P–660HT EE

Интернет-центр с модемом ADSL2+ и 4-портовым коммутатором

P–660HTW EE

Беспроводной интернет-центр 802.11g с модемом ADSL2+
и 4-портовым коммутатором

Руководство пользователя

Версия 3.40
2/2006

ZyXEL

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 право вносить изменения в любые описанные в данном документе изделия без дополнительного уведомления. Информация в этом руководстве также может быть изменена без специального уведомления.

Торговые марки

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.

Техника безопасности

Для обеспечения безопасности необходимо ознакомиться и следовать следующим правилам.

- Для уменьшения опасности возгорания необходимо использовать телефонный провод только №26 или выше по системе AWG (American Wire Gauge — американская система калибровки проводов).
- Не вскрывайте устройство. Не следует открывать или снимать крышку во избежание поражения электрическим током высокого напряжения и других повреждений. Проводить обслуживание может только квалифицированный технический персонал. Пожалуйста, свяжитесь с местным поставщиком для получения информации о техническом обслуживании.
- Используйте источник питания, предназначенный ИМЕННО для Вашего устройства. Подключите кабель питания или адаптер питания к сети электропитания с соответствующим напряжением (110 В переменного тока в Северной Америке или 230 В переменного тока в Европе).
- Не используйте устройство, если источник питания неисправен, так как это может привести к поражению электрическим током.
- Если источник питания поврежден, отключите его от розетки электропитания.
- Не пытайтесь ремонтировать источник питания. Для заказа нового источника питания свяжитесь с местным поставщиком.
- Прокладывайте соединительные кабели в местах, где никто не будет наступать на них или спотыкаться. Не кладите на кабель питания какие-либо предметы и не располагайте его в местах, где могут ходить люди.
- Если устройство должно быть закреплено на стене, проверьте, что при этом не будут повреждены электропроводка, газо- или водопроводы.
- Не устанавливайте и не используйте устройство во время грозы. Существует определенный риск получить удар электрическим током при разряде молнии.
- Не подвергайте устройство воздействию влаги, пыли или агрессивных жидкостей.
- Не используйте изделие в непосредственной близости от воды, например, во влажных подвалах или рядом с бассейном.
- Убедитесь, что все кабели подключены к соответствующим портам.
- Не заслоняйте вентиляционные отверстия устройства, так как недостаточный приток воздуха может стать причиной повреждения устройства.
- Не кладите на устройство предметы.
- Подключайте к устройству ТОЛЬКО соответствующие комплектующие.

Информация о сертификации

Интернет-центры ZyXEL P-660HT EE / P-660HTW EE одобрены для применения государственными органами по сертификации средств связи.

Система сертификации ГОСТ Р, Госстандарт России

P-660HT EE, сертификат соответствия № РОСС TW.АЯ46.В29093. Срок действия с 5.12.2005 по 5.12.2007.

P-660HTW EE, сертификат соответствия № РОСС TW.АЯ46.В29605. Срок действия с 30.12.2005 по 29.12.2007.

Соответствуют требованиям: ГОСТ Р МЭК 60950-2002, ГОСТ Р 51318.22-99, ГОСТ Р 51318.24-99, ГОСТ Р 51317.3.2-99, ГОСТ Р 51317.3.3-99.

Государственная Санитарно-эпидемиологическая служба РФ

Санитарно-эпидемиологическое заключение № 77.01.09.658.П.012182.03.06. Срок действия с 15.03.2006 по 03.03.2011. Соответствует санитарным правилам: СанПиН 2.2.2./2.4.1340-03"Гигиенические требования к персональным электронно-вычислительным машинам и организации работы, СанПиН 2.1.8./2.2.4.1190-03.

Юридический адрес изготовителя

ZyXEL Communications Corporation, N 6, Innovation Road II, Science-Based Industrial Park, Hsin-Chu, Taiwan, R.O.C.

Установленный производителем в порядке п.2 ст.5 Федерального закона РФ "О защите прав потребителей" срок службы изделия равен 5 годам с даты производства при условии, что изделие используется в строгом соответствии с настоящим руководством и применимыми техническими стандартами.

© ZyXEL, 2006. Все права защищены.

Воспроизведение, передача, распространение или хранение в любой форме данного документа или любой его части без предварительного письменного разрешения ZyXEL запрещено. Названия продуктов или компаний, упоминаемые в данном руководстве, могут быть товарными знаками или товарными именами соответствующих владельцев. ZyXEL придерживается политики непрерывного развития и оставляет за собой право вносить любые изменения и улучшения в любой продукт, описанный в этом документе, без предварительного уведомления. Содержание этого документа предоставлено на условиях "как есть". ZyXEL оставляет за собой право пересматривать или изменять содержимое данного документа в любое время без предварительного уведомления.

Гарантийное обслуживание ZyXEL

Благодарим вас за покупку изделия ZyXEL! Мы гордимся надежностью и качеством нашей продукции и верим, что это изделие прослужит вам безотказно долгие годы. Тем не менее, если вы столкнетесь с вопросами при использовании этого изделия, пожалуйста, обратитесь за помощью в региональный офис ZyXEL Communications Corporation.

Гарантийные обязательства

1. Настоящая гарантия действует в течение трех лет с даты приобретения изделия ZyXEL и подразумевает гарантийное обслуживание в случае обнаружения дефектов, связанных с материалами и сборкой. В этом случае потребитель имеет право на бесплатный ремонт изделия.
2. При регистрации приобретенного изделия через Интернет на сайте указанном в таблице потребитель получает дополнительный год гарантийного обслуживания.
3. Максимальный срок гарантии, предоставляемой компанией ZyXEL, исчисляется с даты производства изделия и составляет четыре с половиной года. Дата производства определяется по серийному номеру на корпусе изделия: SYxWWxxxxx, где Y - последняя цифра года, а WW - номер недели с начала года.
4. Настоящая гарантия распространяется только на изделия ZyXEL, проданные через официальные каналы дистрибуции ZyXEL.
5. Настоящая гарантия предоставляется компанией ZyXEL в дополнение к правам потребителя, установленным действующим законодательством в стране приобретения.

Условия гарантии

1. Гарантийное обслуживание изделия ZyXEL осуществляется в авторизованных сервисных центрах (АСЦ) ZyXEL на приведенных ниже условиях.
2. Настоящая гарантия действительна только при предъявлении вместе с неисправным изделием правильно заполненного фирменного гарантийного талона с проставленной датой продажи. Компания ZyXEL оставляет за собой право отказать в бесплатном гарантийном обслуживании, если гарантийный талон не будет предоставлен или если содержащаяся в нем информация будет неполной или неразборчивой.
3. Настоящая гарантия недействительна в случаях, если:
   3.1. серийный номер на изделии изменен, стерт, удален или неразборчив;
   3.2. изделие переделывалось без предварительного письменного согласия ZyXEL;
   3.3. изделие неправильно эксплуатировалось, в том числе: а) использовалось не по назначению или не в соответствии с руководством ZyXEL; б) устанавливалось или эксплуатировалось в условиях, не соответствующих стандартам и нормам безопасности, действующим в стране использования;
   3.4. изделие ремонтировалось не уполномоченными на то сервисными центрами или дилерами;

3.5. изделие вышло из строя по причине несчастного случая, удара молнии, затопления, пожара, неправильной вентиляции и иных причин, находящихся вне контроля ZyXEL;
3.6. изделие пострадало при транспортировке, за исключением случаев, когда она производится АСЦ;
3.7. изделие использовалось в дефектной системе.

Контактная информация

СТРАНА	РОССИЯ	УКРАИНА	КАЗАХСТАН
Поддержка через Интернет	http://zyxel.ru/support	http://ua.zyxel.com/support	http://zyxel.kz/support
Телефон службы поддержки	+ 7 (095) 542-89-29 + 8 (800) 200-89-29 (бесплатный звонок из регионов России)	+380 (44) 247-69-78	+ 7 (3272) 590-689
Сервер в Интернете	http://zyxel.ru	http://www.ua.zyxel.com	http://zyxel.kz
Почтовый адрес	ZyXEL Россия 117279, Москва ул. Островитянова 37а	ZyXEL Украина 04050, Киев ул. Пимоненко 13	ZyXEL Казахстан 0500106, Алматы пр. Достык 43, офис 414

Содержание

Авторское право **2**

Техника безопасности **3**

Информация о сертификации **4**

Юридический адрес изготовителя **5**

Гарантийное обслуживание ZyXEL **6**

Контактная информация **8**

Содержание **10**

Список рисунков **24**

Список таблиц **32**

Предисловие **38**

Введение в DSL **40**

Глава 1
Знакомство с интернет-центром P–660HT/HTW EE **42**

1.1 Знакомство с интернет-центром P–660HT/HTW EE 42
1.2 Характеристики 43
1.2.1 Беспроводной доступ (P–660HTW EE) 46
1.3 Сферы применения интернет-центра P–660HT/HTW EE 47
1.3.1 Защищенный доступ в Интернет 47
1.3.2 Соединение локальных сетей 47
1.4 Светодиоды передней панели 48
1.5 Подключение аппаратных средств 49

Глава 2
Знакомство с Web-конфигуратором **50**

2.1 Описание Web-конфигуратора 50
2.1.1 Доступ к Web-конфигуратору 50
2.1.2 Сброс настроек интернет-центра 51
2.1.2.1 Использование кнопки сброса настроек 51
2.1.3 Интерфейс Web-конфигуратора 52
2.2 Изменение пароля для входа в систему 56

Глава 3
Мастер установки доступа в Интернет 58

3.1 Введение 58
3.1.1 Мастер установки доступа в Интернет 58

Глава 4
Настройка локальной сети 68

4.1 Обзор локальной сети 68
4.1.1 Локальные, глобальные сети и интернет-центр 68
4.1.2 Настройка DHCP 69
4.1.2.1 Настройка диапазона IP 69
4.1.3 Адрес сервера DNS 69
4.1.4 Назначение адреса сервера DNS 70
4.2 Настройка TCP/IP локальной сети 70
4.2.1 IP-адрес и маска подсети 70
4.2.1.1 IP-адреса для частных сетей 71
4.2.2 Настройка RIP 71
4.2.3 Многоадресная рассылка 72
4.2.4 Any IP (Любой IP) 73
4.2.4.1 Как работает функция Any IP (Любой IP) 74
4.3 Настройка локальной сети 74

Глава 5
Беспроводная локальная сеть (WLAN) 78

5.1 Беспроводная локальная сеть — введение 78
5.2 Защита беспроводной сети — общая информация 78
5.2.1 Шифрование 78
5.2.2 Аутентификация 79
5.2.3 Ограниченный доступ 79
5.2.4 Предотвращение обнаружения беспроводной сети 79
5.3 Главное окно настроек беспроводной локальной сети 79
5.4 Настройки в окне Wireless (Беспроводная сеть) 81
5.4.1 WEP-шифрование 81
5.5 Настройка фильтра MAC-адресов 84
5.6 Введение в WPA 86
5.6.1 Пример применения WPA-PSK 86
5.6.2 Пример применения WPA с сервером RADIUS 87
5.6.3 Вспомогательное программное обеспечение для беспроводных клиентов WPA 88
5.7 Настройка IEEE 802.1x и WPA 88
5.7.1 Запрещение доступа или доступ без аутентификации 89
5.7.2 Authentication Required (Требуется аутентификация): 802.1x 91
5.7.3 Authentication Required (Требуется аутентификация): WPA 94

5.7.4 Authentication Required (Требуется аутентификация): WPA-PSK 96
5.8 Настройка локальной аутентификации пользователей 98
5.9 Настройка сервера RADIUS 100

Глава 6
Настройка глобальной сети 102

6.1 Общая информация о глобальной сети 102
6.1.1 Инкапсуляция 102
6.1.1.1 Инкапсуляция ENET ENCAP 102
6.1.1.2 Протокол "точка-точка" поверх Ethernet (PPPoE) 102
6.1.1.3 Протокол "точка-точка" поверх ATM (PPPoA) 103
6.1.1.4 RFC 1483 103
6.1.2 Мультиплексирование 103
6.1.2.1 Мультиплексирование на базе VC 103
6.1.2.2 Мультиплексирование на базе LLC 103
6.1.3 VPI и VCI 104
6.1.4 Назначение IP-адреса 104
6.1.4.1 Назначение IP с инкапсуляцией PPPoA или PPPoE 104
6.1.4.2 Назначение IP с инкапсуляцией RFC 1483 104
6.1.4.3 Назначение IP с инкапсуляцией ENET ENCAP 104
6.1.5 Постоянное соединение (по протоколу "точка-точка" — PPP) 105
6.1.6 NAT (Трансляция сетевых адресов) 105
6.2 Метрика 105
6.3 Инкапсуляция PPPoE 106
6.4 Ограничение трафика 106
6.5 Доступ в Интернет с использованием автоматической настройки модема (Zero Configuration) 107
6.6 Главное окно WAN 108
6.7 Настройка подключения к глобальной сети 108
6.8 Перенаправление трафика (Traffic Redirect) 112
6.9 Настройка резервного соединения с глобальной сетью 113

Глава 7
Окна NAT (Трансляция сетевых адресов)..... 116

7.1 Обзор NAT 116
7.1.1 Определения NAT 116
7.1.2 Назначение NAT 117
7.1.3 Как работает NAT 117
7.1.4 Применение NAT 118
7.1.5 Типы отображения NAT 119
7.2 SUA (Учетная запись одиночного пользователя) в сравнении с NAT 120
7.3 Сервер SUA 120
7.3.1 IP-адрес сервера по умолчанию 120

7.3.2 Переадресация портов: службы и номера портов 121
7.3.3 Настройка серверов, расположенных за SUA (пример) 121
7.4 Выбор режима NAT 122
7.5 Настройка серверов SUA 123
7.6 Настройка правил отображения адресов 125
7.7 Редактирование правил отображения адресов 127

Глава 8
Настройка динамической системы доменных имен (DYNDNS) 130

8.1 Динамическая система доменных имен (DYNDNS) — общая информация 130
8.1.1 Шаблоны DYNDNS 130
8.2 Настройка динамической DNS (DYNDNS) 131

Глава 9
Время и дата 132

9.1 Установка времени и даты 132

Глава 10
Межсетевые экраны..... 136

10.1 Межсетевой экран — общая информация 136
10.2 Типы межсетевых экранов 136
10.2.1 Межсетевые экраны с фильтрацией пакетов 137
10.2.2 Межсетевые экраны на уровне приложений 137
10.2.3 Межсетевые экраны с инспекцией пакетов с учетом состояния 137
10.3 Знакомство с межсетевым экраном ZyXEL 138
10.3.1 Атаки типа "Отказ в обслуживании" (DoS) 139
10.4 Отказ в обслуживании (DoS) 139
10.4.1 Основные сведения 139
10.4.2 Типы атак DoS 140
10.4.2.1 Уязвимость ICMP 142
10.4.2.2 Недопустимые команды (NetBIOS и SMTP) 143
10.4.2.3 Traceroute 143
10.5 Инспекция пакетов с учетом состояния 144
10.5.1 Действие функции инспекции пакетов с учетом состояния 145
10.5.2 Реализация функции в модели P–660HT/HTW EE 146
10.5.3 Безопасность TCP 146
10.5.4 Безопасность UDP/ICMP 147
10.5.5 Протоколы верхнего уровня 147
10.6 Методы усиления безопасности при помощи межсетевого экрана 148
10.6.1 Общая безопасность 148
10.7 Сравнение функций фильтрации пакетов и межсетевого экрана 149
10.7.1 Фильтрация пакетов 149

10.7.1.1 Случаи использования фильтрации 149
10.7.2 Межсетевой экран 150
10.7.2.1 Случаи использования межсетевого экрана 150

Глава 11
Настройка межсетевого экрана 152

11.1 Способы настройки 152
11.2 Обзор правил межсетевого экрана 152
11.3 Обзор логики правил 153
11.3.1 Список вопросов для составления правил 153
11.3.2 Правила с точки зрения безопасности 154
11.3.3 Основные поля для настройки правил 154
11.3.3.1 Action (Действие) 154
11.3.3.2 Service (Служба) 154
11.3.3.3 Source Address (Адрес источника) 154
11.3.3.4 Destination Address (Адрес получателя) 155
11.4 Направление связи 155
11.4.1 Правила LAN–WAN 155
11.4.2 Предупреждения 155
11.5 Настройка политики межсетевого экрана по умолчанию 156
11.6 Список правил 157
11.6.1 Настройка правил межсетевого экрана 159
11.7 Пользовательские службы 162
11.8 Настройка пользовательских служб 163
11.9 Пример правила межсетевого экрана 164
11.10 Предварительно настроенные службы 168
11.11 Anti-Probing (Блокирование эхо-тестирования) 171
11.12 Допустимые пороги для атак "Отказ в обслуживании" (DoS) 172
11.12.1 Значения допустимых порогов 173
11.12.2 Полуоткрытые сеансы связи 173
11.12.2.1 Максимум неполных TCP-соединений и время блокирования 174
11.12.3 Настройка порогов межсетевого экрана 174

Глава 12
Фильтрация на основе содержания (контентная фильтрация) 178

12.1 Фильтрация на основе содержания — общая информация 178
12.2 Главное окно фильтрации на основе содержания 178
12.3 Настройка блокировки по ключевым словам 179
12.4 Настройка графика фильтрации 181
12.5 Настройка списка надежных (доверенных) компьютеров 181

Глава 13
Настройка удаленного управления 184

13.1 Удаленное управление — общая информация 184
13.1.1 Ограничения на удаленное управление 185
13.1.2 Удаленное управление и NAT 185
13.1.3 Время бездействия системы 185
13.2 Управление с помощью Telnet 185
13.3 FTP 186
13.4 Web 186
13.5 Настройка удаленного управления 186

Глава 14
Универсальная функция Plug and Play (UPnP) 188

14.1 Описание универсальной функции Plug and Play 188
14.1.1 Как узнать, используется ли UPnP? 188
14.1.2 NAT Transversal 188
14.1.3 Предупреждения по использованию UPnP 189
14.2 UPnP и ZyXEL 189
14.2.1 Настройка UPnP 189
14.3 Пример установки UPnP в Windows 190
14.4 Пример использования UPnP в Windows XP 194

Глава 15
Экраны регистрационных журналов 202

15.1 Регистрационные журналы — общие сведения 202
15.1.1 Предупреждения и журнальные записи 202
15.2 Настройка параметров журнала 202
15.3 Отображение журнальных записей 206
15.4 Сообщения об ошибках SMTP 207
15.4.1 Пример журнала, высылаемого по электронной почте 207

Глава 16
Расширенная настройка управления пропускной способностью 210

16.1 Управление пропускной способностью среды передачи — общая информация 210
16.2 Классы и фильтры пропускной способности 211
16.3 Пропорциональное распределение пропускной способности 211
16.4 Примеры управления пропускной способностью 211
16.4.1 Управление пропускной способностью на основе приложения 211
16.4.2 Управление пропускной способностью на основе подсети 212
16.4.3 Управление пропускной способностью на основе приложения и подсети 212
16.5 Планировщик 213

16.5.1 Планировщик на основе приоритетов 213
16.5.2 Планировщик на основе равномерного распределения 213
16.6 Увеличение использования пропускной способности 213
16.6.1 Резервирование пропускной способности для трафика, не относящегося к классам пропускной способности 214
16.6.2 Пример увеличения использования пропускной способности 214
16.7 Заимствование пропускной способности 216
16.7.1 Увеличение использования пропускной способности с заимствованием пропускной способности 216
16.8 Главное окно управления пропускной способностью среды передачи ...217
16.9 Настройка — окно "Общие настройки" 218
16.10 Настройка классов пропускной способности 219
16.10.1 Управление пропускной способностью среды передачи — параметры класса 220
16.10.2 Управление пропускной способностью среды передачи: статистика 223
16.11 Монитор пропускной способности 225

Глава 17
Сопровождение 226

17.1 Сопровождение — общая информация 226
17.2 Окно "Состояние системы" 226
17.2.1 Статистика системы 229
17.3 Окно "Таблица DHCP" 230
17.4 Окно "Таблица Any IP" 231
17.5 Окно "Беспроводная сеть" (Wireless) 232
17.5.1 Association List (Список соединений) 232
17.6 Окна диагностики 233
17.6.1 Общая диагностика 233
17.6.2 Диагностика линии DSL 234
17.7 Обновление микропрограммы 236

Глава 18
Знакомство с SMT..... 240

18.1 Описание SMT (System Management Terminal) 240
18.1.1 Процедура настройки при помощи SMT через соединение Telnet .240
18.1.2 Ввод пароля 240
18.1.3 Обзор меню SMT интернет-центра 241
18.2 Работа с интерфейсом SMT 243
18.2.1 Обзор интерфейса SMT 245
18.3 Изменение системного пароля 246

Глава 19
Меню 1 — Настройка общих параметров 248

19.1 Настройка общих параметров 248
19.2 Процедура настройки в Меню 1 248
19.2.1 Процедура настройки динамической DNS (DYNDNS) 250

Глава 20
Меню 2 — Настройка резервирования глобальной сети 252

20.1 Описание настройки резервирования глобальной сети 252
20.2 Настройка резервного соединения через модем в Меню 2 252
20.2.1 Настройка перенаправления трафика 254

Глава 21
Меню 3 — Настройка локальной сети 256

21.1 Настройка локальной сети 256
21.1.1 Настройка сети Ethernet — общие настройки 256
21.2 Настройка Ethernet в зависимости от используемого протокола 257
21.3 Настройка TCP/IP и DHCP для Ethernet 257

Глава 22
Настройка беспроводной локальной сети 260

22.1 Описание беспроводной локальной сети 260
22.2 Настройка беспроводной локальной сети 260
22.2.1 Фильтр MAC-адресов для беспроводной локальной сети 262

Глава 23
Доступ в Интернет 264

23.1 Описание доступа в Интернет 264
23.2 Политики IP (IP Policies) 264
23.3 Псевдоним IP (IP Alias) 264
23.4 Создание псевдонимов IP 265
23.5 Настройка маршрута IP 267
23.6 Настройка доступа в Интернет 267

Глава 24
Настройка удаленного узла 270

24.1 Описание настройки удаленного узла 270
24.2 Настройка удаленного узла 270
24.2.1 Профиль удаленного узла 270
24.2.2 Сценарии инкапсуляции и мультиплексирования 271
24.2.2.1 Сценарий 1: один виртуальный канал, несколько протоколов 271
24.2.2.2 Сценарий 2: один виртуальный канал, один протокол (IP) 271

24.2.2.3 Сценарий 3: несколько виртуальных каналов 271
24.2.3 Протокол аутентификации исходящих вызовов 274
24.3 Параметры сетевого уровня удаленного узла 274
24.3.1 IP-адреса в поле My WAN Addr (Мой адрес в глобальной сети) 276
24.4 Фильтр удаленного узла 277
24.5 Редактирование параметров уровня ATM 278
24.5.1 Мультиплексирование на базе VC (не-PPP инкапсуляция) 278
24.5.2 Мультиплексирование на базе LLC или инкапсуляция PPP 279
24.5.3 Параметры дополнительной настройки 279

