и удаленное управление 114
средство управления 114

R

Разделители частот и микрофильтры 163
Регистрация 31
изделие 217
Регистрация изделия 217
Резервное сохранение 144
Резервный шлюз 70
RFC -1483 55
RFC 1483 54
RFC 1631 87
RFC-2364 55
RIP
версия 76
направление 76
RIP (Routing Information Protocol – протокол обмена информацией о маршрутизации) 76

S

Сброс настроек
и заводские настройки по умолчанию 145
Сброс настроек устройства к заводским установкам 153
Серверы
сервер точного времени 139
серверы и NAT 90
Сервисная служба 219
Сертификация 215
замечания 216
просмотр 216
SIP ALG 91
SIP Application Layer Gateway (Встроенный программный шлюз для приложений, использующих протокол SIP), также см. SIP ALG 91
Системное имя 136
Служба имен доменов
см. DNS
Службы
службы и NAT 93
SNMP (Simple Network Management Protocol — Простой протокол управления сетью). 114
SNMP-менеджер 114
Сопроводительная документация 3
Сплиттеры 163
Справка, Web-конфигуратор 32
Сравнение SUA и NAT
SUA (Single User Account - учетная запись одиночного пользователя) 90
Стандарты ADSL 26, 158
статический маршрут
как работает 101
пример 101
удаленные узлы 101
Стоимость передачи 56
SUA 90
SUA (Single User Account - учетная запись одиночного пользователя) 90

T

Техника безопасности 6
Технические характеристики 157

габариты 157
питание 157
Тип резервирования 71
Товарные знаки 215
Traffic shaping 57
Трансляция сетевых адресов (NAT) 87

U

Удаленное управление
отключение 109
109
виды сеансов связи 109
и FTP 113
и LAN 109
и SNMP 114
и WAN 109
Удаленное управление и NAT 110
Универсальная функция Plug and Play 121
применение 121
UPnP 121
вопросы безопасности 122
форум 122
установка 123
установка, Windows Me 123
установка, Windows XP 125
Управление
типы 158
Управление с помощью Telnet 111
и удаленное управление 109, 111
Управление устройством
использование командного интерфейса См. командный интерфейс.
полезные советы 26
с использованием FTP. См. FTP
с использованием SNMP. См. SNMP.
с использованием Web-конфигуратора. См. Web-конфигуратор.
Уровень 5 адаптации ATM (AAL5) 54
Условные обозначения 4

V

VPI и VCI 55

W

WAN (Глобальная сеть) 53
инкапсуляция 53
инкапсуляция ENET ENCAP 53
протокол "точка-точка" поверх Ethernet (PPPoE) 53
настройка 53
тип резервирования 71
PPPoA 54
WAN backup (резервное подключени WAN) 70
Характеристики 158
Web и удаленное управление 110
Web-конфигуратор 26, 29, 32
работа с интерфейсом 32
главное окно 32
help 32
сводная таблица окон 32