Глава 25
Настройка статических маршрутов..... 282

25.1 Статические маршруты IP — общая информация 282
25.2 Настройка 282

Глава 26
Настройка моста..... 286

26.1 Общие сведения о мосте 286
26.2 Настройка Ethernet для организации моста 286
26.2.1 Настройка моста для удаленного узла 286
26.2.2 Настройка статического маршрута для моста 288

Глава 27
Трансляция сетевых адресов (NAT)..... 290

27.1 Применение NAT 290
27.1.1 SUA (Учетная запись одиночного пользователя) в сравнении с NAT 290
27.2 Применение NAT 290
27.3 Настройка NAT 292
27.3.1 Наборы отображения адресов 292
27.3.1.1 Набор отображения адресов SUA 293
27.3.1.2 Пользовательские наборы отображения адресов 294
27.3.1.3 Порядок применения правил 295
27.4 Настройка сервера, расположенного за NAT 297
27.5 Примеры применения NAT 299
27.5.1 Пример 1: только доступ в Интернет 299
27.5.2 Пример 2: доступ в Интернет с внутренним сервером 300
27.5.3 Пример 3: несколько общедоступных IP-адресов для внутренних серверов 301
27.5.4 Пример 4: прикладные программы, не поддерживающие NAT 305

Глава 28
Активация межсетевого экрана 308

28.1 Удаленное управление и межсетевой экран 308
28.2 Способы настройки 308
28.3 Активация межсетевого экрана 308

Глава 29
Настройка фильтров..... 310

29.1 О фильтрации 310
29.1.1 Структура фильтра 312
29.2 Настройка набора фильтров 313
29.3 Меню "Список правил фильтра" 315
29.4 Настройка правила фильтра 317
29.4.1 Правило фильтра TCP/IP 317
29.4.2 Правило фильтра общего типа 320
29.5 Типы фильтров и NAT 322
29.6 Пример фильтра 323
29.7 Применение фильтров и заводских настроек по умолчанию 325
29.7.1 Трафик Ethernet 325
29.7.2 Фильтры для удаленного узла 326

Глава 30
Настройка SNMP 328

30.1 О протоколе SNMP 328
30.2 Поддерживаемые базы управляющей информации 329
30.3 Настройка SNMP 329
30.4 Прерывания SNMP 331

Глава 31
Системные функции безопасности..... 332

31.1 Системные функции безопасности 332
31.1.1 Системный пароль 332
31.1.2 Настройка внешнего сервера RADIUS 332
31.1.3 IEEE 802.1x 334
31.2 Создание учетных записей пользователей в интернет-центре 338

Глава 32
Информация о системе и диагностика..... 340

32.1 Обзор 340
32.2 Состояние системы 340
32.3 Информация о системе 343
32.3.1 Информация о системе 343
32.3.2 Скорость консольного порта 345

32.4 Журнал регистрации и трассировка 345
32.4.1 Просмотр журнала регистрации ошибок 345
32.4.2 Системный журнал и учет ресурсов 346
32.5 Диагностика 349

Глава 33
Сопровождение файлов конфигурации и микропрограммы..... 352

33.1 Структура имен файлов 352
33.2 Резервное сохранение конфигурации 353
33.2.1 Резервное сохранение конфигурации 353
33.2.2 Использование команд FTP в командной строке 354
33.2.3 Пример использования команд FTP в командной строке 354
33.2.4 Клиенты FTP на основе графического интерфейса 355
33.2.5 Ограничение управления через глобальную сеть по TFTP и FTP ..355
33.2.6 Резервное сохранение конфигурации с помощью TFTP 356
33.2.7 Пример команды TFTP 356
33.2.8 Клиенты TFTP на основе графического интерфейса 357
33.3 Восстановление конфигурации 357
33.3.1 Восстановление конфигурации с помощью FTP 358
33.3.2 Пример восстановления конфигурации с помощью сеанса FTP 359
33.4 Загрузка файлов конфигурации и микропрограммы 359
33.4.1 Загрузка микропрограммы 359
33.4.2 Загрузка файла конфигурации 360
33.4.3 Пример загрузки файлов по FTP из командной строки DOS 361
33.4.4 Пример загрузки микропрограммы с помощью сеанса FTP 361
33.4.5 Загрузка файлов с помощью TFTP 361
33.4.6 Пример команды для загрузки файла с помощью сеанса TFTP 362

Глава 34
Сопровождение системы..... 364

34.1 Режим интерпретатора команд 364
34.2 Контроль вызовов 365
34.2.1 Управление бюджетом 365
34.3 Установка времени и даты 367
34.3.1 Обновление времени 369

Глава 35
Удаленное управление..... 370

35.1 Удаленное управление — общая информация 370
35.2 Удаленное управление 370
35.2.1 Настройка удаленного управления 370
35.2.2 Ограничения на удаленное управление 372
35.3 Удаленное управление и NAT 372

35.4 Время бездействия системы 372

Глава 36
Политика маршрутизации IP (IPPR) 374

36.1 Описание политики маршрутизации IP (IP Policy Routing) 374
36.2 Преимущества политики маршрутизации IP 374
36.3 Политика маршрутизации 375
36.4 Настройка политики маршрутизации IP 375
36.5 Применение политики IP 379
36.5.1 Политики IP для Ethernet 379
36.6 Пример политики маршрутизации IP 380

Глава 37
Расписание вызовов 384

37.1 Введение 384

Глава 38
Поиск и устранение неисправностей..... 388

38.1 Неисправности при запуске интернет-центра 388
38.2 Проблемы с локальной сетью 388
38.3 Проблемы с глобальной сетью (WAN) 389
38.4 Проблемы с доступом к интернет-центру 390
38.4.1 Всплывающие окна, сценарии и разрешения Java 390
38.4.1.1 Блокирование всплывающих окон в Internet Explorer 390
38.4.1.2 Сценарии Java (JavaScripts) 394
38.4.1.3 Разрешения Java 396
38.4.2 Управление элементами ActiveX Internet Explorer 398

Приложение A
Характеристики устройства 402

Приложение B
Инструкции по настенному монтажу 406

Приложение C
Настройка IP-адреса компьютера 408

Windows 95/98/Me..... 408
Windows 2000/NT/XP 411
Macintosh OS 8/9..... 416
Macintosh OS X 418
Linux..... 420
Рис. 256 Проверка конфигурации 424

Приложение D

Организация подсетей IP 426

Адресация IP 426
Классы IP 426
Маска подсети 427
Организация подсетей 428
Пример: две подсети 429
Пример: четыре подсети 430
Пример: восемь подсетей 432
Организация подсетей в сетях класса A и класса B. 433

Приложение E
Команды начальной загрузки 434

Приложение F
Интерпретатор команд 436

Синтаксис команд 436
Использование команд 436

Приложение G
Команды управления межсетевым экраном 438

Приложение H
Команды фильтра NetBIOS 444

Введение 444
Вывод настроек фильтра NetBIOS 444
Настройка фильтров NetBIOS 445

Приложение I
Сплиттеры и микрофильтры 448

Подключение телефонного сплиттера 448
Телефонные микрофильтры 449
Использование интернет-центра с ISDN 449

Приложение J
PPPoE (Протокол "точка-точка" поверх Ethernet) 452

PPPoE в действии 452
Преимущества PPPoE 452
Традиционный сценарий доступа по коммутируемой линии 452
Как работает PPPoE 453
Интернет-центр в качестве клиента PPPoE 453

Приложение K

Беспроводные локальные сети 456

Топологии беспроводных локальных сетей 456
Канал 458
RTS/CTS (Запрос на передачу/Подтверждение готовности к приему) 458
Порог фрагментации 460
Тип заголовка (Preamble Type) 460
IEEE 802.1x 461
RADIUS 461
Методы аутентификации 463
WPA 465
Обзор параметров безопасности 466

Приложение L
Описание сообщений журнала 468

Команды регистрационного журнала 485
Пример команды управления журналом 487

Приложение M
Внутренний генератор таблицы системных параметров (SPTGEN) 488

Внутренний SPTGEN — общая информация 488
Формат текстового файла конфигурации 488
Пример скачивания файла внутреннего генератора таблицы системных параметров по протоколу FTP 490
Пример загрузки внутреннего генератора таблицы системных параметров по протоколу FTP 490
Примеры команд 523

Алфавитный указатель 524

Список рисунков

Рис. 1 Использование защищенного доступа в Интернет 47
Рис. 2 Соединение двух локальных сетей 48
Рис. 3 Светодиоды передней панели P–660HT EE 48
Рис. 4 Окно ввода пароля 51
Рис. 5 Изменение пароля при входе 51
Рис. 6 Web-конфигуратор: окно Site Map (Карта сайта) 53
Рис. 7 Пароль 56
Рис. 8 Мастер установки доступа в Интернет: ISP Parameters (Параметры Интернет-провайдера) 58
Рис. 9 Подключение к Интернету с использованием PPPoE 60
Рис. 10 Подключение к Интернету с использованием RFC 1483 61
Рис. 11 Подключение к Интернету с использованием ENET ENCAP (Протокол маршрутизации канального уровня и инкапсуляцией MAC) 62
Рис. 12 Подключение к Интернету с использованием PPPoA 63
Рис. 13 Мастер установки доступа в Интернет: третье окно 64
Рис. 14 Мастер установки доступа в Интернет: LAN Configuration (Настройки локальной сети) 65
Рис. 15 Мастер установки доступа в Интернет: Connection Tests (Тестирование соединения) 66
Рис. 16 Локальные и глобальные IP-адреса 68
Рис. 17 Пример Any IP 73
Рис. 18 Настройка локальной сети 75
Рис. 19 Wireless LAN (Беспроводная локальная сеть) 80
Рис. 20 Методы защиты беспроводной сети 81
Рис. 21 Окно "Беспроводная связь" (Wireless) 82
Рис. 22 MAC Filter (Фильтр MAC-адресов) 85
Рис. 23 Проверка подлинности с помощью WPA-PSK 87
Рис. 24 Пример применения WPA с RADIUS2 88
Рис. 25 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: No Access Allowed (Доступ запрещен) 90
Рис. 26 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: No Authentication Required (Аутентификация не требуется) 90
Рис. 27 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: 802.1x 92
Рис. 28 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: WPA 95
Рис. 29 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA:WPA-PSK 97
Рис. 30 Local User Database (Встроенная база данных пользователей) 99
Рис. 31 RADIUS 100
Рис. 32 Пример формирования трафика 107
Рис. 33 WAN (Глобальная сеть) 108

Рис. 34 Настройка подключения к глобальной сети (PPPoE) 109
Рис. 35 Пример перенаправления трафика 112
Рис. 36 Настройка локальной сети для перенаправления трафика 113
Рис. 37 WAN Backup (Резервирование глобальной сети) 114
Рис. 38 Как работает NAT 118
Рис. 39 Применение NAT с использованием псевдонимов IP 118
Рис. 40 Пример: несколько серверов расположены за NAT 122
Рис. 41 NAT Mode (Режим NAT) 122
Рис. 42 Edit SUA/NAT Server Set (Редактировать набор серверов SUA/NAT) 124
Рис. 43 Address Mapping Rules (Правила отображения адресов) 126
Рис. 44 Edit Address Mapping Rule (Редактирование правил отображения адресов) .. 128
Рис. 45 Динамическая система доменных имен (DYNDNS) 131
Рис. 46 Time and Date (Время и дата) 132
Рис. 47 Применение межсетевого экрана интернет-центра P–660HT/HTW EE 139
Рис. 48 Трехстороннее квитирование 141
Рис. 49 SYN Flood 141
Рис. 50 Атака Smurf 142
Рис. 51 Инспекция пакетов с учетом состояния 144
Рис. 52 Firewall (Межсетевой экран): Default Policy (Политика по умолчанию) 156
Рис. 53 Firewall (Межсетевой экран): Rule Summary (Список правил) 158
Рис. 54 Firewall (Межсетевой экран): Edit Rule (Редактировать правило) 160
Рис. 55 Firewall (Межсетевой экран): Customized Services (Пользовательские службы) 163
Рис. 56 Firewall (Межсетевой экран): Configure Customized Services (Настройка пользовательских служб) 164
Рис. 57 Пример правила межсетевого экрана: Rule Summary (Список правил) 165
Рис. 58 Пример правила межсетевого экрана: Edit Rule (Редактировать правило): Destination Address (Адрес получателя) 166
Рис. 59 Пример редактирования настроек пользовательского порта 166
Рис. 60 Пример правила межсетевого экрана: Edit Rule (Редактировать правило): Select Customized Services (Выбор пользовательских служб) 167
Рис. 61 Пример правила межсетевого экрана: Rule Summary (Список правил): My Service (Моя служба) 168
Рис. 62 Firewall (Межсетевой экран): Anti Probing (Блокирование эхо-тестирования) . 172
Рис. 63 Firewall (Межсетевой экран): Threshold (Пороговое значение) 175
Рис. 64 Фильтрация на основе содержания (контентная фильтрация) 179
Рис. 65 Content Filter (Контент-фильтр): Keyword (Ключевое слово) 180
Рис. 66 Content Filter (Контент-фильтр): Schedule (График) 181
Рис. 67 Content Filter (Контент-фильтр): Trusted (Доверенные) 182
Рис. 68 Настройка Telnet в сети TCP/IP 186
Рис. 69 Удаленное управление 187
Рис. 70 Настройка UPnP 190
Рис. 71 Установка и удаление программ: Установка Windows: Связь 191
Рис. 72 Установка и удаление программ: Установка Windows: Связь: Компоненты 192

Рис. 73 Сетевые подключения 192
Рис. 74 Мастер установки дополнительных компонентов Windows 193
Рис. 75 Сетевые службы 194
Рис. 76 Сетевые подключения 195
Рис. 77 Internet Connection Properties (Свойства подключения к Интернет) 196
Рис. 78 Internet Connection Properties (Свойства подключения к Интернет): Advanced Settings (Дополнительные настройки) 197
Рис. 79 Internet Connection Properties (Свойства подключения к Интернет): Advanced Settings (Дополнительные настройки): Add (Добавить) 197
Рис. 80 Значок в области уведомлений (на панели задач) 198
Рис. 81 Состояние подключения к Интернет 198
Рис. 82 Сетевые подключения 199
Рис. 83 Сетевые подключения: Сетевое окружение 200
Рис. 84 Сетевые подключения: Сетевое окружение: Свойства: Пример 200
Рис. 85 Log Settings (Настройки журналов) 204
Рис. 86 Просмотр журналов 206
Рис. 87 Пример журнала, высылаемого по E-mail 208
Рис. 88 Пример управления пропускной способностью на основе приложения 212
Рис. 89 Пример управления пропускной способностью на основе подсети 212
Рис. 90 Пример управления пропускной способностью на основе приложения и подсети 213
Рис. 91 Пример распределения пропускной способности 215
Рис. 92 Пример увеличения использования пропускной способности 216
Рис. 93 Media Bandwidth Mgnt (Управление пропускной способностью среды передачи) 217
Рис. 94 Media Bandwidth Management (Управление пропускной способностью среды передачи): Summary (Общие настройки) 218
Рис. 95 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Setup (Настройка классов пропускной способности) 220
Рис. 96 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Configuration (Параметры класса) 221
Рис. 97 Управление пропускной способностью среды передачи — Статистика 224
Рис. 98 Media Bandwidth Management (Управление пропускной способностью среды передачи): Monitor (Монитор) 225
Рис. 99 System Status (Состояние системы) 227
Рис. 100 System Status (Состояние системы): Show Statistics (Показать статистику) . 229
Рис. 101 Таблица DHCP 231
Рис. 102 Таблица Any IP (Любой IP) 232
Рис. 103 Association List (Список соединений) 233
Рис. 104 Diagnostic (Диагностика): General (Общая) 234
Рис. 105 Diagnostic (Диагностика): DSL Line (DSL линия) 235
Рис. 106 Firmware Upgrade (Обновление микропрограммы) 237
Рис. 107 Временное отключение сети 238
Рис. 108 Error Message (Сообщение об ошибке) 238
Рис. 109 Экран регистрации 241

Рис. 110 Меню 23.1 — Изменение пароля 247
Рис. 111 Меню 1 — Настройка общих параметров 249
Рис. 112 Меню 1.1 — Настройка динамической DNS 250
Рис. 113 Меню 2 — Настройка резервирования глобальной сети 253
Рис. 114 Меню 2.1 — Настройка перенаправления трафика 254
Рис. 115 Меню 3 — Настройка локальной сети 256
Рис. 116 Меню 3.1 — Настройка фильтра порта LAN 257
Рис. 117 Меню 3.2 — Настройка TCP/IP и DHCP для Ethernet 258
Рис. 118 Меню 3.5 — Настройка беспроводной локальной сети 261
Рис. 119 Меню 3.5.1 Фильтр MAC-адресов беспроводной сети 263
Рис. 120 Пример сети с использованием псевдонимов IP 265
Рис. 121 Меню 3.2 — Настройка TCP/IP и DHCP 265
Рис. 122 Меню 3.2.1 — Настройка псевдонима IP 266
Рис. 123 Меню 1 — Настройка общих параметров 267
Рис. 124 Меню 4 — Настройка доступа в Интернет 268
Рис. 125 Меню 11 — Настройка удаленного узла 271
Рис. 126 Меню 11.1 — Профиль удаленного узла 272
Рис. 127 Меню 11.3 — Параметры сетевого уровня удаленного узла 275
Рис. 128 Пример IP-адресов для соединения локальных сетей на базе TCP/IP 277
Рис. 129 Меню 11.5 — Фильтр удаленного узла (инкапсуляция RFC 1483 или ENET) 277
Рис. 130 Меню 11.5 — Фильтр удаленного узла (инкапсуляция RFC или ENET) 278
Рис. 131 Меню 11.6 — Мультиплексирование на базе VC 279
Рис. 132 Меню 11.6 — Мультиплексирование на базе LLC или инкапсуляция PPP 279
Рис. 133 Меню 11.1 — Профиль удаленного узла 280
Рис. 134 Меню 11.8 — Параметры дополнительной настройки 280
Рис. 135 Пример топологии статической маршрутизации 282
Рис. 136 Меню 12 - Настройка статического маршрута 283
Рис. 137 Меню 12.1 — Настройка статического маршрута IP 283
Рис. 138 Меню 12.1.1 — Редактирование статического маршрута IP 283
Рис. 139 Меню 11.1 — Профиль удаленного узла 287
Рис. 140 Меню 11.3 — Параметры сетевого уровня удаленного узла 287
Рис. 141 Меню 12.3.1 — Редактировать статический маршрут для моста 288
Рис. 142 Меню 4 — Применение NAT для доступа в Интернет 291
Рис. 143 Применение NAT в Меню 4 и Меню 11.3 291
Рис. 144 Меню 15 — Настройка NAT 292
Рис. 145 Меню 15.1 — Наборы отображения адресов 293
Рис. 146 Меню 15.1.255 — Правила отображения адресов SUA 293
Рис. 147 Меню 15.1.1 — Первый набор 295
Рис. 148 Меню 15.1.1.1 — Редактирование/создание конкретного правила в наборе 296
Рис. 149 Меню 15.2 — Настройка серверов за NAT 298
Рис. 150 Меню 15.2.1 — Настройка серверов за NAT 298
Рис. 151 Пример: Несколько серверов расположены за NAT 299
Рис. 152 Пример применения NAT 1 300

Рис. 153 Меню 4 — Пример доступа в Интернет при использовании NAT 300
Рис. 154 Пример применения NAT 2 301
Рис. 155 Меню 15.2.1 — Определение внутреннего сервера 301
Рис. 156 Пример применения NAT 3 302
Рис. 157 Пример 3: Меню 11.3 303
Рис. 158 Пример 3: Меню 15.1.1.1 303
Рис. 159 Пример 3: Окончательный вид Меню 15.1.1 304
Рис. 160 Пример 3: Меню 15.2.1 304
Рис. 161 Пример применения NAT 4 305
Рис. 162 Пример 4: Меню 15.1.1.1 — Правило отображения адресов 305
Рис. 163 Пример 4: Меню 15.1.1 — Правила отображения адресов 306
Рис. 164 Меню 21.2 — Firewall Setup (Настройка межсетевого экрана) 309
Рис. 165 Процесс фильтрации исходящего пакета 311
Рис. 166 Процесс реализации правил фильтра 312
Рис. 167 Меню 21 — Filter Set Configuration (Настройка наборов фильтров) 313
Рис. 168 Список правил фильтра NetBIOS_WAN 314
Рис. 169 Список правил фильтра NetBIOS_LAN 315
Рис. 170 Список правил фильтра IGMP 315
Рис. 171 Меню 21.1.x.1 — TCP/IP Filter Rule (Правило фильтра TCP/IP) 318
Рис. 172 Применение фильтра IP 320
Рис. 173 Меню 21.1.5.1 — Generic Filter Rule (Правило фильтра общего типа) 321
Рис. 174 Наборы фильтров протоколов и фильтров устройств 323
Рис. 175 Пример фильтра Telnet 323
Рис. 176 Меню 21.1.6.1 — Пример фильтра 324
Рис. 177 Меню 21.1.6.1 — Список правил фильтра, созданного в примере 325
Рис. 178 Фильтрация трафика Ethernet 326
Рис. 179 Filtering Remote Node Traffic (Фильтрация трафика удаленного узла) 326
Рис. 180 Модель управления SNMP 328
Рис. 181 Меню 22 — SNMP Configuration (Настройка SNMP) 330
Рис. 182 Меню 23 — System Security (Системные функции безопасности) 332
Рис. 183 Меню 23.2 — System Security (Системные функции безопасности): RADIUS Server (Сервер RADIUS) 333
Рис. 184 Меню 23 — System Security (Системные функции безопасности) 334
Рис. 185 Меню 23.4 — System Security (Системные функции безопасности): IEEE 802.1x 335
Рис. 186 Меню 14 — Dial-in User Setup (Настройка подключения удаленного пользователя) 338
Рис. 187 Меню 14.1 — Edit Dial-in User (Редактирование настроек удаленного коммутируемого пользователя) 339
Рис. 188 Меню 24 — System Maintenance (Сопровождение системы) 340
Рис. 189 Меню 24.1 — System Maintenance (Сопровождение системы): Status (Состояние) 341
Рис. 190 Меню 24.2 — System Information and Console Port Speed (Информация о системе и скорость консольного порта) 343

Рис. 191 Меню 24.2.1 — System Maintenance (Сопровождение системы): Information (Информация) 344
Рис. 192 Меню 24.2.2 — System Maintenance (Сопровождение системы): Change Console Port Speed (Изменение скорости консольного порта) 345
Рис. 193 Меню 24.3 — System Maintenance (Сопровождение системы): Log and Trace (Журнал регистрации и трассировка) 346
Рис. 194 Пример уведомлений и сообщений об ошибках 346
Рис. 195 Меню 24.3.2 — System Maintenance (Сопровождение системы): Syslog and Accounting (Системный журнал и учет ресурсов) 347
Рис. 196 Пример системного журнала 347
Рис. 197 Меню 24 — System Maintenance (Сопровождение системы): Diagnostic (Диагностика) 349
Рис. 198 Сеанс Telnet в Меню 24.5 354
Рис. 199 Пример сеанса FTP 355
Рис. 200 Установка соединения Telnet в Меню 24.6 358
Рис. 201 Пример восстановления конфигурации с помощью сеанса FTP 359
Рис. 202 Подключение Telnet в Menu 24.7.1 — Upload System Firmware (Загрузка системной микропрограммы) 360
Рис. 203 Подключение с помощью Telnet в Меню 24.7.2 — System Maintenance (Сопровождение системы) 360
Рис. 204 Пример загрузки микропрограммы с помощью сеанса FTP 361
Рис. 205 Режим интерпретатора команд в Меню 24 364
Рис. 206 Доступные команды 365
Рис. 207 Меню 24.9 — System Maintenance (Сопровождение системы): Call Control (Контроль вызовов) 365
Рис. 208 Меню 24.9.1 — System Maintenance (Сопровождение системы): Budget Management (Управление бюджетом) 366
Рис. 209 Меню 24 — System Maintenance (Сопровождение системы) 367
Рис. 210 Меню 24.10 — System Maintenance (Сопровождение системы): Time and Date Setting (Установка времени и даты) 368
Рис. 211 Меню 24.11 — Remote Management Control (Контроль удаленного управления) 371
Рис. 212 Меню 25 — IP Routing Policy Setup (Настройка политики маршрутизации IP) 375
Рис. 213 Меню 25.1 — IP Routing Policy Setup (Настройка политики маршрутизации IP) 377
Рис. 214 Меню 25.1.1 — IP Routing Policy (Политика маршрутизации IP) 378
Рис. 215 Меню 3.2 — Настройка TCP/IP и DHCP для Ethernet 380
Рис. 216 Меню 11.3 — Remote Node Network Layer Options (Параметры сетевого уровня удаленного узла) 380
Рис. 217 Пример политики маршрутизации IP 381
Рис. 218 Пример политики маршрутизации IP 382
Рис. 219 Пример политики маршрутизации IP 383
Рис. 220 Пример применения политик IP 383
Рис. 221 Меню 26 — Schedule Setup (Создание расписания) 384
Рис. 222 Меню 26.1 — Schedule Set Setup (Создание набора расписания) 385

Рис. 223 Применение расписания к удаленному узлу (PPPoE) 387
Рис. 224 Блокирование всплывающих окон 391
Рис. 225 Свойства обозревателя 392
Рис. 226 Свойства обозревателя 393
Рис. 227 Параметры блокирования всплывающих окон 394
Рис. 228 Свойства обозревателя 395
Рис. 229 Параметры безопасности — Выполнение сценариев приложений Java 396
Рис. 230 Параметры безопасности — Java 397
Рис. 231 Java (Sun) 398
Рис. 232 Свойства обозревателя — Безопасность 399
Рис. 233 Параметры безопасности — элементы ActiveX 400
Рис. 234 Пример настенного монтажа 406
Рис. 235 Windows 95/98/Me: Network (Сеть): Configuration (Конфигурация) 409
Рис. 236 Windows 95/98/Me: TCP/IP Properties (Свойства: TCP/IP): IP Address (IP-адрес) 410
Рис. 237 Windows 95/98/Me: TCP/IP Properties (Свойства: TCP/IP): DNS Configuration (Конфигурация DNS) 411
Рис. 238 Windows XP: Меню start (пуск) 412
Рис. 239 Windows XP: Control Panel (Панель управления) 412
Рис. 240 Windows XP: Control Panel (Панель управления): Network Connections (Сетевые подключения): Properties (Свойства) 413
Рис. 241 Windows XP: Local Area Connection Properties (Подключение по локальной сети — свойства) 413
Рис. 242 Windows XP: Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP)) 414
Рис. 243 Windows XP: Advanced TCP/IP Properties (Дополнительные параметры TCP/IP) 415
Рис. 244 Windows XP: Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP)) 416
Рис. 245 Macintosh OS 8/9: Меню Apple 417
Рис. 246 Macintosh OS 8/9: TCP/IP 418
Рис. 247 Macintosh OS X: Меню Apple 419
Рис. 248 Macintosh OS X: Сеть 419
Рис. 249 Red Hat 9.0: KDE: Network Configuration (Конфигурация сети): Devices (Устройства) 420
Рис. 250 Red Hat 9.0: KDE: Ethernet Device (Устройство Ethernet): General (общие) ... 421
Рис. 251 Red Hat 9.0: KDE: Network Configuration (Конфигурация сети): DNS 422
Рис. 252 Red Hat 9.0: KDE: Network Configuration (Конфигурация сети): Activate (Активировать) 422
Рис. 253 Red Hat 9.0: Настройка динамического IP-адреса (Dynamic IP Address Setting) в файле ifconfig-eth0 423
Рис. 254 Red Hat 9.0: Настройка статического IP-адреса (Dynamic IP Address Setting) в файле ifconfig-eth0 423
Рис. 255 Red Hat 9.0: Настройки DNS в файле resolv.conf 423
Рис. 256 Red Hat 9.0: Restart Ethernet Card (Перезагрузить карту Ethernet) 424

Рис. 257 Red Hat 9.0: Checking TCP/IP Properties (Проверка свойств TCP/IP) 424
Рис. 258 Функция входа в режим отладки 434
Рис. 259 Команды модуля начальной загрузки 435
Рис. 260 Подключение телефонного сплиттера 448
Рис. 261 Подключение микрофильтра 449
Рис. 262 Использование интернет-центра с ISDN 450
Рис. 263 Конфигурация оборудования "один маршрутизатор для одного компьютера" 453
Рис. 264 Интернет-центр в качестве клиента PPPoE 454
Рис. 265 Одноранговая связь во временной (Ad-hoc) беспроводной сети 456
Рис. 266 Базовый набор служб 457
Рис. 267 Фиксированная беспроводная сеть 458
Рис. 268 RTS/CTS 459
Рис. 269 Пример отображения категорий регистрационных записей 485
Рис. 270 Пример отображения параметров регистрационных записей 486
Рис. 271 Формат текстового файла конфигурации: описания столбцов 489
Рис. 272 Введен неверный параметр: пример сообщения в командной строке 489
Рис. 273 Введен корректный параметр: пример сообщения в командной строке 490
Рис. 274 Пример скачивания файла внутреннего генератора таблицы системных параметров по протоколу FTP 490
Рис. 275 Пример загрузки внутреннего генератора таблицы системных параметров по протоколу FTP 491

Список таблиц

Табл. 1 Стандарты ADSL 42
Табл. 2 Светодиоды передней панели 48
Табл. 3 Сводная таблица окон Web-конфигуратора 53
Табл. 4 Пароль 56
Табл. 5 Мастер установки доступа в Интернет: ISP Parameters (Параметры Интернет-провайдера) 59
Табл. 6 Подключение к Интернету с использованием PPPoE 60
Табл. 7 Подключение к Интернету с использованием RFC 1483 61
Табл. 8 Подключение к Интернету с использованием ENET ENCAP 62
Табл. 9 Подключение к Интернету с использованием PPPoA 63
Табл. 10 Мастер установки доступа в Интернет: LAN Configuration (Настройки локальной сети) 65
Табл. 11 LAN Setup (Настройка локальной сети) 75
Табл. 12 Wireless LAN (Беспроводная локальная сеть) 80
Табл. 13 Wireless LAN (Беспроводная сеть) 82
Табл. 14 Фильтр MAC-адресов 85
Табл. 15 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: No Access/ Authentication 90
Табл. 16 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: 802.1x 92
Табл. 17 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: WPA 95
Табл. 18 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: WPA-PSK 97
Табл. 19 Local User Database (Встроенная база данных пользователей) 99
Табл. 20 RADIUS 100
Табл. 21 WAN 108
Табл. 22 WAN Setup (Настройка глобальной сети) 109
Табл. 23 Резервирование глобальной сети 114
Табл. 24 Определения NAT 116
Табл. 25 Типы отображения NAT 119
Табл. 26 Службы и номера портов 121
Табл. 27 NAT Mode (Режим NAT) 122
Табл. 28 Редактировать набор серверов SUA/NAT 124
Табл. 29 Address Mapping Rules (Правила отображения адресов) 126
Табл. 30 Edit Address Mapping Rule (Редактирование правил отображения адресов) 128
Табл. 31 Динамическая система доменных имен (DYNDNS) 131
Табл. 32 Время и дата 133
Табл. 33 Общепринятые порты IP 140
Табл. 34 Команды ICMP, выдающие предупреждение 142
Табл. 35 Команды NetBIOS 143
Табл. 36 Команды SMTP 143

Табл. 37 Firewall (Межсетевой экран): Default Policy (Политика по умолчанию) 156
Табл. 38 Rule Summary (Список правил) 158
Табл. 39 Firewall (Межсетевой экран): Edit Rule (Редактировать правило) 161
Табл. 40 Customized Services (Пользовательские службы) 163
Табл. 41 Firewall (Межсетевой экран): Configure Customized Services (Настройка пользовательских служб) 164
Табл. 42 Предварительно настроенные службы 169
Табл. 43 Firewall (Межсетевой экран): Anti Probing (Блокирование эхо-тестирования) 172
Табл. 44 Firewall (Межсетевой экран): Threshold (Пороговое значение) 175
Табл. 45 Фильтрация на основе содержания (контентная фильтрация) 179
Табл. 46 Content Filter (Контент-фильтр): Keyword (Ключевое слово) 180
Табл. 47 Content Filter (Контент-фильтр): Schedule (График) 181
Табл. 48 Content Filter (Контент-фильтр): Trusted (Доверенные) 182
Табл. 49 Удаленное управление 187
Табл. 50 Настройка UPnP 190
Табл. 51 Log Settings (Настройки журналов) 204
Табл. 52 Просмотр журналов 206
Табл. 53 Сообщения об ошибках SMTP 207
Табл. 54 Пример управления пропускной способностью на основе приложения и подсети 212
Табл. 55 Media Bandwidth Mgnt (Управление пропускной способностью среды передачи) 217
Табл. 56 Media Bandwidth Management (Управление пропускной способностью среды передачи): Summary (Общие настройки) 218
Табл. 57 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Setup (Настройка классов пропускной способности) 220
Табл. 58 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Configuration (Параметры класса) 221
Табл. 59 Службы и номера портов 223
Табл. 60 Media Bandwidth Management Statistics (Управление пропускной способностью среды передачи: Статистика) 224
Табл. 61 Media Bandwidth Management (Управление пропускной способностью среды передачи): Monitor (Монитор) 225
Табл. 62 Состояние системы 227
Табл. 63 Состояние системы: Показать статистику 229
Табл. 64 Таблица DHCP 231
Табл. 65 Таблица Any IP (Любой IP) 232
Табл. 66 Association List (Список соединений) 233
Табл. 67 Diagnostic (Диагностика): General (Общая) 234
Табл. 68 Diagnostic (Диагностика): DSL Line (DSL линия) 235
Табл. 69 Firmware Upgrade (Обновление микропрограммы) 237
Табл. 70 Обзор меню SMT модема 241
Табл. 71 Работа с интерфейсом SMT 244
Табл. 72 Главное меню SMT 245

Табл. 73 Обзор Главного меню 245
Табл. 74 Меню 1 — Настройка общих параметров 249
Табл. 75 Меню 1.1 — Настройка динамической DNS 250
Табл. 76 Меню 2 — Настройка резервирования глобальной сети 253
Табл. 77 Меню 2.1 — Настройка перенаправления трафика 254
Табл. 78 Настройка DHCP для Ethernet 258
Табл. 79 Настройка TCP/IP порта Ethernet 259
Табл. 80 Меню 3.5 — Настройка беспроводной локальной сети 261
Табл. 81 Меню 3.5.1 Фильтр MAC-адресов беспроводной сети 263
Табл. 82 Меню 3.2.1 — Настройка псевдонима IP 266
Табл. 83 Меню 4 — Настройка доступа в Интернет 268
Табл. 84 Меню 11.1 — Профиль удаленного узла 272
Табл. 85 Меню 11.3 — Параметры сетевого уровня удаленного узла 275
Табл. 86 Меню 11.8 — Параметры дополнительной настройки 280
Табл. 87 Меню 12.1.1 — Редактирование статического маршрута IP 284
Табл. 88 Параметры сетевого уровня удаленного узла: Поля для настройки моста .. 287
Табл. 89 Меню 12.3.1 — Редактировать статический маршрут для моста 288
Табл. 90 Применение NAT в Меню 4 и Меню 11.3 292
Табл. 91 Правила отображения адресов SUA 293
Табл. 92 Меню 15.1.1 — Первый набор 296
Табл. 93 Меню 15.1.1.1 — Редактирование/создание конкретного правила в наборе 297
Табл. 94 Сокращения, используемые в меню Filter Rules Summary (Список правил фильтра) 315
Табл. 95 Сокращения, используемые в правилах 316
Табл. 96 Меню 21.1.x.1 — Правило фильтра TCP/IP 318
Табл. 97 Меню 21.1.5.1 — Generic Filter Rule (Правило фильтра общего типа) 321
Табл. 98 Таблица наборов фильтров 325
Табл. 99 Меню 22 — SNMP Configuration (Настройка SNMP) 330
Табл. 100 Прерывания SNMP 331
Табл. 101 Порты и постоянные виртуальные каналы 331
Табл. 102 Меню 23.2 — System Security (Системные функции безопасности): RADIUS Server (Сервер RADIUS) 333
Табл. 103 Меню 23.4 — System Security (Системные функции безопасности): IEEE 802.1x 335
Табл. 104 Меню 14.1 — Edit Dial-in User (Редактирование настроек удаленного коммутируемого пользователя) 339
Табл. 105 Меню 24.1 — System Maintenance (Сопровождение системы): Status (Состояние) 341
Табл. 106 Меню 24.2.1 — System Maintenance (Сопровождение системы): Information (Информация) 344
Табл. 107 Меню 24.3.2 — System Maintenance (Сопровождение системы): Syslog and Accounting (Системный журнал и учет ресурсов) 347
Табл. 108 Меню 24 — System Maintenance (Сопровождение системы): Diagnostic (Диагностика) 350
Табл. 109 Структура имен файлов 353

Табл. 110 Основные команды для клиентов FTP на основе GUI 355
Табл. 111 Основные команды клиентов TFTP на основе GUI 357
Табл. 112 Меню 24.9.1 — System Maintenance (Сопровождение системы): Budget Management (Управление бюджетом) 366
Табл. 113 Меню 24.10 — System Maintenance (Сопровождение системы): Time and Date Setting (Установка времени и даты) 368
Табл. 114 Меню 24.11 — Remote Management Control (Контроль удаленного управления) 371
Табл. 115 Меню 25.1 — IP Routing Policy Setup (Настройка политики маршрутизации IP) 377
Табл. 116 Меню 25.1.1 — IP Routing Policy (Политика маршрутизации IP) 378
Табл. 117 Меню 26.1 — Schedule Set Setup (Создание набора расписания) 385
Табл. 118 Устранение неполадок при запуске интернет-центра P–660HT/HTW EE ... 388
Табл. 119 Устранение неисправностей в локальной сети 388
Табл. 120 Поиск и устранение неполадок с WAN 389
Табл. 121 Проблемы с доступом к интернет-центру 390
Табл. 122 Фильтры 402
Табл. 123 Firmware (Микропрограмма) 403
Табл. 124 Классы IP-адресов 426
Табл. 125 Допустимые диапазоны IP-адресов для каждого класса 427
Табл. 126 “Естественные” маски 427
Табл. 127 Альтернативные варианты записи маски подсети 428
Табл. 128 Пример организации 2-х подсетей 429
Табл. 129 Подсеть 1 429
Табл. 130 Подсеть 2 430
Табл. 131 Подсеть 1 430
Табл. 132 Подсеть 2 431
Табл. 133 Подсеть 3 431
Табл. 134 Подсеть 4 431
Табл. 135 Восемь подсетей 432
Табл. 136 Организация подсетей класса C 432
Табл. 137 Организация подсетей класса B 433
Табл. 138 Команды управления межсетевым экраном 438
Табл. 139 Настройки фильтров NetBIOS по умолчанию 445
Табл. 140 IEEE 802.11g 461
Табл. 141 Сравнительный анализ методов аутентификации EAP 465
Табл. 142 Сравнительная таблица беспроводной безопасности 466
Табл. 143 Журнальные сообщения, связанные с обслуживанием системы 468
Табл. 144 Журнальные сообщения о системных ошибках 469
Табл. 145 Журнальные сообщения, связанные с управлением доступом 469
Табл. 146 Журнальные сообщения о сбросе сеансов TCP 470
Табл. 147 Журнальные сообщения о фильтре пакетов 471
Табл. 148 Журнальные сообщения ICMP (протокол межсетевых управляющих сообщений) 471

Табл. 149 Журнальные сообщения CDR (журнала регистрации вызовов) 472
Табл. 150 Журнальные сообщения PPP (протокола "точка-точка") 472
Табл. 151 Журнальные сообщения UPnP 473
Табл. 152 Журнальные сообщения о фильтрации содержания 473
Табл. 153 Журнальные сообщения об атаках 474
Табл. 154 Журнальные сообщения IPSec 475
Табл. 155 Журнальные сообщения протокола обмена ключами (IKE) 475
Табл. 156 Журнальные сообщения PKI (инфраструктуры сертификации открытых ключей) 479
Табл. 157 Коды причин непрохождения сверки путей сертификатов 480
Табл. 158 Журнальные сообщения 802.1X 481
Табл. 159 Настройка списка управления доступом (ACL) 482
Табл. 160 Записи ICMP 483
Табл. 161 Сообщения системного журнала 484
Табл. 162 Типы данных сообщений RFC-2408 ISAKMP 484
Табл. 163 Сокращения, использованные в экранных формах внутреннего генератора таблицы системных параметров 491
Табл. 164 Меню 1 Общая настройка (SMT-меню 1) 491
Табл. 165 Меню 3 (SMT-меню 3) 492
Табл. 166 Меню 4 — Internet Access Setup (Настройка доступа в Интернет) (SMT-меню 4) 496
Табл. 167 Меню 12 (SMT-меню 12) 498
Табл. 168 Меню 15 — SUA Server Setup (Настройка сервера SUA) (SMT-меню 15) .. 506
Табл. 169 Меню 21.1 — Filter set #1 (Набор фильтров #1) (SMT-меню 21.1) 509
Табл. 170 Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1) 515
Табл. 171 Меню 23 — System Menus (Системные меню) (SMT-меню 23) 521
Табл. 172 Меню 24.11 — Remote Management Control (Удаленное управление) (SMT-меню 24.11) 522
Табл. 173 Примеры команд 523

Предисловие

Поздравляем Вас с приобретением интернет-центра ZyXEL. Модель P–660HTW EE имеет встроенный модуль беспроводной связи стандарта IEEE 802.11g. В моделях P–660HT EE и P–660HTW EE имеется 4-портовый коммутатор, позволяющий подключать к интернет-центру до 4 компьютеров, не приобретая отдельный коммутатор или концентратор.

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

О данном Руководстве пользователя

В данном руководстве описывается настройка устройства P–660HT/HTW EE для различных применений. В разделах руководства о Web-конфигураторе содержится вводная информация по функциям устройства, настраиваемым с помощью Web-конфигуратора. В разделах руководства, посвященных SMT, содержится вводная информация только по функциям устройства, которые нельзя настроить с помощью Web-конфигуратора.

ПРИМЕЧАНИЕ: Для настройки устройства P–660HT/HTW EE используются Web-конфигуратор, SMT (System Management Terminal — системная консоль) и интерфейс интерпретатора команд. Не все интерфейсы обеспечивают настройку всех функций устройства.

Условные обозначения

- “Введите” означает, что Вам следует напечатать один или более символов. "Выберите" означает, что Вам следует использовать одну из стандартных опций.
- Заголовки и названия полей меню SMT выполнены **полужирным шрифтом Times New Roman**. Стандартные пункты меню выполнены **полужирным шрифтом Arial**. Названия команд и клавиш со стрелками заключены в квадратные скобки. [ENTER] обозначает клавишу "Enter" или клавишу возврата каретки. [ESC] обозначает клавишу "Escape", а [Space Bar] обозначает клавишу пробела.
- Действия в последовательности операций, выполняемых с помощью мыши, разделяются запятой. Например, “щелкните по значку Apple, **Control Panels (Панели управления)** и затем **Modem (Модем)**” означает, что сначала нужно щелкнуть по значку Apple, затем щелкнуть **Control Panels (Панели управления)** и затем щелкнуть **Modem (Модем)**.
- Для краткости в данном руководстве будет использоваться "напр." вместо "например" и "т. е." вместо "то есть" и "другими словами".

- Далее в данном Руководстве модели P-600H/HTW EE могут именоваться как "P–660HT/HTW EE" либо обозначаться словами: "интернет-центр", "модем ADSL", "маршрутизатор", "Prestige".

Сопроводительная документация

- Справочный компакт-диск

  На компакт-диске, входящем в комплект поставки, находится справочная документация.

- Краткое руководство

  Краткое руководство разработано с целью помочь Вам изучить устройство и начать работать с ним. Оно содержит информацию по подключению оборудования и инструкции для начала работы.

- Встроенная справка Web-конфигуратора

  Встроенная справка по технологии web при работе с конкретными окнами, а также дополнительная информация.

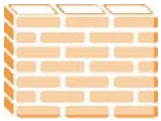
- Глоссарий и Web-сайт корпорации ZyXEL

  Для получения интерактивного глоссария с основными сетевыми терминами, а также дополнительной документации обратитесь на сайт www.zyxel.com.

Обратная связь с пользователем

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.

Пояснения к графическим значкам

Интернет-центр P–660HT/HTW EE	Компьютер	Ноутбук
Сервер	DSL-коммутатор (DSLAM)	Межсетевой экран 
Телефон	Коммутатор	Маршрутизатор
Сигнал беспроводного доступа		

Введение в DSL

Технология DSL (Digital Subscriber Line/Цифровая абонентская линия) увеличивает производительность передачи данных по существующим линиям связи "витая пара", которые соединяют телефонные станции местных телефонных компаний и большинство домашних и офисных телефонов. В то время как сам кабель может работать на более высоких частотах, коммутационное оборудование телефонных станций отсекает сигналы с частотой выше 4000 Гц с целью отфильтровывания помех на линии голосовой связи. Однако в настоящий момент идет поиск способов увеличения пропускной способности телефонных линий для облегчения доступа во всемирную сеть и поэтому используются технологии DSL.

Существует семь типов услуг DSL в зависимости от скорости (от 16 кбит/с до 52 Мбит/с). Услуги являются либо симметричными (одинаковая скорость трафика в обоих направлениях), либо несимметричными (объем входящего трафика больше, чем объем исходящего трафика). Несимметричные услуги (ADSL) подходят, прежде всего, для пользователей Интернета, так как при этом обычно принимается больше информации, чем передается. Например, простым нажатием на кнопку в web-браузере можно запустить расширенную загрузку, включающую графику и текст.

При возрастании скорости передачи данных, уменьшается расстояние передачи. Это означает, что пользователи, которые находятся дальше определенного расстояния от центральной телефонной станции, не смогут работать на высоких скоростях.

Соединение DSL представляет собой выделенный канал "точка-точка", что означает, что соединение существует постоянно, и выполнение вызова не требуется.

Введение в ADSL

ASDL представляет собой несимметричную технологию, что означает, что скорость входящего трафика гораздо выше, чем скорость исходящего трафика. Как уже было сказано, эта технология прекрасно подходит для обычных сеансов связи в Интернете, при которых загружается больше информации, например, с Web-серверов, чем отсылается. ADSL работает в диапазоне частот, который расположен выше частотного диапазона голосовых услуг, поэтому обе системы могут работать по одному кабелю.

Глава 1
Знакомство с интернет-центром P–660HT/HTW EE

В этой главе описываются основные функции и варианты применения интернет-центра P–660HT/HTW EE.

1.1 Знакомство с интернет-центром P–660HT/HTW EE

P–660HT/HTW EE — это интернет-центр стандарта ADSL2+, обеспечивающий сверхбыстрый и безопасный доступ в Интернет по аналоговым (POTS) и цифровым (ISDN) телефонным линиям (в зависимости от конкретной модели).

Литера “H” в наименовании модели P–660HT/HTW EE обозначает встроенный 4-портовый коммутатор, а “W” - наличие беспроводного сетевого адаптера для подключения к беспроводной сети, “T” - тип встроенного модема ADSL2+.

“1” в конце номера модели (например, P-660HW-T1), обозначает устройство, работающее через аналоговую телефонную систему POTS (традиционная телефонная сеть общего пользования). "3" в конце номера модели обозначает устройство, работающее через ISDN (Integrated Services Digital Network — Цифровая сеть с предоставлением комплексных услуг). “7” в конце номера модели, обозначает устройство, работающее через T-ISDN (UR-2).

ПРИМЕЧАНИЕ: Необходимо использовать микропрограммное обеспечение P–660HT/HTW EE строго в соответствии с конкретной моделью устройства. См. наклейку, находящуюся на нижней панели интернет-центра P–660HT/HTW EE.

Модели DSL RJ-11 (ADSL с подключением через POTS) или RJ-45 (ADSL с подключением через ISDN) подключаются к телефонной линии, обеспечивающей подключение по ADSL. P–660HT/HTW EE совместим со стандартами ADSL/ADSL2/ADSL2+. Максимальные скорости передачи данных, достигаемые P–660HT/HTW EE для каждого стандарта, представлены в следующей таблице.

Табл. 1 Стандарты ADSL

СТАНДАРТ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ	ПЕРЕДАЧА ДАННЫХ	ПРИЕМ ДАННЫХ
ADSL	832 Кбит/с	8 Мбит/с

Табл. 1 Стандарты ADSL

СТАНДАРТ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ	ПЕРЕДАЧА ДАННЫХ	ПРИЕМ ДАННЫХ
ADSL2	3,5 Мбит/с	12 Мбит/с
ADSL2+	3,5 Мбит/с	24 Мбит/с

ПРИМЕЧАНИЕ: Стандарт, который поддерживает ваш Интернет-провайдер, 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 Характеристики

В следующих разделах описаны функции интернет-центра P–660HT/HTW EE.

ПРИМЕЧАНИЕ: Более подробное описание функций и информацию по стандартам см. в технических характеристиках изделия (в Приложении).

Высокоскоростной доступ в Интернет

P–660HT/HTW EE поддерживает стандарты ADSL/ADSL2/ADSL2+ со скоростью приема данных до 24 Мбит/с и скорость передачи данных до 3,5 Мбит/с. Фактически достигаемые скорости зависят также от тарифного плана ADSL, растояния до Интернет-провайдера, качества линии и т.д.

Доступ в Интернет с использованием автоматической настройки модема (Zero Configuration)

После подключения и включения интернет-центр P–660HT/HTW EE автоматически определяет настройки подключения к Интернету (такие как номер VCI/VPI и метод инкапсуляции) через Интернет-провайдера и выполняет необходимые изменения в конфигурации. В случае, если требуется ввод данных учетной записи Интернет (таких как имя пользователя и пароль) или если интернет-центр не может подключиться к оборудованию Интернет-провайдера, на экране появляется окно(а) для ввода регистрационной информации или поиска и устранения неисправностей.

Any IP (Любой IP)

Функция Any IP (Любой IP) позволяет компьютеру получить доступ в Интернет и к настройкам P–660HT/HTW EE без изменения сетевых параметров компьютера (таких как IP-адрес и маска подсети), если IP-адреса компьютера и P–660HT/HTW EE находятся в разных подсетях.

Firewall (Межсетевой экран)

В интернет-центре P–660HT/HTW EE реализован полнофункциональный межсетевой экран с защитой от атак DoS (Denial of Service/Отказ в обслуживании). По умолчанию, когда межсетевой экран включен, весь входящий трафик от глобальной вычислительной сети (WAN) к локальной (LAN) блокируется, если только он не инициируется локальной сетью (LAN). Межсетевой экран интернет-центра контролирует TCP/UDP, распознает и предотвращает DoS, выдает сигналы тревоги и ведет регистрацию событий и сообщений.

Фильтрация на основе содержания (контентная фильтрация)

Фильтрация на основе содержания позволяет блокировать доступ на запрещенные web-сайты, планировать график фильтрации для интернет-центра P–660HT/HTW EE и предоставлять доверенным компьютерам локальной сети (LAN) нефильтруемый доступ в Интернет по IP-адресам.

Перенаправление трафика (Traffic Redirect)

Функция перенаправления трафика автоматически направляет трафик WAN к резервному шлюзу LAN, если P–660HT/HTW EE не может установить соединение с Интернетом, выполняя, таким образом, функции дополнительного резервирования в случае невозможности подключения к WAN обычным образом.

Управление пропускной способностью среды передачи

Система управления пропускной способностью среды передачи от ZyXEL позволяет определять классы пропускной способности для отдельных приложений и/или подсетей. Вы можете назначить конкретную информационную емкость (бюджет пропускной способности) различным классам.

Универсальная функция "Plug and Play" (UPnP)

При помощи стандартного протокола TCP/IP интернет-центр P–660HT/HTW EE и другие устройства с поддержкой функции UPnP могут динамически подключаться к сети, получать IP-адрес и предоставлять свои ресурсы другим устройствам в сети.

PPPoE (RFC2516)

PPPoE (Протокол "точка-точка" поверх Ethernet) эмулирует коммутируемое соединение. Он позволяет Интернет-провайдеру использовать существующую конфигурацию сети совместно с новейшими широкополосными технологиями, такими как ADSL. Драйвер PPPoE в устройстве P–660HT/HTW EE является “прозрачным” для компьютеров в локальной сети, которые работают только по Ethernet и не поддерживают протокол PPPoE, что устраняет необходимость настраивать PPPoE клиенты на отдельных компьютерах. В интернет-центре предусмотрено также отключение PPPoE при простое

(соединение по PPPoE разрывается, если по прошествии указанного времени не зафиксировано информационного трафика) и подключение по PPPoE по требованию (соединение по PPPoE устанавливается только при поступлении запроса на доступ в Интернет).

Трансляция сетевых адресов (NAT)

NAT (Network Address Translation — Трансляция сетевых адресов) позволяет выполнять преобразование IP-адреса, используемого внутри одной сети (например, частного IP-адреса, используемого в локальной сети) в другой IP-адрес, известный в другой сети (например, общедоступный IP-адрес, используемый в Интернет).

Поддержка динамической DNS (DYNDNS)

Поддержка динамической системы доменных имен (DYNDNS) позволяет обеспечивать узел с динамическим IP-адресом постоянным именем, что упрощает доступ к этому узлу из любого места в Интернете. Для использования этой услуги необходимо зарегистрироваться у провайдера услуг динамической DNS (DYNDNS).

DHCP

DHCP (Dynamic Host Configuration Protocol/Протокол динамической настройки узлов) позволяет отдельным клиентским компьютерам получать настройки TCP/IP при загрузке от центрального сервера DHCP. Интернет-центр P–660HT/HTW EE имеет встроенную функцию сервера DHCP, которая включена по умолчанию. Модем может назначать IP-адреса, шлюз IP по умолчанию и серверы DNS клиентам DHCP. P–660HT/HTW EE также может функционировать как фиктивный сервер DHCP (ретранслятор DHCP), т.е. передавать клиентам назначенные IP-адреса от настоящего сервера DHCP.

Псевдоним IP (IP Alias)

Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей с использованием одного порта Ethernet. Интернет-центр поддерживает три логических порта локальной сети на одном физическом порте Ethernet, при этом сам интернет-центр является шлюзом для каждой логической сети.

Политика маршрутизации 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.

Фильтры пакетов

Функции фильтрации пакетов, имеющиеся в P–660HT/HTW EE, обеспечивают дополнительные возможности защиты и управления сетью.

Корпус

Компактный, не требующий принудительной вентиляции корпус P–660HT/HTW EE занимает мало пространства и легко помещается в любом месте.

4-портовый коммутатор (P–-660HT/HTW EE)

Интернет-центр P–660HT/HTW EE является выгодным и конкурентоспособным сетевым решением, благодаря комбинации функций коммутатора и маршрутизатора. Вы можете подключить к P–660HT/HTW EE до четырех компьютеров, при этом не приобретая коммутатор. Если к локальной сети нужно подключить более четырех компьютеров, используйте дополнительный коммутатор.

1.2.1 Беспроводной доступ (P–660HTW EE)

Беспроводная локальная сеть (WLAN)

Интернет-центр P–660HTW EE поддерживает стандарт IEEE 802.11g и полностью совместим со стандартом IEEE 802.11b. Это означает, что в одной беспроводной сети у Вас могут быть беспроводные клиенты двух стандартов: и IEEE 802.11b, и IEEE 802.11g.

ПРИМЕЧАНИЕ: Интернет-центр P–660HTW EE может быть подвержен радиочастотным (RF) помехам от других устройств с частотой 2,4 ГГц, таких как микроволновые печи, беспроводные телефоны, устройства, работающие с модулем Bluetooth и другие беспроводные локальные сети.

Защищенный доступ Wi-Fi (WPA)

Защищенный доступ Wi-Fi (WPA) представляет собой подкласс стандарта безопасности IEEE 802.11i. Основные отличия WPA от WEP заключаются в аутентификации пользователя и более совершенном шифровании данных.

Антенна

Интернет-центр P–660HT/HTW EE оборудован фиксированной антенной на 5 дБ, обеспечивающей четкую передачу радиосигнала между беспроводными устройствами и точками доступа.

Фильтрация MAC-адресов беспроводной ЛВС

Интернет-центр P–660HT/HTW EE может проверять MAC-адреса беспроводных устройств по списку допущенных или запрещенных MAC-адресов.

WEP-шифрование

WEP (Конфиденциальность эквивалентная проводным сетям) шифрует пакеты данных до их передачи через беспроводную сеть для обеспечения соблюдения конфиденциальности связи в сети.

1.3 Сферы применения интернет-центра P–660HT/HTW EE

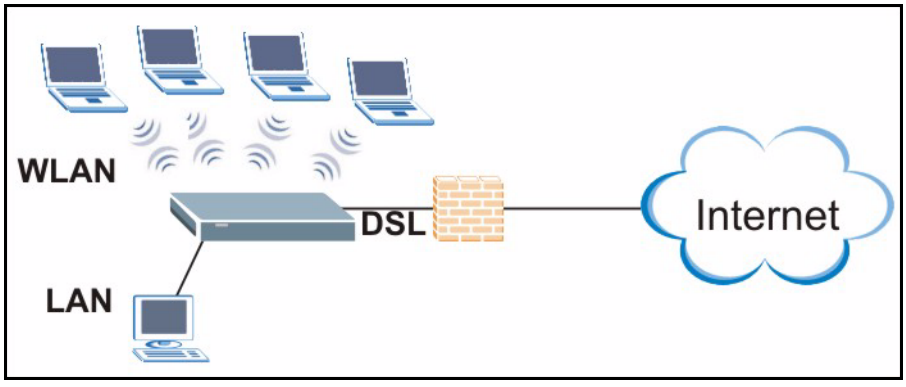
Далее приведено несколько примеров наиболее подходящего применения интернет-центра P–660HT/HTW EE.

1.3.1 Защищенный доступ в Интернет

Интернет-центр P–660HT/HTW EE является идеальным решением для высокоскоростного доступа в Интернет. Он совместим со всеми основными провайдерами ADSL DSLAM (Digital Subscriber Line Access Multiplexer — Мультиплексор цифровых абонентских линий) и поддерживает стандарты ADSL (см. Табл. 1 на с. 42). Кроме того, интернет-центр обеспечивает беспроводным клиентам доступ к ресурсам сети.

Интернет-центр обеспечивает защиту от атак Интернет-хакеров. По умолчанию межсетевой экран блокирует весь входящий трафик из глобальной сети (WAN). Межсетевой экран модема контролирует TCP/UDP, распознает и предотвращает DoS, выдает сигналы тревоги и ведет регистрацию событий и сообщений.

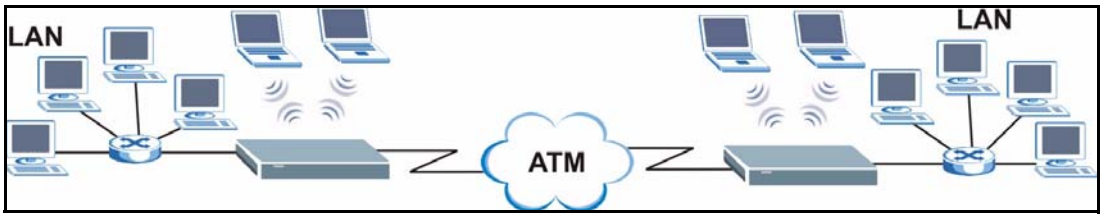
Рис. 1 Использование защищенного доступа в Интернет



1.3.2 Соединение локальных сетей

Интернет-центр можно использовать для соединения двух географически удаленных сетей по ADSL линиям. Типичный пример соединения двух локальных сетей приводится ниже.

Рис. 2 Соединение двух локальных сетей



1.4 Светодиоды передней панели

На следующих рисунках показаны светодиоды передней панели.

Рис. 3 Светодиоды передней панели P–660HT EE

Светодиоды передней панели P–660HTW EE

Описание светодиодов представлено в следующей таблице.

Табл. 2 Светодиоды передней панели

СВЕТОДИОД	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
PWR/SYS (Пит./ Сист.)	Зеленый	Горит	Электропитание интернет-центра включено, устройство работает нормально.
		Мигает	Интернет-центр перезагружается или проводит самодиагностику.
	Красный	Горит	На интернет-центр подается недостаточное питание.
		Не горит	Система не готова или неисправна.
LAN (ЛВС)	Зеленый	Горит	Успешно установлено соединение Ethernet на скорости 10/100 Мбит/с.
		Мигает	Интернет-центр передает/принимает данные.
		Не горит	Локальная сеть не подключена.

Табл. 2 Светодиоды передней панели (продолжение)

СВЕТОДИОД	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
WLAN (беспр. сеть — только для P–660HTW EE)	Зеленый	Горит	Интернет-центр готов, но не передает и не принимает данные по беспроводной сети.
		Мигает	Интернет-центр принимает или передает данные по беспроводной сети.
		Не горит	Беспроводная сеть не готова или неисправна.
DSL	Зеленый	Горит	Соединение DSL установлено.
		Мигает	P–660HT/HTW EE инициализирует линию DSL.
		Не горит	Канал DSL не работает.
INTERNET (Интернет)	Зеленый	Горит	Установлено соединение с Интернетом.
		Мигает	P–660HT/HTW EE передает/принимает данные.
		Не горит	Соединение с Интернетом не установлено.

1.5 Подключение аппаратных средств

Подключение аппаратных средств описано в Кратком руководстве.

Глава 2 Знакомство с Web-конфигуратором

В этой главе описывается как получить доступ к Web-конфигуратору и работать с его интерфейсом.

2.1 Описание Web-конфигуратора

Web-конфигуратор — это интерфейс управления на основе технологии HTML, который позволяет выполнять настройку и управление интернет-центром 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:

- Исходящие от модема 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".

2.1.1 Доступ к Web-конфигуратору

ПРИМЕЧАНИЕ: Несмотря на то, что существует возможность беспроводного подключения к интернет-центру, для начальной конфигурации рекомендуется подключить компьютер к порту LAN.

1. Убедитесь, что оборудование подключено правильно (см. Краткое руководство).
2. Подготовьте компьютер/компьютерную сеть для подключения к интернет-центру (см. Краткое руководство).
3. Запустите Web-браузер.
4. Укажите "192.168.1.1" в строке адреса.
5. Появится показанное ниже окно. В поле **Password (Пароль)** уже содержится пароль по умолчанию: “1234”. Нажмите кнопку **Login (Регистрация)**, чтобы

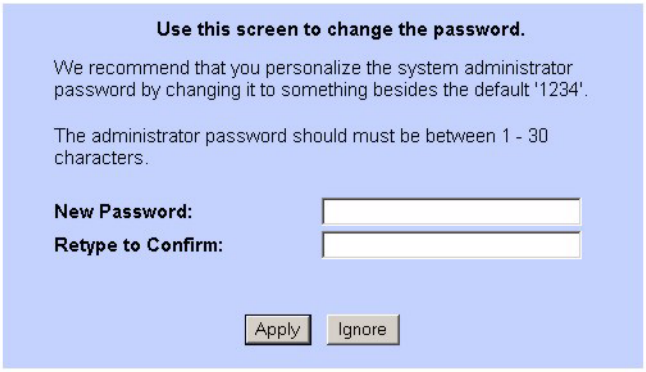
перейти в окно изменения пароля или **Cancel (Отмена)**, чтобы сохранить пароль по умолчанию.

Рис. 4 Окно ввода пароля

6 Настоятельно рекомендуется изменить пароль по умолчанию! Введите новый пароль (от 1 до 30 символов), еще раз введите его для подтверждения и нажмите кнопку **Apply (Применить)**; если в настоящее время вы не хотите изменять пароль, можно также нажать кнопку **Ignore (Пропустить)**, чтобы перейти в Главное меню.

ПРИМЕЧАНИЕ: Если вы не изменили пароль, то каждый раз при входе будет появляться следующее окно.

Рис. 5 Изменение пароля при входе



7 Далее появится окно **SITE MAP (КАРТА САЙТА)**.

ПРИМЕЧАНИЕ: Интернет-центр автоматически завершает сеанс после пяти минут бездействия. Если это произойдет, просто повторно подключитесь к интернет-центру через сеть и зарегистрируйтесь в системе.

2.1.2 Сброс настроек интернет-центра

В случае если вы забыли пароль или не можете получить доступ к Web-конфигуратору, необходимо воспользоваться кнопкой **RESET (СБРОС)**, расположенной на задней панели интернет-центра, для загрузки файла конфигурации, установленного изготовителем по умолчанию. Это означает, что прежняя конфигурация будет полностью потеряна и пароль будет установлен на значение по умолчанию “1234”.

2.1.2.1 Использование кнопки сброса настроек

1 Убедитесь, что светодиод **PWR/SYS** горит (не мигает).

2 Нажмите и удерживайте кнопку **RESET (СБРОС)** в течение десяти секунд или до тех пор, пока светодиод **PWR/SYS** не начнет мигать, затем отпустите ее. Когда светодиод **PWR/SYS** начинает мигать, произойдет восстановление настроек по умолчанию, и интернет-центр перезагрузится.

2.1.3 Интерфейс Web-конфигуратора

Далее описывается, как работать с интерфейсом Web-конфигуратора из окна **SITE MAP (КАРТА САЙТА)**. Вид окна зависит от конкретной модели интернет-центра.

- Нажмите **Wizard Setup (Мастер установки)** для запуска мастера, который поможет Вам произвести первоначальную настройку интернет-центра.
- Для выставления параметров дополнительных функциональных возможностей интернет-центра щелкните по ссылке **Advanced Setup (Дополнительная настройка)**.
- Щелкните по ссылке **Maintenance (Сопровождение)** для просмотра статистики о работе интернет-центра, информации о версии микропрограммы, сохранения файла конфигурации или восстановления сохраненной ранее копии конфигурации.
- Щелкните по ссылке **Site Map (Карта сайта)** для перехода к окну **Site Map (Карта сайта)**.
- Нажмите **Logout (Выход)** на навигационной панели после завершения сеанса управления устройством.

Рис. 6 Web-конфигуратор: окно Site Map (Карта сайта)

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

Табл. 3 Сводная таблица окон Web-конфигуратора

ССЫЛКА	ПОДРАЗДЕЛ	ФУНКЦИЯ
Wizard Setup (Мастер установки)	Connection Setup (Настройка соединения)	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.
	Media Bandwidth Mgnt (Управление пропускной способностью среды передачи)	Эти окна используются для ограничения пропускной способности приложением.
Advanced Setup (Дополнительная настройка)		
Password (Пароль)		Это окно используется для изменения пароля.
LAN (ЛВС)		Это окно используется для настройки параметров DHCP и TCP/IP локальной сети.
Wireless LAN (Беспроводная локальная сеть) (только P–660HTW EE)	Wireless (Беспроводная сеть)	Это окно используется для настройки беспроводной ЛВС.
	MAC Filter (Фильтр MAC-адресов)	Это окно используется для изменения настроек фильтра MAC-адресов в интернет-центре.
	802.1x/WPA	Это окно используется для настройки аутентификации и безопасности WLAN.
	Local User Database (Встроенная база данных пользователей)	Это окно используется для создания пользовательских профилей для аутентификации беспроводных устройств.
	RADIUS	Это окно используется для определения внешнего сервера RADIUS для аутентификации беспроводных устройств.

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

ССЫЛКА	ПОДРАЗДЕЛ	ФУНКЦИЯ
WAN (Глобальная сеть)	WAN Setup (Настройка глобальной сети)	Это окно используется для изменения в интернет-центре параметров доступа в глобальную сеть.
	WAN Backup (Резервирование глобальной сети)	Это окно используется для настройки параметров перенаправления трафика и резервирования глобальной сети.
NAT (Трансляция сетевых адресов)	SUA Only (Только SUA)	Это окно используется для настройки серверов, расположенных за интернет-центром.
	Full Feature (Полный набор функциональных возможностей)	Это окно используется для настройки правил отображения сетевых адресов.
Dynamic DNS (Динамическая DNS)		Это окно используется для установки динамического сервера DNS.
Time and Date (Время и дата)		Это окно используется для установки времени и даты в интернет-центре.
Firewall (Межсетевой экран)	Default Policy (Политика по умолчанию)	Это окно используется для активации/деактивации межсетевого экрана и направления сетевого трафика, для которого применяется правила.
	Rule Summary (Список правил)	Это окно показывает список правил межсетевого экрана и позволяет редактировать/добавлять правила.
	Anti Probing (Блокирование эхо-тестирования)	Это окно используется для изменения настроек блокирования эхо-тестирования.
	Threshold (Пороговое значение)	Это окно используется для настройки допустимого порога для атаки типа DoS.
Content Filter (Контент-фильтр)	Keyword (Ключевое слово)	Это окно используется для блокировки сайтов, содержащих определенные ключевые слова в URL.
	Schedule (График)	Это окно используется для установки дней и времени, когда интернет-центр будет производить контентную фильтрацию.
	Trusted (Доверенный)	Это окно используется для исключения диапазона пользователей в ЛВС из контент-фильтрования интернет-центром.
Remote Management (Удаленное управление)		Это окно используется для настройки портов и IP-адреса(ов), с которых пользователям разрешается выполнять управление интернет-центром по протоколам Telnet/FTP/Web.
UPnP		Это окно используется для включения в интернет-центре функции UPnP.
Logs (Журналы регистрации)	Log Settings (Настройки журналов регистрации)	Это окно используется для изменения настроек журналов регистрации интернет-центра.

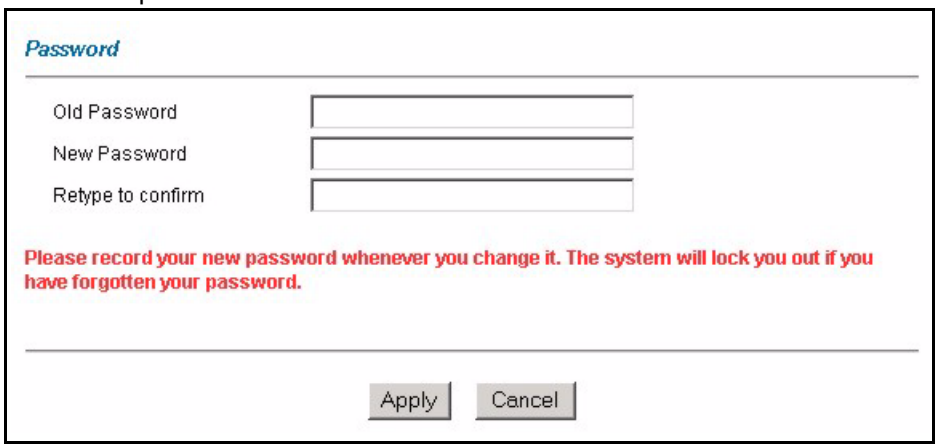
Табл. 3 Сводная таблица окон Web-конфигуратора (продолжение)

ССЫЛКА	ПОДРАЗДЕЛ	ФУНКЦИЯ
	View Log (Просмотр журнала регистрации)	Это окно используется для просмотра журналов регистрации для категорий, которые Вы выбрали.
Media Bandwidth Management (Управление пропускной способностью среды передачи)	Summary (Общие настройки)	Это окно используется для ограничения пропускной способности для определенных видов трафика.
	Class Setup (Настройка классов пропускной способности)	Это окно используется для определения класса пропускной способности.
	Monitor (Монитор)	Это окно используется для просмотра статистики по классам пропускной способности.
Maintenance (Сопровождение)		
System Status (Состояние системы)		В этом окне содержится сводная информация о системе.
DHCP Table (Таблица DHCP)		В этом окне отображается информация DHCP (Протокол динамической настройки узлов) в режиме ТОЛЬКО ДЛЯ ЧТЕНИЯ.
Таблица Any IP (Любой IP)		Это окно используется для просмотра IP- и MAC-адресов компьютеров локальной сети, подключенных к интернет-центру.
Wireless LAN (Беспроводная ЛВС) (только P–660HTW EE)	Association List (Список соединений)	Это окно отображает MAC-адрес(а) беспроводных устройств, соединенных с интернет-центром в данный момент.
Diagnostic (Диагностика)	General (Общие)	Информация в этих окнах помогает выявлять неполадки основного подключения интернет-центра.
	DSL Line (DSL линия)	Информация в этих окнах помогает выявлять неполадки DSL линии.
Firmware (Микро-программа)		Это окно используется для загрузки микропрограммы в интернет-центр.
Logout (Конец сеанса)		Для выхода из Web-конфигуратора нажмите **Logout (Конец сеанса)**.

2.2 Изменение пароля для входа в систему

Настоятельно рекомендуется периодически менять пароль доступа к интернет-центру. Если Вы не изменяли пароль по умолчанию после регистрации в системе или хотите снова сменить пароль, нажмите кнопку **Password (Пароль)** в окне **Site Map (Карта сайта)** — при этом откроется показанное ниже окно.

Рис. 7 Пароль



В следующей таблице даны описания полей этого окна.

Табл. 4 Пароль

ПОЛЕ	ОПИСАНИЕ
Old Password (Старый пароль)	Введите в данное поле пароль по умолчанию или текущий пароль, который используется для доступа к системе.
New Password (Новый пароль)	Введите в данное поле новый пароль.
Retype to Confirm (Повторный ввод для подтверждения)	Введите в данное поле новый пароль еще раз.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

Глава 3
Мастер установки доступа в Интернет

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

3.1 Введение

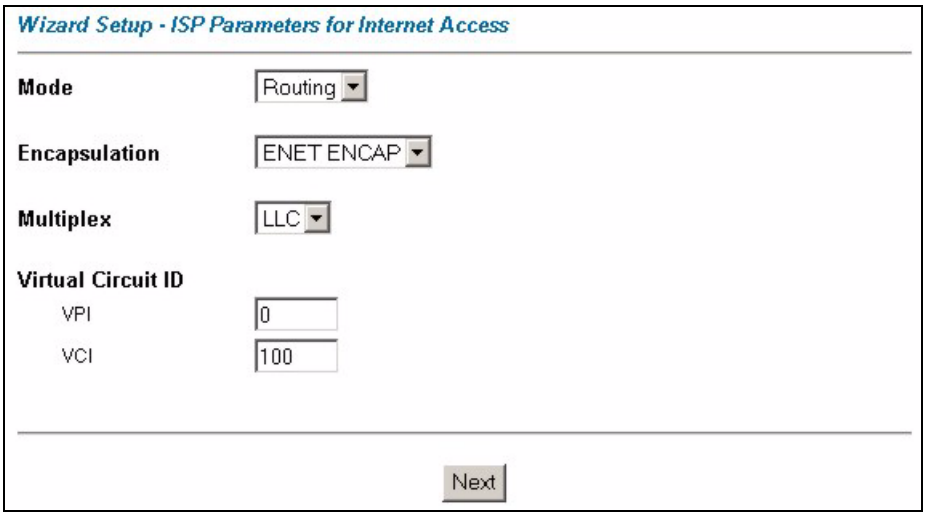
Окна **Мастера установки** используются для настройки системы для выхода в Интернет на основе параметров, предоставленных Интернет-провайдером.

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

3.1.1 Мастер установки доступа в Интернет

1 В окне **SITE MAP (КАРТА САЙТА)** нажмите **Wizard Setup (Мастер установки)**, чтобы открыть первое окно мастера.

Рис. 8 Мастер установки доступа в Интернет: ISP Parameters (Параметры Интернет-провайдера)



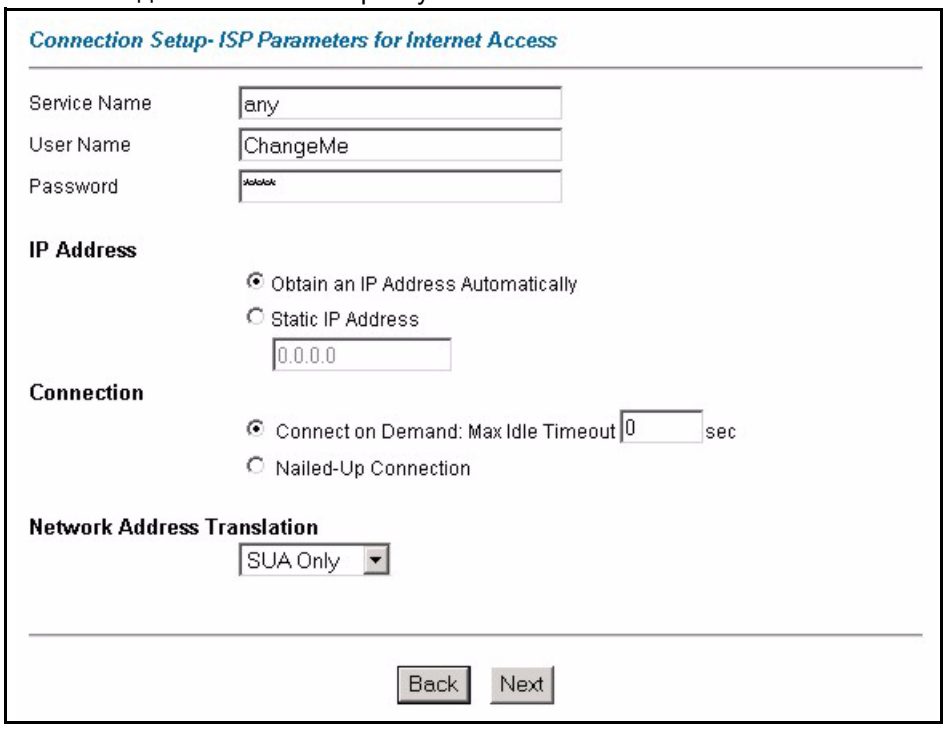
В следующей таблице даны описания полей этого окна.

Табл. 5 Мастер установки доступа в Интернет: ISP Parameters (Параметры Интернет-провайдера)

ПОЛЕ	ОПИСАНИЕ
Mode (Режим)	Из раскрывающегося списка поля **Mode (Режим)** выберите **Routing (Маршрутизация)** (установлено по умолчанию), если ваш Интернет-провайдер позволяет использовать одну учетную запись для подключения к Интернету нескольких компьютеров. В противном случае выберите **Bridge (Мост)**.
Encapsulation (Инкапсуляция)	Из раскрывающегося списка поля **Encapsulation (Инкапсуляция)** выберите тип инкапсуляции, используемый вашим Интернет-провайдером. Опции в списке зависят от значения, установленного в поле **Mode (Режим)**. Если в поле **Mode (Режим)** вы установили **Bridge (Мост)**, то выберите **PPPoA** или **RFC 1483**. Если в поле **Mode (Режим)** вы установили **Routing (Маршрутизация)**, то выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
Multiplex (Мультиплексирование)	Из раскрывающегося списка поля **Multiplex (Мультиплексирование)** выберите метод мультиплексирования, который использует ваш Интернет-провайдер: VC-based (на основе VC) или LLC-based (на основе LLC).
Virtual Circuit ID (Идентификатор виртуальной линии передачи)	VPI (Virtual Path Identifier — Идентификатор виртуального пути) и VCI (Virtual Channel Identifier — Идентификатор виртуального канала) определяют виртуальную линию передачи. Более подробную информацию см. в *Приложении*.
VPI	Введите назначенный вам номер VPI. Это поле может быть уже заполнено.
VCI	Введите назначенный вам номер VCI. Это поле может быть уже заполнено.
Next (Далее)	Нажмите на эту кнопку для перехода к следующему окну Мастера. Вид следующего окна зависит от выбранного выше протокола. Щелкните по ссылке протокола, чтобы перейти к следующему окну мастера для этого протокола.

2 Вид следующего окна **Мастера установки** зависит от выбранного режима и используемого типа инкапсуляции. Далее все примеры окон даны с учетом включенного режима маршрутизации. Заполните поля и нажмите кнопку **Next (Далее)** для продолжения.

Рис. 9 Подключение к Интернету с использованием PPPoE



В следующей таблице даны описания полей этого окна.

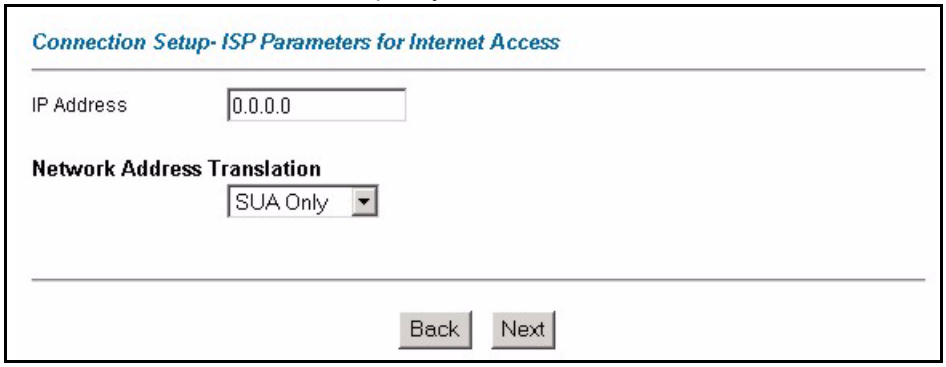
Табл. 6 Подключение к Интернету с использованием PPPoE

ПОЛЕ	ОПИСАНИЕ
Service Name (Имя услуги)	Введите имя провайдера услуг PPPoE.
User Name (Имя пользователя)	Введите имя пользователя, предоставленное Интернет-провайдером. Если имя назначается в формате user@domain, где domain означает имя услуги, то вводите оба элемента имени в полном соответствии с данными от провайдера.
Password (Пароль)	Введите пароль для данного имени пользователя.
IP Address (IP-адрес)	Статический IP-адрес — это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является постоянным. В этом случае Интернет-провайдер будет назначать новый адрес при каждом подключении к Интернету. Выберите **Obtain an IP Address Automatically (Получить IP-адрес автоматически)**, если у вас динамический IP-адрес; либо выберите **Static IP Address (Статический IP-адрес)** и введите предоставленный Интернет-провайдером IP-адрес в расположенное ниже текстовое поле.

Табл. 6 Подключение к Интернету с использованием PPPoE (продолжение)

ПОЛЕ	ОПИСАНИЕ
Connection (Подключение)	Выберите **Connect on Demand (Подключение по требованию)**, если постоянное соединение не требуется, и укажите в поле **Max. Idle Timeout (Максимальное время простоя)** время простоя (в секундах). По умолчанию для режима **Подключение по требованию** время простоя равно 0, что означает, что сеанс связи Интернет не будет разрываться. Выберите **Nailed-Up Connection (Постоянное соединение)**, если требуется постоянное соединение. При разрыве соединения интернет-центр будет автоматически пытаться его восстановить. Правило(а) расписания связи в меню SMT 26 имеет приоритет над настройками полей **Connection (Подключение)**.
Network Address Translation (Трансляция сетевых адресов)	Из раскрывающегося списка выберите **None (Нет)**, **SUA Only (Только SUA)** или **Full Feature (Полный набор функциональных возможностей)**. Подробную информацию см. в главе NAT.
Back (Назад)	Для возврата к первому окну Мастера нажмите кнопку **Back (Назад)**.
Next (Далее)	Для перехода к следующему окну Мастера нажмите кнопку **Next (Далее)**.

Рис. 10 Подключение к Интернету с использованием RFC 1483

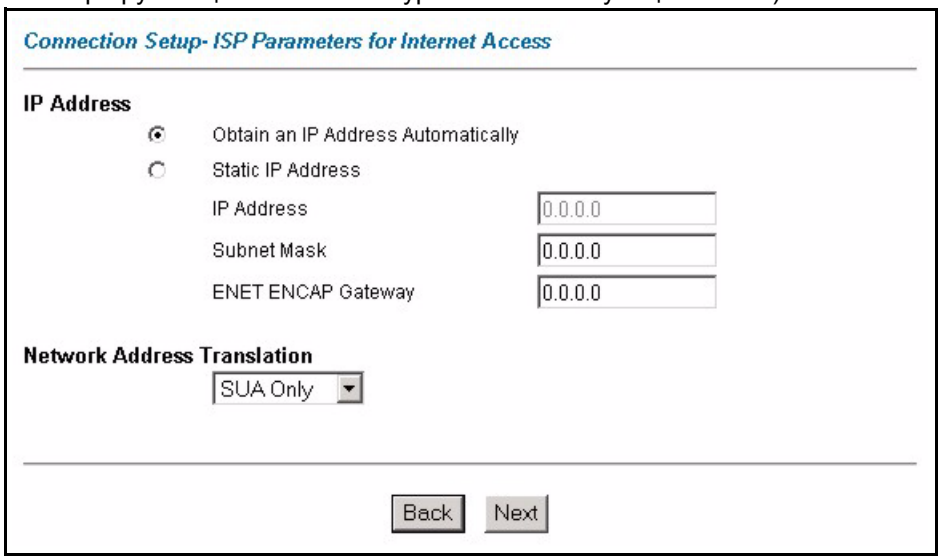


В следующей таблице даны описания полей этого окна.

Табл. 7 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.
Network Address Translation (Трансляция сетевых адресов)	Из раскрывающегося списка выберите **None (Нет)**, **SUA Only (Только SUA)** или **Full Feature (Полный набор функциональных возможностей)**. Подробную информацию см. в главе NAT.
Back (Назад)	Для возврата к первому окну Мастера нажмите кнопку **Back (Назад)**.
Next (Далее)	Для перехода к следующему окну Мастера нажмите кнопку **Next (Далее)**.

Рис. 11 Подключение к Интернету с использованием ENET ENCAP (Протокол маршрутизации канального уровня и инкапсуляцией MAC)

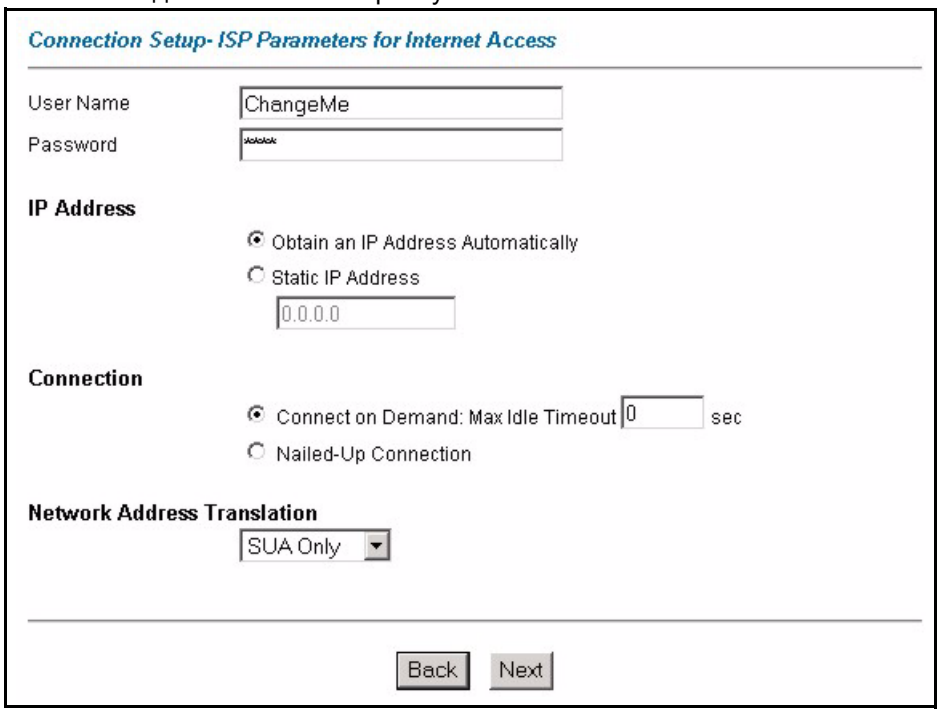


В следующей таблице даны описания полей этого окна.

Табл. 8 Подключение к Интернету с использованием ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Статический IP-адрес — это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является постоянным. В этом случае Интернет-провайдер будет назначать новый адрес при каждом подключении к Интернету. Выберите **Obtain an IP Address Automatically (Получить IP-адрес автоматически)**, если у вас динамический IP-адрес; или выберите **Static IP Address (Статический IP-адрес)** и введите предоставленный Интернет-провайдером IP-адрес в расположенное ниже текстовое поле "IP Address".
Subnet Mask (Маска подсети)	Введите маску подсети в десятичном формате с разделительными точками. Если требуется создание подсетей, см. *Приложения* для расчета маски подсети.
ENET ENCAP Gateway (Шлюз ENET ENCAP)	Необходимо указать IP-адрес шлюза (предоставленный вашим Интернет-провайдером), если в предыдущем окне в поле **Encapsulation (Инкапсуляция)** установлен тип инкапсуляции **ENET ENCAP**.
Network Address Translation (Трансляция сетевых адресов)	Из раскрывающегося списка выберите **None (Нет)**, **SUA Only (Только SUA)** или **Full Feature (Полный набор функциональных возможностей)**. Подробную информацию см. в главе NAT.
Back (Назад)	Для возврата к первому окну Мастера нажмите кнопку **Back (Назад)**.
Next (Далее)	Для перехода к следующему окну Мастера нажмите кнопку **Next (Далее)**.

Рис. 12 Подключение к Интернету с использованием PPPoA



В следующей таблице даны описания полей этого окна.

Табл. 9 Подключение к Интернету с использованием PPPoA

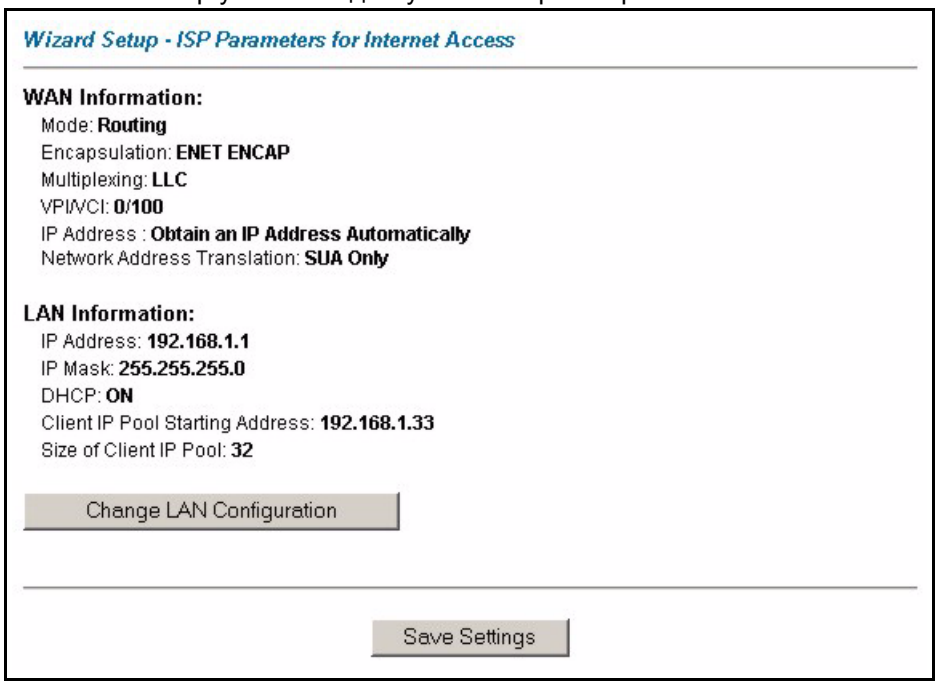
ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите регистрационное имя, предоставленное Интернет-провайдером.
Password (Пароль)	Введите пароль для данного имени пользователя.
IP Address (IP-адрес)	Это поле доступно, если в поле **Mode (Режим)** выбран режим **Routing (Маршрутизация)**. Статический IP-адрес — это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является постоянным. В этом случае Интернет-провайдер будет назначать новый адрес при каждом подключении к Интернету. Выберите **Obtain an IP Address Automatically (Получить IP-адрес автоматически)**, если у вас динамический IP-адрес; или выберите **Static IP Address (Статический IP-адрес)** и введите предоставленный Интернет-провайдером IP-адрес в расположенное ниже текстовое поле "IP Address".
Connection (Подключение)	Выберите **Connect on Demand (Подключение по требованию)**, если постоянное соединение не требуется, и укажите в поле **Max. Idle Timeout (Максимальное время простоя)** время простоя (в секундах). По умолчанию для режима **Подключение по требованию** время простоя равно 0, что означает, что сеанс связи Интернет не будет разрываться. Выберите **Nailed-Up Connection (Постоянное соединение)**, если требуется постоянное соединение. При разрыве соединения интернет-центр будет автоматически пытаться его восстановить. Правило(а) расписания связи в меню SMT 26 имеет приоритет над настройками полей **Connection (Подключение)**.

Табл. 9 Подключение к Интернету с использованием PPPoA (продолжение)

ПОЛЕ	ОПИСАНИЕ
Network Address Translation (Трансляция сетевых адресов)	Это поле доступно, если в поле **Mode (Режим)** выбран режим **Routing (Маршрутизация)**. Из раскрывающегося списка выберите **None (Нет)**, **SUA Only (Только SUA)** или **Full Feature (Полный набор функциональных возможностей)**. Подробную информацию см. в главе NAT.
Back (Назад)	Для возврата к первому окну Мастера нажмите кнопку **Back (Назад)**.
Next (Далее)	Для перехода к следующему окну Мастера нажмите кнопку **Next (Далее)**.

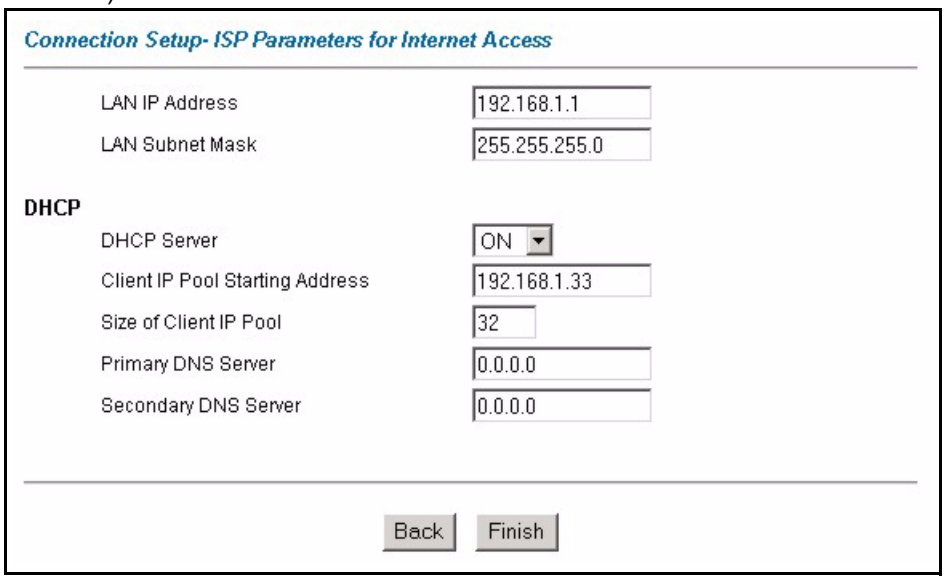
3 Проверьте сделанные установки в окне, показанном ниже. Для изменения параметров локальной сети в интернет-центре, нажмите **Change LAN Configurations (Изменить настройки локальной сети)**. Либо нажмите **Save Settings (Сохранить настойки)** для сохранения конфигурации и перехода к разделу 3.13.

Рис. 13 Мастер установки доступа в Интернет: третье окно



Если необходимо изменить настройки локальной сети в интернет-центре, нажмите **Change LAN Configuration (Изменить настройки локальной сети)** для отображения показанного ниже окна.

Рис. 14 Мастер установки доступа в Интернет: LAN Configuration (Настройки локальной сети)



В следующей таблице даны описания полей этого окна.

Табл. 10 Мастер установки доступа в Интернет: LAN Configuration (Настройки локальной сети)

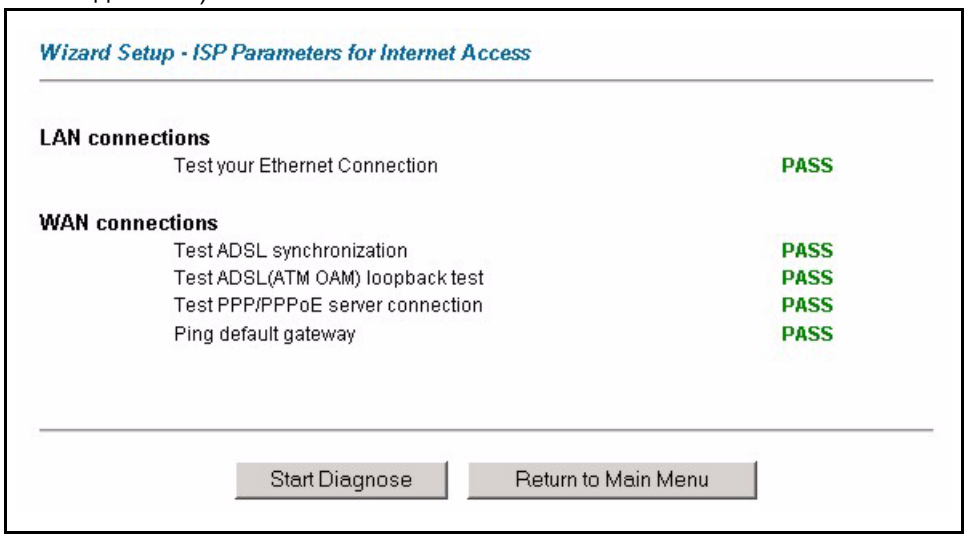
ПОЛЕ	ОПИСАНИЕ
LAN IP Address (IP-адрес в локальной сети)	Введите IP-адрес интернет-центра в десятичном формате с разделительными точками, например, 192.168.1.1 (установлен изготовителем по умолчанию). Если вы изменили IP-адрес интернет-центра в локальной сети, то для доступа к Web-конфигуратору необходимо использовать новый IP-адрес.
LAN Subnet Mask (Маска подсети локальной сети)	Введите маску подсети в десятичном формате с разделительными точками.
DHCP	
DHCP Server (Сервер DHCP)	Из раскрывающегося списка поля **DHCP Server (Сервер DHCP)** выберите **On (Включить)**, чтобы разрешить интернет-центру назначать IP-адреса, шлюз IP по умолчанию и серверы DNS компьютерам, поддерживающим функцию клиента DHCP. Выберите **Off (Выключить)** для отключения функции сервера DHCP. Если функция DHCP включена, необходимо ввести следующие параметры:
Client IP Pool Starting Address (Начальный IP-адрес клиентского диапазона)	В этом поле вводится первый адрес из непрерывного диапазона IP-адресов.
Size of Client IP Pool (Размер диапазона IP-адресов клиентов)	В этом поле устанавливается размер непрерывного диапазона IP-адресов.
Primary DNS Server (Основной сервер DNS)	Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.

Табл. 10 Мастер установки доступа в Интернет: LAN Configuration (Настройки локальной сети) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Secondary DNS Server (Дополнительный сервер DNS)	Аналогично предыдущей записи.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Finish (Готово)	Нажмите кнопку **Finish (Готово)** для сохранения настроек и перехода к следующему окну Мастера.

4 Интернет-центр автоматически тестирует соединение с компьютером(ами), подключенным(и) к порту LAN. Для тестирования соединения от интернет-центра до Интернет-провайдера, нажмите кнопку **Start Diagnose (Начать диагностику)**. В другом случае нажмите кнопку **Return to Main Menu (Возврат в Главное меню)** для возврата к окну **Site Map (Карта сайта)**.

Рис. 15 Мастер установки доступа в Интернет: Connection Tests (Тестирование соединения)



5 Запустите Web-браузер и перейдите на сайт www.zyxel.ru. Обеспечение доступа в Интернет — это всего лишь одна из возможностей устройства. Подробную информацию по всем функциональным возможностям интернет-центра см. далее в этом Руководстве пользователя. Если вы не можете получить доступ в Интернет, снова откройте Web-конфигуратор и проверьте правильность заданных настроек.

Глава 4
Настройка локальной сети

В этой главе описывается настройка параметров локальной сети.

4.1 Обзор локальной сети

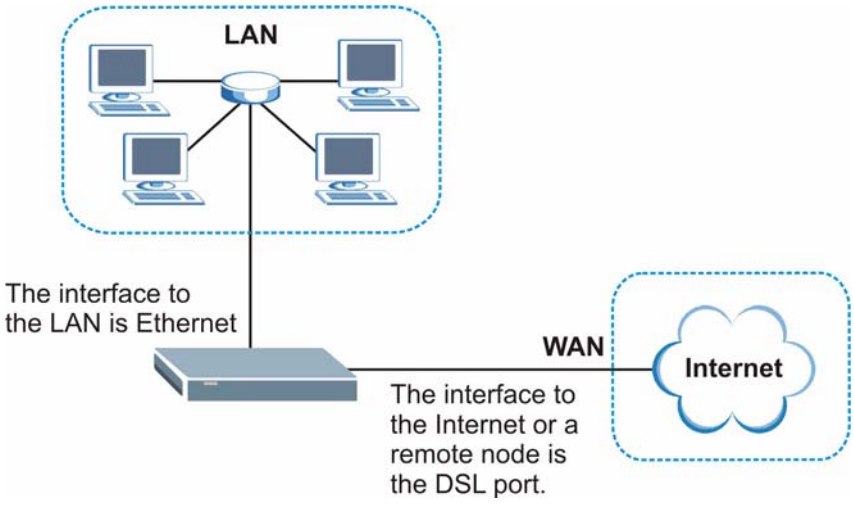
LAN (Local Area Network — Локальная сеть) — это коллективно используемая система связи, к которой подключено множество компьютеров. Локальная сеть представляет собой компьютерную сеть, ограниченную ближайшей территорией, обычно это здание или этаж в здании. Окна настройки LAN используются для настройки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

Информацию об окнах настройки **LAN** см. в Разд. 4.3 на с. 74.

4.1.1 Локальные, глобальные сети и интернет-центр

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

Рис. 16 Локальные и глобальные IP-адреса



4.1.2 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 интернет-центр как сервер DHCP или отключить эту функцию. При включенной функции сервера DHCP, интернет-центр предоставляет клиентам настройки TCP/IP. При отключении службы DHCP требуется наличие другого сервера DHCP в локальной сети, или настройка компьютера вручную.

4.1.2.1 Настройка диапазона IP

Интернет-центр настроен на работу с диапазоном IP-адресов для DHCP-клиентов (диапазоном DHCP). См. характеристики изделия в приложениях. Не присваивайте статических IP-адресов из диапазона DHCP компьютерам в Вашей локальной сети.

4.1.3 Адрес сервера DNS

DNS (Domain Name System — Система доменных имен) предназначена для отображения доменного имени на соответствующий ему IP-адрес и наоборот. Сервер DNS играет очень важную роль, так как без него нужно было бы точно знать IP-адрес узла, к которому необходимо получить доступ. Адреса серверов DNS, которые устанавливаются при настройке DHCP, передаются клиентским узлам вместе с назначенным IP-адресом и маской подсети.

Существует два способа распространения адресов серверов DNS Интернет-провайдером. Первый из них заключается в том, что Интернет-провайдер сообщает клиенту адреса серверов DNS, обычно в виде информационного листка, который клиент подписывает. Если Интернет-провайдер предоставил Вам адреса серверов DNS, следует ввести их в поля **DNS Server (Сервер DNS)** в Меню **DHCP Setup (Настройка DHCP)**, в противном случае оставьте эти поля пустыми.

Некоторые Интернет-провайдеры предпочитают передавать адреса серверов DNS после установления соединения с помощью серверных расширений DNS протокола PPP IPCP (IP Control Protocol — Протокол управления IP). Если Интернет-провайдер не предоставляет адресов серверов DNS в явной форме, значит, они передаются в процессе согласования по IPCP. Интернет-центр поддерживает серверные расширения DNS IPCP через функцию proxy-сервера DNS.

Если поля **Primary (Основной)** и **Secondary DNS Server (Дополнительный сервер DNS)** в окне **LAN Setup (Настройка локальной сети)** не заполнены, например, установлено значение 0.0.0.0, интернет-центр сообщает клиентам DHCP, что он сам является сервером DNS. Когда компьютер посылает интернет-центру DNS запрос, то интернет-центр пересылает этот запрос на действительный сервер DNS, который был обнаружен с помощью протокола IPCP и ретранслирует ответ назад компьютеру.

Следует отметить, что proxy-сервер DNS может работать, только если Интернет-провайдер использует серверные расширения DNS IPCP. Это не означает, что можно не включать серверы DNS при настройке 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)**. Таким образом, интернет-центр может пересылать информацию от серверов DNS к компьютерам; а компьютеры могут обращаться непосредственно к серверу DNS без вмешательства интернет-центра.

4.1.4 Назначение адреса сервера DNS

DNS (Система доменных имен) предназначена для отображения доменного имени на соответствующий ему 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.

Существует два способа распространения адресов серверов DNS Интернет-провайдером.

- Интернет-провайдер сообщает адреса серверов DNS, обычно в виде информационного листка, который вы подписываете. Если Интернет-провайдер предоставляет адреса серверов DNS, введите их в поля для серверов DNS в окне **LAN Setup (Настройка локальной сети)**.
- Интернет-центр функционирует как proxy-сервер DNS, если поля **Primary (Основной)** и **Secondary DNS Server (Дополнительный сервер DNS) в окне LAN Setup (Настройка локальной сети)** оставлены пустыми.

4.2 Настройка TCP/IP локальной сети

Интернет-центр имеет встроенную функцию сервера DHCP, что позволяет назначать IP-адреса и серверы DNS компьютерам, которые поддерживают клиента DHCP.

4.2.1 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.

Как назначается номер сети, зависит от конкретной ситуации. Если Интернет-провайдер или сетевой администратор назначают блок зарегистрированных IP-адресов, то необходимо руководствоваться их указаниями при выборе IP-адреса и маски подсети.

Если Интернет-провайдер не предоставляет явным образом адрес сети, то, скорее всего, вы используете учетную запись одиночного пользователя, и Интернет-провайдер будет назначать динамический IP-адрес при каждом установлении соединения. В этом случае необходимо выбрать IP-адрес из диапазона 192.168.0.0 – 192.168.255.0 и включить функцию NAT (Network Address Translation — Трансляция сетевых адресов) в интернет-

центре. Этот диапазон IP-адресов специально зарезервирован Агентством по назначению имен и уникальных параметров протоколов Интернет (IANA) для частного использования. Если не предписано иное, не следует использовать номера за пределами этого диапазона. Если выбрать адрес 192.168.1.0 в качестве номера сети, то получится 254 индивидуальных адреса от 192.168.1.1 до 192.168.1.254 (числа ноль и 255 зарезервированы). Иными словами, первые три числа в адресе задают номер сети, а остальные определяют конкретный компьютер в этой сети.

После принятия решения относительно номера сети выберите для интернет-центра IP-адрес, который легко запомнить, например 192.168.1.1 и убедитесь, что другое устройство в сети не использует этот IP-адрес.

Маска подсети определяет сетевую часть IP-адреса. Интернет-центр вычисляет маску подсети автоматически на основе введенного IP-адреса. Если не указано иное, не следует изменять маску подсети, вычисленную интернет-центром.

4.2.1.1 IP-адреса для частных сетей

Каждый компьютер в сети Интернет должен иметь 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, Агентство 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 Интернет для локальной сети. С другой стороны, если организация является частью большой компании, следует проконсультироваться с сетевым администратором по поводу назначения IP-адресов.

ПРИМЕЧАНИЕ: Независимо от конкретной ситуации, не рекомендуется назначать произвольные IP-адреса; необходимо 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.*

4.2.2 Настройка RIP

RIP (Routing Information Protocol — Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. С помощью настройки поля **RIP Direction (Направление RIP)** производится управление передачей и приемом пакетов RIP. Когда в этом поле установлено значение:

- **Both (Оба)** — интернет-центр осуществляет периодическую широковещательную рассылку своей маршрутной таблицы и принятых данных RIP.
- **In Only (Только входящие)** — интернет-центр не посылает пакеты RIP, но принимает поступающие пакеты RIP.
- **Out Only (Только исходящие)** — интернет-центр посылает пакеты RIP, но не принимает поступающие пакеты RIP.
- **None** — интернет-центр не посылает пакеты RIP и игнорирует поступающие пакеты RIP.

Настройка поля **Version (Версия)** управляет форматом и методом широковещательной рассылки пакетов RIP, которые посылает интернет-центр (оба формата распознаются при приеме). Формат **RIP-1** является общепринятым, однако формат RIP-2 содержит больше информации. Формат RIP-1 подходит для большинства сетей, если только сеть не имеет специальной топологии.

Как **RIP-2B**, так и **RIP-2M** осуществляют передачу данных маршрутизации в формате RIP-2. Их отличие заключается в том, что **RIP-2B** использует широковещательную рассылку в подсети, а **RIP-2M** — многоадресную рассылку.

4.2.3 Многоадресная рассылка

Как правило, пакеты IP передаются одним из двух способов: одноадресная рассылка (1 отправитель — 1 получатель) или широковещательная рассылка (1 отправитель — все абоненты 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. Для получения более подробной информации о взаимодействии между IGMP версии 2 и версии 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, выполняющими многоадресную рассылку. Адрес 224.0.0.1 используется для запросов и назначается постоянной группе, в которую входят все узлы (включая шлюзы). Чтобы участвовать в многоадресной рассылке IGMP, в группу 224.0.0.1 должны входить все узлы. Адрес 224.0.0.2 назначается группе маршрутизаторов, участвующих в многоадресной рассылке.

Интернет-центр поддерживает как версию 1 IGMP (**IGMP-v1**), так и версию 2 IGMP (**IGMP-v2**). При запуске интернет-центр опрашивает все непосредственно подключенные сети, с целью сбора информации о членстве в группах. В дальнейшем интернет-центр периодически обновляет эту информацию. Функцию многоадресной рассылки можно включить/отключить для портов интернет-центра LAN и/или WAN с помощью Web-конфигуратора (окна **Локальная сеть**,**Глобальная сеть**). Для отключения многоадресной рассылки для этих портов установите **None (Нет)**.

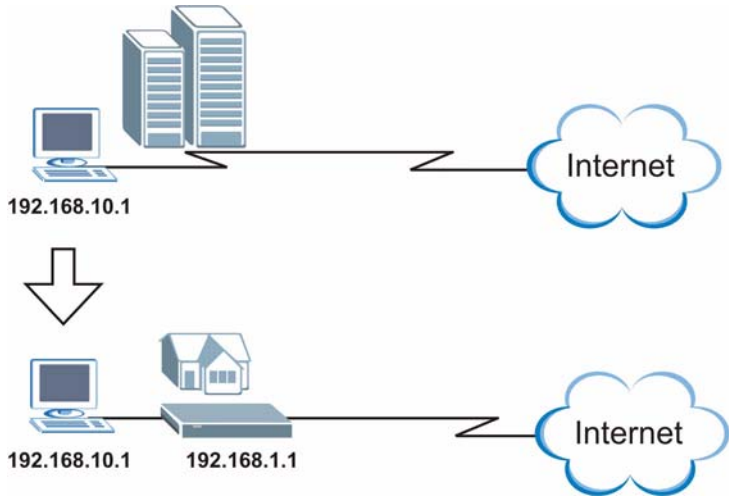
4.2.4 Any IP (Любой IP)

Обычно для того, чтобы компьютер мог получить доступ в Интернет (через интернет-центр), необходимо, чтобы IP-адреса и маски подсети компьютера и интернет-центра находились в одной подсети. В случае, если компьютер должен использовать статический IP-адрес, находящийся в другой сети, то, возможно, потребуется вручную изменять настройки сети компьютера каждый раз, когда вы захотите подключиться к Интернету через интернет-центр.

С помощью функции Any IP и включенной функции NAT интернет-центр позволяет компьютеру получить доступ в Интернет без изменения сетевых параметров (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и интернет-центра находятся в разных подсетях. Независимо от того, динамический или статический IP-адрес назначен компьютеру, вы можете просто подключить компьютер к интернет-центру и получить доступ в Интернет.

На следующем рисунке представлен сценарий, где компьютеру назначен статический частный IP-адрес в корпоративной сети. В жилом доме, где установлен интернет-центр, все равно можно использовать этот компьютер для доступа в Интернет без изменения сетевых настроек, даже если IP-адреса компьютера и интернет-центра находятся в разных подсетях.

Рис. 17 Пример Any IP



Функция Any IP не применяется для компьютера с динамическим или статическим IP-адресом, который находится в той же подсети, что и IP-адрес интернет-центра.

ПРИМЕЧАНИЕ: Чтобы использовать функцию Any IP, *необходимо* включить функцию NAT/SUA.

4.2.4.1 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 составляется в устройстве IP Ethernet (интернет-центре) для принятия решения, какой следующий транзитный пункт необходимо использовать для пересылки данных конкретному адресату.

Далее перечислены действия, которые выполняются, когда компьютер первый раз пытается получить доступ в Интернет через интернет-центр.

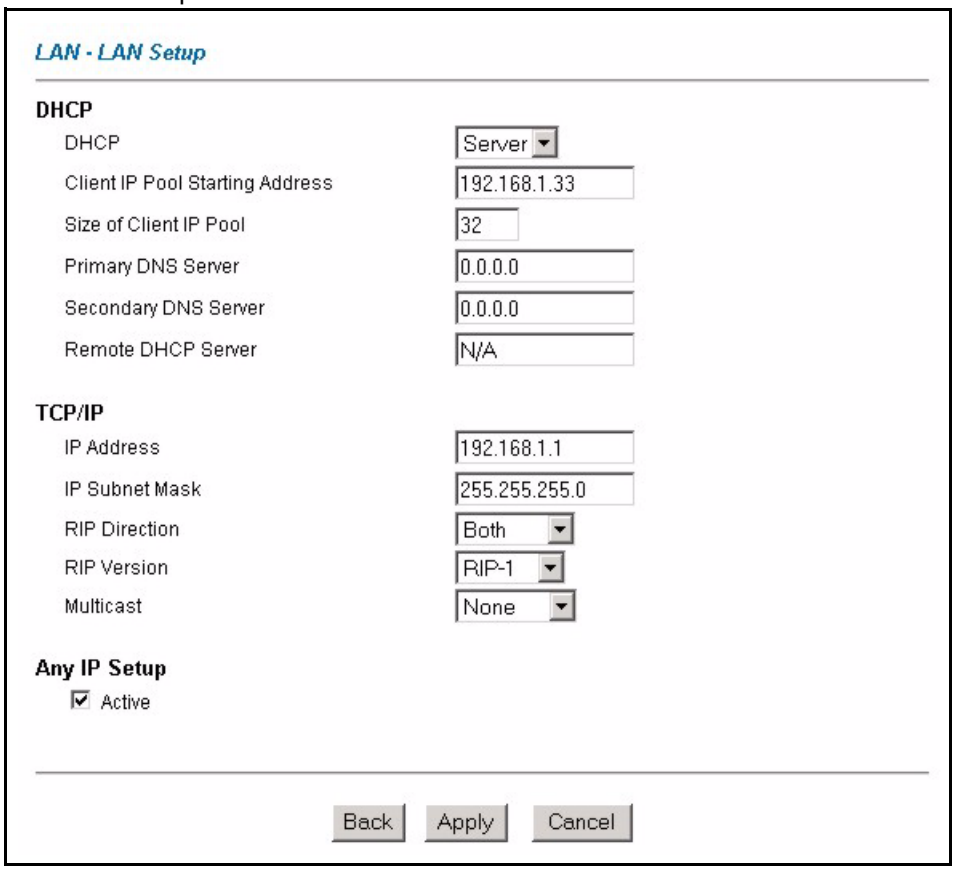
1. Когда компьютер (находящийся в другой подсети) пытается первый раз получить доступ в Интернет, он посылает пакет на шлюз по умолчанию (не интернет-центр) с помощью поиска его MAC-адреса в своей таблице ARP.
2. Если компьютер не может обнаружить шлюз по умолчанию, посылается широковещательный запрос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

После обновления информации о маршрутизации, компьютер имеет доступ к интернет-центру и доступ в Интернет, как будто он находится в той же подсети, что и интернет-центр.

4.3 Настройка локальной сети

Нажмите **LAN (Локальная сеть)** — откроется окно **LAN Setup (Настройка локальной сети)**. Более подробную информацию см. в Разд. 4.1 на с. 68.

Рис. 18 Настройка локальной сети



В следующей таблице даны описания полей этого окна.

Табл. 11 LAN Setup (Настройка локальной сети)

ПОЛЕ	ОПИСАНИЕ
DHCP	
DHCP	Если выбрано значение **Server (Сервер)**, интернет-центр может назначать IP-адреса, шлюз IP 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)**, интернет-центр работает в качестве фиктивного сервера DHCP и ретранслирует запросы и ответы DHCP между удаленным сервером и клиентами. В этом случае следует ввести IP-адрес фактического удаленного сервера DHCP в поле **Remote DHCP Server (Удаленный сервер DHCP)**. Если функция DHCP включена, необходимо установить следующие параметры:
Client IP Pool Starting Address (Начальный IP-адрес клиентского диапазона)	В этом поле вводится первый адрес из непрерывного диапазона IP-адресов.

Табл. 11 LAN Setup (Настройка локальной сети) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Size of Client IP Pool (Размер диапазона IP-адресов клиентов)	В этом поле устанавливается размер непрерывного диапазона IP-адресов.
Primary DNS Server (Основной сервер DNS)	Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Secondary DNS Server (Дополнительный сервер DNS)	Аналогично предыдущей записи.
Remote DHCP Server (Удаленный сервер DHCP)	Если в поле **DHCP** выбрано значение **Relay (Ретранслятор)**, следует ввести IP-адрес фактического удаленного сервера DHCP.
TCP/IP	
IP Address (IP-адрес)	Введите IP-адрес интернет-центра в десятичном формате 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 задана).
RIP Direction (Направление RIP)	Выберите направление RIP из раскрывающего списка со значениями **None (Нет)**, **Both (Оба)**, **In Only (Только входящие)** и **Out Only (Только исходящие)**.
RIP Version (Версия RIP)	Выберите версию RIP, где возможны варианты: **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. Интернет-центр поддерживает обе версии IGMP: версию 1 (**IGMP-v1**) и версию 2 (**IGMP-v2**). Для отключения выберите **None (Нет)**.
Any IP Setup (Настройка Any IP)	Поставьте флажок в окошке **Active (Активировать)** для включения функции Any IP (Любой IP). Функция Any IP позволяет компьютеру получить доступ в Интернет без изменения сетевых настроек (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и интернет-центра находятся в разных подсетях. При отключении функции Any IP только компьютеры с динамическими или статическими IP-адресами, находящимися в той же подсети, что и IP-адрес интернет-центра, смогут подключиться к интернет-центру или получить доступ в Интернет через интернет-центр.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

Глава 5 Беспроводная локальная сеть (WLAN)

В этой главе описывается окна настройки беспроводной локальной сети для модели P-660HTW EE.

5.1 Беспроводная локальная сеть — введение

Беспроводная локальная сеть может быть простой (два компьютера с сетевыми адаптерами, соединенные в одноранговую сеть) или сложной (множество компьютеров с сетевыми адаптерами, соединенные через точки доступа, которые передают сетевой трафик в проводную локальную сеть).

Настройки беспроводной локальной сети — см. Разд. 5.3 на с. 79.

ПРИМЕЧАНИЕ: Дополнительную информацию о беспроводных сетях см. в приложении "Беспроводные локальные сети (WLAN)".

5.2 Защита беспроводной сети — общая информация

Безопасность беспроводных соединений имеет важное значение для безопасности всей сети. Необходимо обеспечивать защиту связи между беспроводными устройствами, точками доступа и проводной сетью.

Методы защиты беспроводной сети, предлагаемые интернет-центром P–660HTW EE, включают шифрование данных, проверку подлинности (аутентификация) беспроводных клиентов, ограничение доступа по MAC-адресам устройств и скрытие беспроводной сети от обнаружения.

5.2.1 Шифрование

- При наличии сервера RADIUS и беспроводных клиентов, поддерживающих WPA, используйте метод WPA. Метод WPA обеспечивает аутентификацию пользователей и улучшенное шифрование данных (по сравнению с WEP).
- При наличии беспроводных клиентов, поддерживающих WPA, но при отсутствии сервера RADIUS используйте WPA-PSK.

- Если беспроводные клиенты не поддерживают WPA, необходимо использовать WEP-шифрование. Ключ с большим числом битов (разрядов) улучшает защиту, но при этом ухудшает пропускную способность. С помощью идентификационной фразы можно автоматически сгенерировать 64-разрядные или 128-разрядные ключи WEP либо ввести ключи WEP вручную.

5.2.2 Аутентификация

WPA выполняет проверку подлинности пользователей, кроме того можно настроить устройство, поддерживающее IEEE 802.1x, для использования встроенной базы данных пользователей или сервера RADIUS для аутентификации беспроводных клиентов перед их подключением к сети.

- При наличии сервера RADIUS используйте аутентификацию RADIUS. Информация о протоколах, используемых при аутентификации клиентского устройства сервером RADIUS через интернет-центр приведена в приложениях.
- Если в сети меньше 32 беспроводных устройств, используйте встроенную базу данных пользователей. При аутентификации клиентского устройства встроенной базой данных пользователей интернет-центр использует шифрование MD5.

5.2.3 Ограниченный доступ

В окне **MAC Filter** можно настроить точку доступа (AP) на предоставление доступа только определенным устройствам (**Allow Association**) либо исключить их из списка устройств, подключаемых к точке доступа (**Deny Association**).

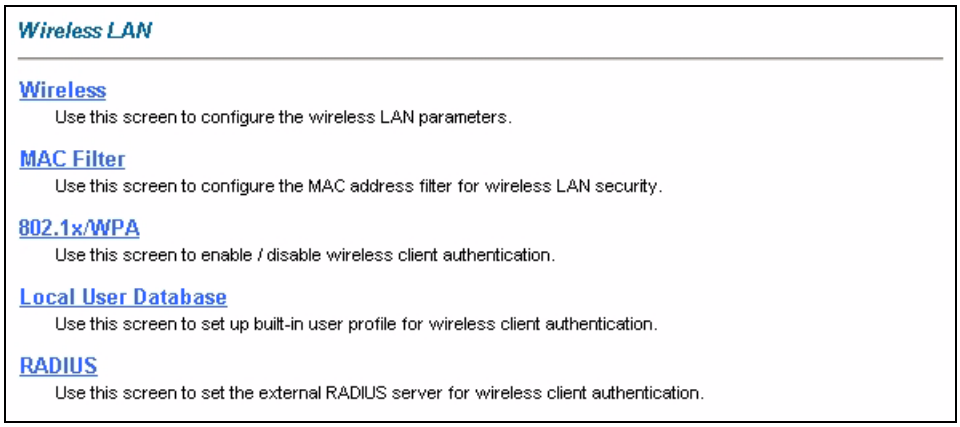
5.2.4 Предотвращение обнаружения беспроводной сети

Если скрыть идентификатор ESSID, то беспроводные клиенты не смогут обнаружить беспроводную сеть путем сканирования точек доступа. Недостатком повышения безопасности методом "скрытия" интернет-центра являются неудобства для некоторых клиентов, действительно имеющих право доступа к беспроводной сети. Если не скрывать ESSID, рекомендуется изменить его значение по умолчанию на другое.

5.3 Главное окно настроек беспроводной локальной сети

Чтобы открыть главное окно **Wireless LAN (Беспроводная локальная сеть)**, нажмите кнопку **Wireless LAN** на панели навигации.

Рис. 19 Wireless LAN (Беспроводная локальная сеть)



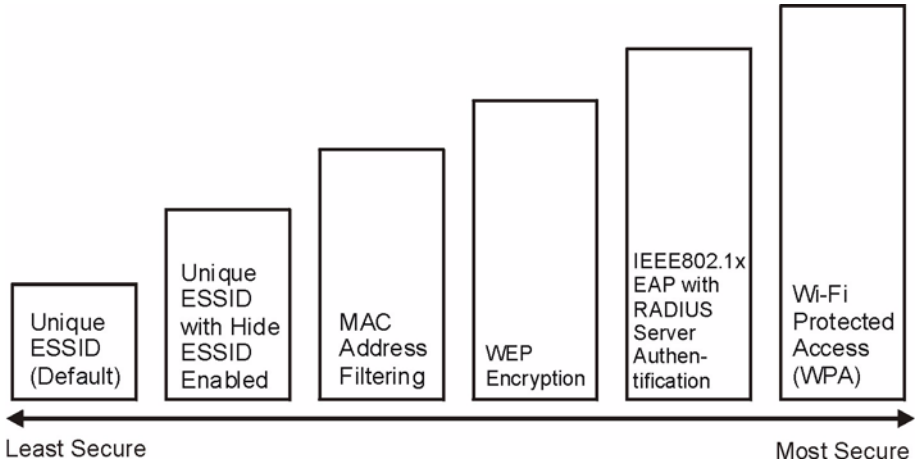
В следующей таблице даны описания ссылок в этом окне.

Табл. 12 Wireless LAN (Беспроводная локальная сеть)

ССЫЛКА	ОПИСАНИЕ
Wireless (Беспроводная сеть)	Щелкните по этой ссылке для перехода к окну настройки **ESSID** и **WEP**. **ПРИМЕЧАНИЕ:** При настройке **WEP** нельзя настроить ни **WPA**, ни **WPA-PSK**.
MAC Filter (Фильтр MAC-адресов)	Щелкните по этой ссылке для перехода к окну, где можно ограничить доступ к беспроводной сети по MAC-адресу беспроводного адаптера.
802.1x/WPA	Щелкните по этой ссылке для перехода к окну настройки WPA или WPA-PSK. В этом окне также можно настроить проверку подлинности беспроводных клиентов 802.1x.
RADIUS	Щелкните по этой ссылке для перехода к окну настройки аутентификационной базы данных внешнего сервера RADIUS.
Local User Database (Встроенная база данных пользователей)	Щелкните по этой ссылке для перехода к окну настройки встроенной базы данных аутентификации пользователей.

На приведенном ниже рисунке показана сравнительная эффективность методов защиты беспроводных сетей, имеющихся в модели P–660HTW EE.

Рис. 20 Методы защиты беспроводной сети



ПРИМЕЧАНИЕ: Необходимо активировать в интернет-центре те же настройки безопасности беспроводного соединения, что и на всех беспроводных устройствах, которые будут подключены к интернет-центру.

Если функция беспроводной безопасности интернет-центра выключена, сеть будет доступна для любого беспроводного сетевого устройства, находящегося в зоне охвата сети.

5.4 Настройки в окне Wireless (Беспроводная сеть)

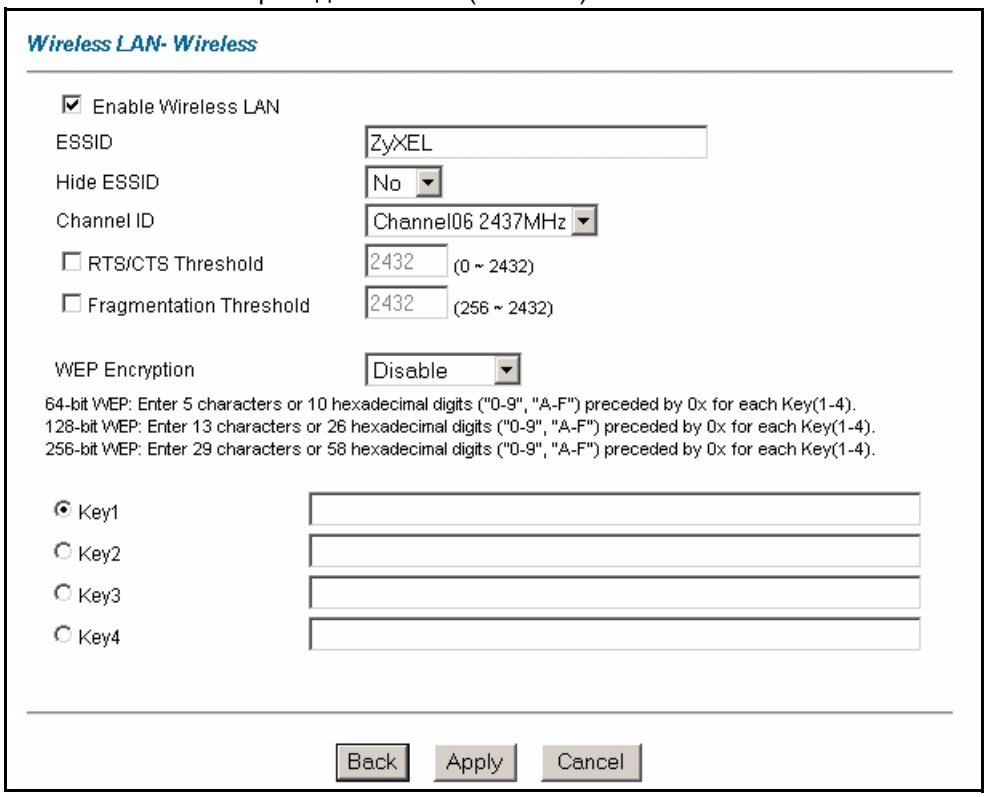
5.4.1 WEP-шифрование

WEP-шифрование кодирует передачу данных между беспроводными устройствами и точками доступа для предотвращения несанкционированного доступа. Шифруются передачи одноадресных и многоадресных рассылок в сети. Как беспроводные устройства, так и точки доступа должны использовать одинаковые ключи WEP.

Для модели P–660HTW EE можно настроить до четырех 64-, 128- или 256-разрядных ключей WEP, но одновременно может быть активирован только один ключ.

Чтобы настроить и включить шифрование WEP нажмите **Wireless LAN** и **Wireless**, чтобы перейти в окно **Wireless**.

Рис. 21 Окно "Беспроводная связь" (Wireless)



В следующей таблице даны описания полей этого окна.

Табл. 13 Wireless LAN (Беспроводная сеть)

ПОЛЕ	ОПИСАНИЕ
Enable Wireless LAN (Включить беспроводную локальную сеть)	При включении беспроводной локальной сети необходимо выбрать один из уровней ее защиты (см. Рис. 20 на с. 81). Выберите эту опцию, чтобы включить беспроводную локальную сеть.
ESSID	Идентификатор набора дополнительных услуг (ESSID) представляет собой уникальное имя, предназначенное для идентификации интернет-центра в беспроводной локальной сети. Беспроводные устройства, подключенные к интернет-центру должны иметь одинаковый ESSID. Введите описательное имя длиной не более 32 печатных символов ASCII (включая пробелы и с учетом регистра для букв алфавита).
Hide ESSID (Скрыть ESSID)	Выберите **Yes** для скрытия ESSID, чтобы другие устройства не могли получать ESSID путем сканирования точки доступа. Выберите **No**, чтобы сделать ESSID видимой для того, чтобы устройства могли получать ESSID путем сканирования точки доступа.
Channel ID (Идентификатор канала)	Радиочастота, используемая беспроводными устройствами стандартов IEEE 802.11b/g называется каналом. Выберите канал из раскрывающегося списка.

Табл. 13 Wireless LAN (Беспроводная сеть) (продолжение)

ПОЛЕ	ОПИСАНИЕ
RTS/CTS Threshold (RTS/CTS Порог)	Порог RTS (Request To Send/Запрос на передачу) (количество байт) предназначен для включения RTS/CTS. Данные, размер кадра которых превышает это значение, проходят квитирование RTS/CTS. Если это значение превышает максимальный размер MSDU (Сервисного блока данных MAC), RTS/CTS выключится. Если это значение установлено на ноль, RTS/CTS включится. Отметьте опцию для изменения значения по умолчанию и введите новое значение от 0 до 2432.
Fragmentation Threshold (Порог фрагментации)	Порог (количество байт) фрагментации предназначен для прямых сообщений. Это максимальный размер фрагмента данных, который можно послать. Отметьте опцию для изменения значения по умолчанию и введите новое значение от 256 до 2432.
Перечисленные ниже поля не будут доступны для WEP, если включен **WPA** или **WPA-PSK**.	
Passphrase (Контрольная фраза)	Введите контрольную фразу (до 63 печатных символов с учетом регистра) и нажмите **Generate**. Интернет-центр создаст четыре различных ключа WEP. На момент составления данного Руководства невозможно использование контрольной фразы для генерирования 256-разрядных ключей WEP.
Generate (Генерировать)	После ввода контрольной фразы нажмите кнопку **Generate**, чтобы интернет-центр автоматически создал четыре различных ключа WEP. Ключи будут отображены в показанных ниже полях.
WEP Encryption (WEP-шифрование)	При использовании WEP (Wired Equivalent Privacy — Конфиденциальность эквивалентная проводным сетям) пакеты данных сначала шифруются, а затем передаются по беспроводной сети. Выберите **Disable** для того, чтобы все беспроводные устройства поддерживали связь с точками доступа без шифрования данных. Выберите **64-bit WEP**, **128-bit WEP** или **256-bit WEP** для использования шифрования данных соответствующей разрядности.
Key 1 - Key 4 (Ключ 1 — Ключ 4)	Ключи WEP используются для шифрования данных. Как интернет-центр, так и беспроводные устройства должны использовать одинаковые ключи WEP для передачи данных. Если Вы хотите вручную установить ключи WEP, введите ключ WEP в предназначенном для этого поле. При выборе **64-bit WEP** нужно ввести 5 символов ASCII или 10 шестнадцатеричных символов ("0-9", "A-F"). При выборе **128-bit WEP** нужно ввести 13 символов ASCII или 26 шестнадцатеричных символов ("0-9", "A-F"). При выборе **256-bit WEP** нужно ввести 29 символов ASCII или 58 шестнадцатеричных символов ("0-9", "A-F"). Значения ключей WEP необходимо установить в точности одинаковыми для всех беспроводных устройств, работающих в одной беспроводной локальной сети. Настроить следует все четыре ключа, но одновременно может использоваться только один ключ. По умолчанию активирован ключ 1.
Back (Назад)	Нажмите **Back**, чтобы вернуться к экрану основного меню настроек беспроводной локальной сети.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

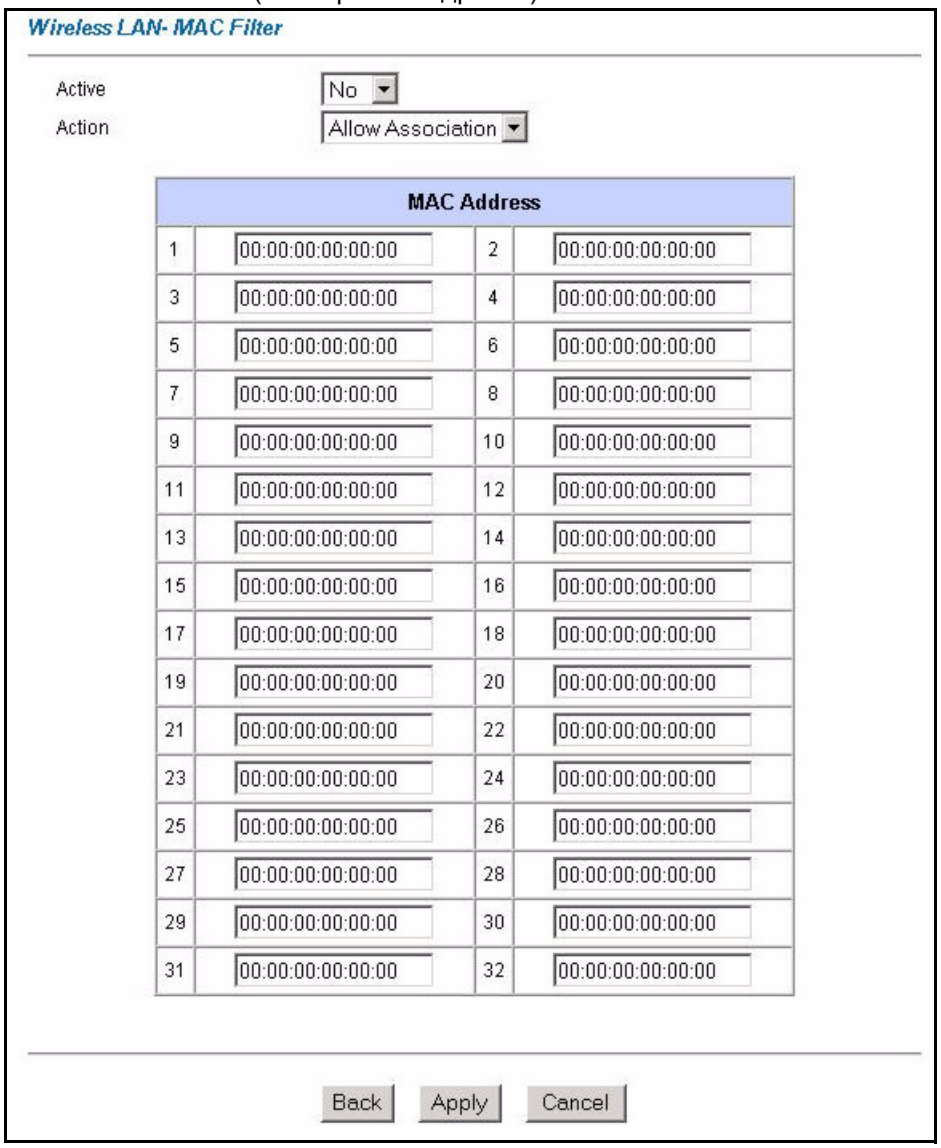
ПРИМЕЧАНИЕ: Если при настройке интернет-центра с компьютера в беспроводной локальной сети изменить параметры ESSID или настройки безопасности (Рис. 20 на с. 81), беспроводное соединение будет разорвано при нажатии клавиши **Apply (Применить)**. В этом случае необходимо изменить беспроводные настройки компьютера для соответствия новым настройкам интернет-центра.

5.5 Настройка фильтра MAC-адресов

Каждое устройство Ethernet имеет уникальный MAC-адрес (MAC — Media Access Control — Управление доступом к среде передачи). MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатиричных символов, например, 00:A0:C5:00:00:02. Для настройки этого окна необходимо знать MAC-адреса устройств. Для изменения настроек фильтра MAC-адресов интернет-центра нажмите **Wireless LAN**, **MAC Filter (Фильтр MAC-адресов)** для отображения экрана **MAC Filter**. При этом откроется показанное ниже окно.

ПРИМЕЧАНИЕ: При управлении интернет-центром через беспроводное соединение нельзя указывать MAC-адрес компьютера в списке и устанавливать для него **Deny Association (Запретить подключение)** в поле **Action (Действие)**. Иначе компьютер будет заблокирован.

Рис. 22 MAC Filter (Фильтр MAC-адресов)



В следующей таблице описываются поля данного меню.

Табл. 14 Фильтр MAC-адресов

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Выберите из раскрывающегося списка **Yes**, чтобы включить фильтрацию MAC-адресов.
Action (Действие)	Определите способ фильтрации для списка MAC-адресов в таблице **MAC Address**. Выберите **Deny Association (Запретить подключение)**, чтобы блокировать доступ к маршрутизатору. MAC-адресам, не указанным в списке, будет разрешен доступ к интернет-центру. Выберите опцию **Allow Association (Разрешить подключение)**, если нужно разрешить доступ к маршрутизатору; при этом для MAC-адресов, не попавших в список доступ к маршрутизатору будет запрещен.

Табл. 14 Фильтр MAC-адресов (продолжение)

ПОЛЕ	ОПИСАНИЕ
MAC Address (MAC-адрес)	Введите MAC-адреса беспроводных устройств, которым разрешен либо запрещен доступ к интернет-центру, в корректном формате, т.е. в виде шести пар шестнадцатиричных символов, например, 12:34:56:78:9a:bc.
Back (Назад)	Нажмите **Back**, чтобы вернуться к экрану основного меню настроек беспроводной локальной сети.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

5.6 Введение в WPA

Wi-Fi Protected Access (WPA — Защищенный доступ Wi-Fi) представляет собой элемент из набора средств безопасности стандарта IEEE 802.11i. WPA является более предпочтительным по сравнению с WEP, поскольку WPA обеспечивает аутентификацию пользователя и более надежное шифрование данных. Более подробная информация о проверке подлинности пользователей и шифровании с помощью WPA приведена в приложении.

Если внешний сервер RADIUS отсутствует, то следует использовать WPA-PSK (WPA - Pre-Shared Key, WPA с предварительно согласованным ключом). WPA-PSK требует только ввода одного (идентичного) пароля для каждого устройства беспроводной сети. Если пароль совпадает, клиенту будет предоставлен доступ к беспроводной сети.

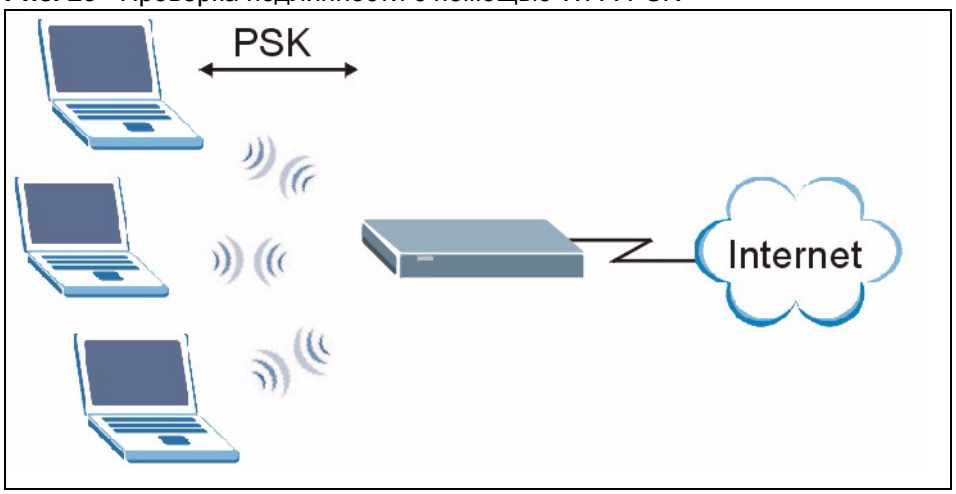
ПРИМЕЧАНИЕ: При выборе WPA нельзя использовать для проверки подлинности пользователей встроенную базу данных.

5.6.1 Пример применения WPA-PSK

Применение WPA-PSK выглядит следующим образом.

1. Вначале введите идентичные пароли для точки доступа и всех беспроводных устройств. Длина предварительно согласованного ключа (PSK) должна составлять от 8 до 63 печатных знаков (включая пробелы и с учетом регистра для букв алфавита).
2. Точка доступа проверяет пароль каждого клиента и разрешает ему подключиться к сети в случае совпадения паролей.
3. Точка доступа устанавливает и распределяет ключи для беспроводных клиентов.
4. Точка доступа и беспроводные клиенты используют процесс шифрования TKIP для шифрования данных, передаваемых между ними.

Рис. 23 Проверка подлинности с помощью WPA-PSK

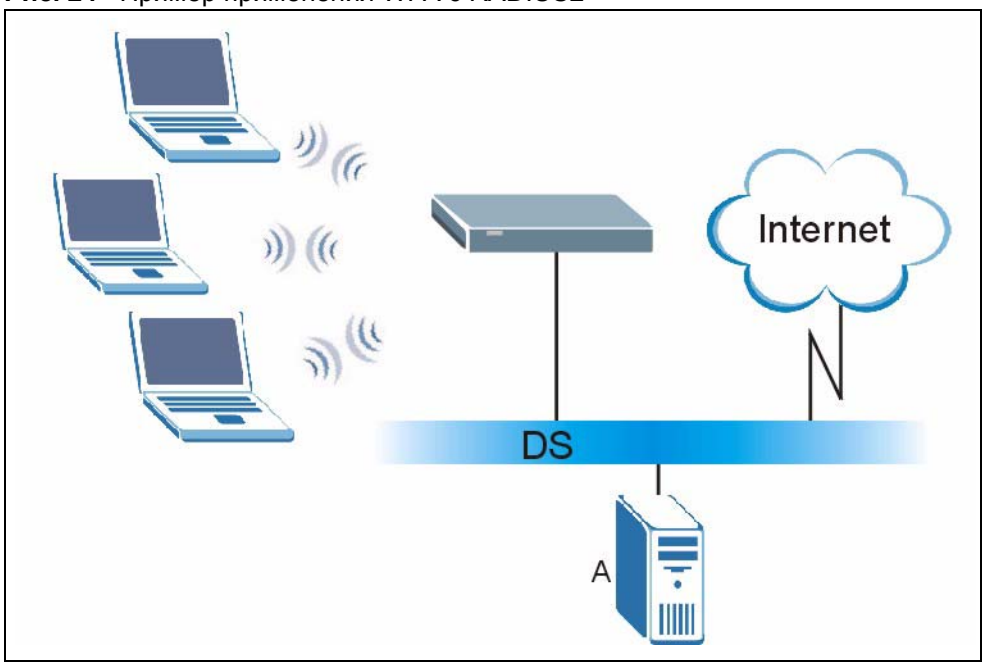


5.6.2 Пример применения WPA с сервером RADIUS

Потребуются IP-адрес, номер порта (по умолчанию 1812) и общий секретный ключ сервера RADIUS. Далее приводится пример подключения по WPA с внешним сервером RADIUS. "A" — это сервер RADIUS. "DS" — это система распределения (проводное подключение к ЛВС).

1. Точка доступа пересылает запрос на аутентификацию беспроводного клиента на сервер RADIUS.
2. Сервер RADIUS проводит идентификацию пользователя по своей базе данных и соответственно предоставляет или запрещает доступ в сеть.
3. Сервер RADIUS выдает парный главный ключ (PMK) точке доступа, которая затем создает систему управления и иерархии ключей с использованием парного ключа для динамического генерирования уникальных ключей шифрования данных для шифрования каждого пакета данных, передаваемого беспроводным методом между точкой доступа и беспроводными клиентами.

Рис. 24 Пример применения WPA с RADIUS2



5.6.3 Вспомогательное программное обеспечение для беспроводных клиентов WPA

Вспомогательное ПО беспроводного клиента — это программа, работающая в операционной системе и дающая беспроводному клиенту инструкции по использованию WPA. На момент составления данного Руководства самое распространенное вспомогательное ПО — это обновление WPA для Windows XP, клиент Funk Software's Odyssey и клиент AEGIS Meetinghouse Data Communications.

Обновление для Windows XP представляет собой бесплатную подпрограмму, которая добавляет функцию WPA к встроенному беспроводному клиенту Windows XP с функцией "Zero Configuration" (Автоматическая настройка). Однако, для ее использования необходимо работать в Windows XP.

Инструкции по настройке см. в Разд. 5.7.3 на с. 94 и Разд. 5.7.4 на с. 96.

5.7 Настройка IEEE 802.1x и WPA

Для изменения параметров аутентификации интернет-центра щелкните по ссылке **Wireless LAN** под **Advanced Setup** и откройте вкладку **802.1x/WPA**. Вид экрана может отличаться в зависимости от того, какой протокол управления ключами выбран.

- Инструкции по разрешению беспроводного доступа без аутентификации или блокировка беспроводного доступа к интернет-центру см. в Разд. 5.7.1 на с. 89.
- Инструкции по настройке аутентификации IEEE 802.1x см. в Разд. 5.7.2 на с. 91.
- Инструкции по настройке WPA см. в Разд. 5.7.3 на с. 94.

- Инструкции по настройке WPA-PSK см. в Разд. 5.7.4 на с. 96.

5.7.1 Запрещение доступа или доступ без аутентификации

Выберите **No Access Allowed (Доступ запрещен)** или **No Authentication Required (Аутентификация не требуется)** в поле **Wireless Port Control (Управление беспроводной точкой доступа)**.

Рис. 25 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: No Access Allowed (Доступ запрещен)

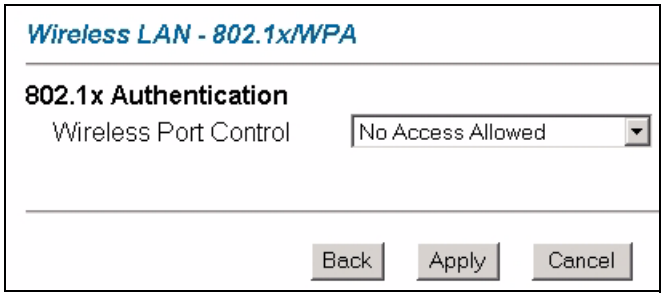
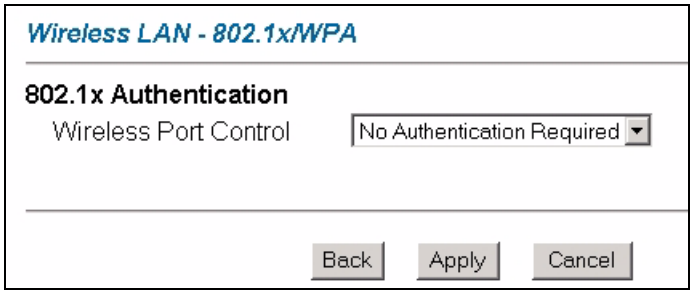


Рис. 26 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: No Authentication Required (Аутентификация не требуется)



В следующей таблице представлено описание полей в этих окнах.

Табл. 15 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: No Access/ Authentication

ПОЛЕ	ОПИСАНИЕ
Wireless Port Control (Управление беспроводной точкой доступа)	Для управления доступом беспроводного устройства к проводной сети выберите метод управления из раскрывающегося списка. Выберите **No Access Allowed (Доступ запрещен)**, **No Authentication Required (Аутентификация не требуется)** или **Authentication Required (Требуется аутентификация)**. **No Access Allowed** блокирует доступ всех беспроводных устройств к проводной сети. **No Authentication Required** разрешает доступ всех беспроводных устройств к проводной сети без введения имен пользователей и паролей. Этот вариант является значением по умолчанию. **Authentication Required** означает, что все беспроводные устройства должны ввести имена пользователей и пароли для подключения к проводной сети. Для настройки **Key Management Protocol** (Протокола управления ключами) и других относящихся к нему полей выберите **Authentication Required**.
Back (Назад)	Нажмите **Back**, чтобы вернуться к экрану основного меню настроек беспроводной локальной сети.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

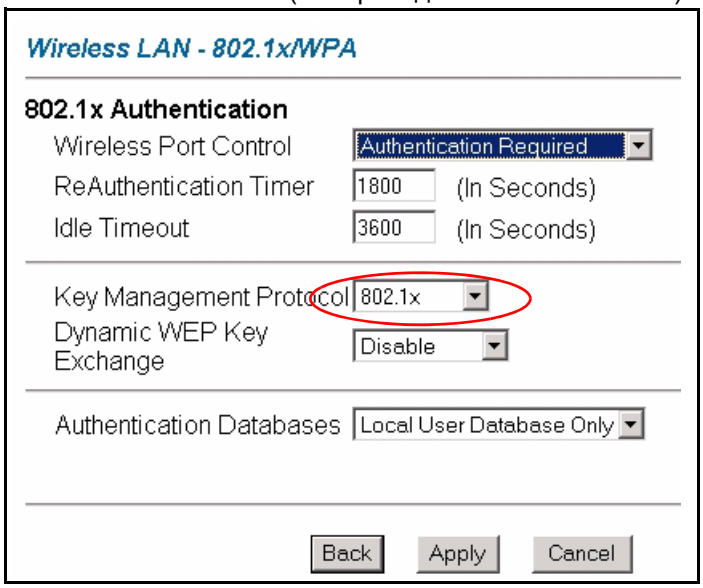
5.7.2 Authentication Required (Требуется аутентификация): 802.1x

Для аутентификации IEEE 802.1x необходимо следующее:

- Компьютер с сетевым адаптером IEEE 802.11b/g и Web-браузером (с поддержкой JavaScript) и/или Telnet.
- Компьютер с беспроводным устройством должен управляться IEEE 802.1x-совместимым программным обеспечением. Не все операционные системы Windows поддерживают стандарт IEEE 802.1x (подробную информацию можно найти на сайте Microsoft). По другим операционным системам см. соответствующую сопроводительную документацию. Если операционная система не поддерживает IEEE 802.1x, необходимо установить клиентское программное обеспечение IEEE 802.1x.
- Дополнительно: сетевой сервер RADIUS для аутентификации и учета удаленных пользователей.

Выберите **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа)** и **802.1x** в поле **Key Management Protocol (Протокол управления ключами)** — откроется следующее окно.

Рис. 27 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: 802.1x



В следующей таблице даны описания полей этого окна.

Табл. 16 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: 802.1x

ПОЛЕ	ОПИСАНИЕ
Wireless Port Control (Управление беспроводной точкой доступа)	Для управления доступом беспроводного устройства к проводной сети выберите метод управления из раскрывающегося списка. Выберите **No Authentication Required (Аутентификация не требуется)**, **Authentication Required (Требуется аутентификация)** или **No Access Allowed (Доступ запрещен)**. Следующие поля доступны только, если выберано **Authentication Required**.
ReAuthentication Timer (Таймер повторной аутентификации (в секундах)	Определите как часто беспроводное устройство должно повторно передавать имя пользователя и пароль для того, чтобы оставаться в сети. Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа).** Введите период времени в диапазоне от 10 до 9999 секунд. Временной интервал по умолчанию — **1800** секунд (30 минут). **ПРИМЕЧАНИЕ:** Если аутентификация беспроводного устройства производится с помощью сервера RADIUS, таймер повторной аутентификации на сервере RADIUS имеет приоритет.
Idle Timeout (Время простоя, сек.)	Интернет-центр автоматически отключает беспроводное устройство от проводной сети по истечении периода простоя. Для подключения к проводной сети беспроводное устройство должно снова отправить имя пользователя и пароль. Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа).** По умолчанию устанавливается значение в **3600** секунд (или 1 час).

Табл. 16 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: 802.1x

ПОЛЕ	ОПИСАНИЕ
Key Management Protocol (Протокол управления ключами)	Выберите **802.1x** из раскрывающегося списка.
Dynamic WEP Key Exchange (динамический обмен ключами WEP)	Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа).** Также в поле **Authentication Databases (Базы данных аутентификации)** установите опцию **RADIUS Only (Только RADIUS)**. Встроенные базы данных пользователей можно не использовать. Чтобы беспроводные устройства могли поддерживать связь с точками доступа без использования динамического обмена ключами WEP, выберите опцию **Disable (Отключить)**. Выберите **64-bit WEP**, **128-bit WEP** или **256-bit WEP** для использования шифрования данных соответствующей разрядности. При заданных параметрах динамического обмена ключами WEP, доступ к интернет-центру могут получить до 32 устройств. Это поле недоступно, если **Протокол управления ключами (Key Management Protocol)** установлен на **WPA** или **WPA-PSK**.
Authentication Databases (Базы данных аутентификации)	База данных аутентификации содержит регистрационные сведения о беспроводном устройстве. Локальная база данных пользователей — это встроенная база данных интернет-центра. RADIUS — это внешний сервер. Используйте этот раскрывающийся список для выбора базы данных, которой интернет-центр будет пользоваться для аутентификации беспроводного устройства (в первую очередь). Прежде, чем выставить приоритет, убедитесь, что соответствующая база данных установлена надлежащим образом. Для того, чтобы интернет-центр выполнял проверку имени пользователя и пароля беспроводного устройства по встроенной базе данных пользователя, выберите опцию **Local User Database Only (Только встроенная база данных пользователей)**. Для того, чтобы интернет-центр выполнял проверку имени пользователя и пароля беспроводного устройства по базе данных пользователя, находящейся на указанном сервере RADIUS, выберите опцию **RADIUS Only (Только RADIUS)**. Для того, чтобы интернет-центр выполнял проверку имени пользователя и пароля беспроводного устройства сначала по базе данных пользователя, находящейся в интернет-центре, выберите опцию **Local first, then RADIUS (Сначала встроенная база данных пользователей, затем RADIUS)**. Если имя пользователя не найдено, интернет-центр производит проверку по базе данных пользователей, находящейся на указанном сервере RADIUS. Для того, чтобы интернет-центр выполнял проверку имени пользователя и пароля беспроводного устройства сначала по базе данных пользователя, находящейся на указанном сервере RADIUS, выберите опцию **RADIUS first, then Local (Сначала RADIUS, затем встроенная база данных пользователей)**. Если интернет-центр не может получить доступ к серверу RADIUS, то он производит проверку по встроенной базе данных пользователей, находящейся в самом интернет-центре. Если имя пользователя не найдено или пароль не соответствует тому, что указано на сервере RADIUS, интернет-центр не производит их проверку по встроенной базе данных пользователей и аутентификация не проходит.
Back (Назад)	Нажмите **Back**, чтобы вернуться к экрану основного меню настроек беспроводной локальной сети.

Табл. 16 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: 802.1x

ПОЛЕ	ОПИСАНИЕ
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

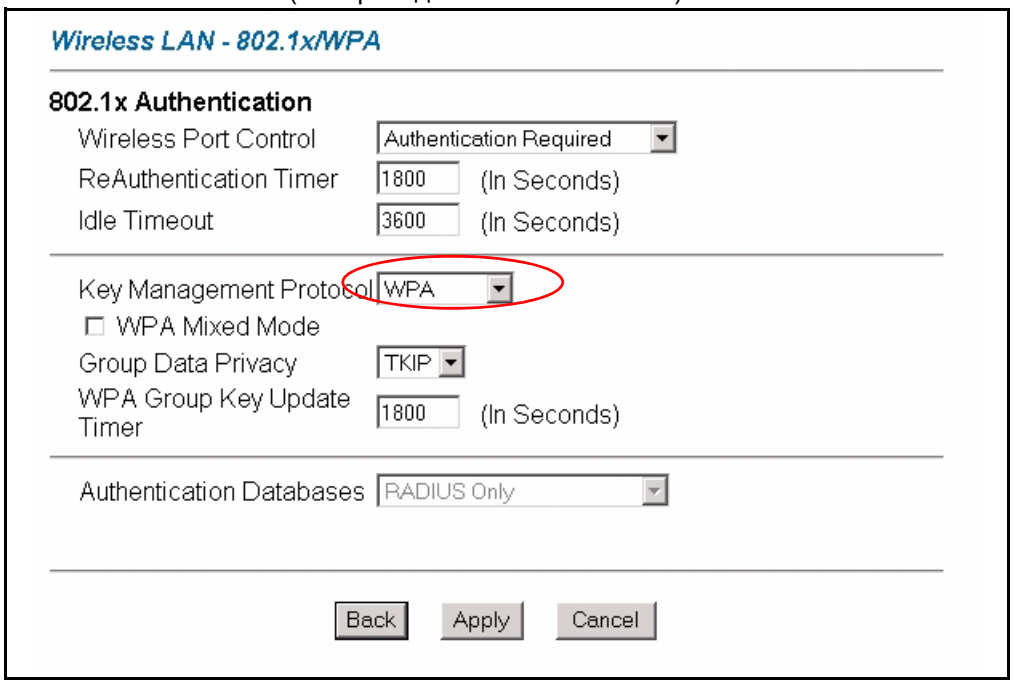
ПРИМЕЧАНИЕ: Если функция аутентификации пользователей включена, необходимо указать внешний сервер RADIUS или создать локальные учетные записи пользователей в интернет-центре.

5.7.3 Authentication Required (Требуется аутентификация): WPA

Выберите **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа)** и **WPA** в поле **Key Management Protocol (Протокол управления ключами)** — откроется следующее окно.

Более подробную информацию см. в Разд. 5.6 на с. 86.

Рис. 28 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: WPA



В приведенной ниже таблице даны описания полей, не рассматривавшихся ранее.

Табл. 17 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: WPA

ПОЛЕ	ОПИСАНИЕ
Key Management Protocol (Протокол управления ключами)	В данном поле выберите **WPA**.
WPA Mixed Mode (Смешанный режим WPA)	Интернет-центр может функционировать в режиме **WPA Mixed Mode**, который обеспечивает работу в одной сети Wi-Fi как клиентов, использующих WPA, так и клиентов, использующих динамический обмен ключами WEP при помощи 802.1x. Поставьте флажок для включения режима **WPA mixed**, или уберите флажок и заполните поле **Group Data Privacy (Конфиденциальность данных группы)**.
Group Data Privacy (Конфиденциальность данных группы)	В поле **Group Data Privacy** можно выбрать **TKIP** (рекомендуется) или **WEP** для широковещательного и многоадресного ("группового") трафика, если в **Key Management Protocol** выбран **WPA,** а **WPA Mixed Mode** — отключен. При включении **смешанного режима WPA (WPA Mixed Mode) WEP** задействуется автоматически. При выборе **протокола управления ключами WPA** или **WPA-PSK**, весь одноадресный трафик автоматически шифруется методом **TKIP**.

Табл. 17 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: WPA

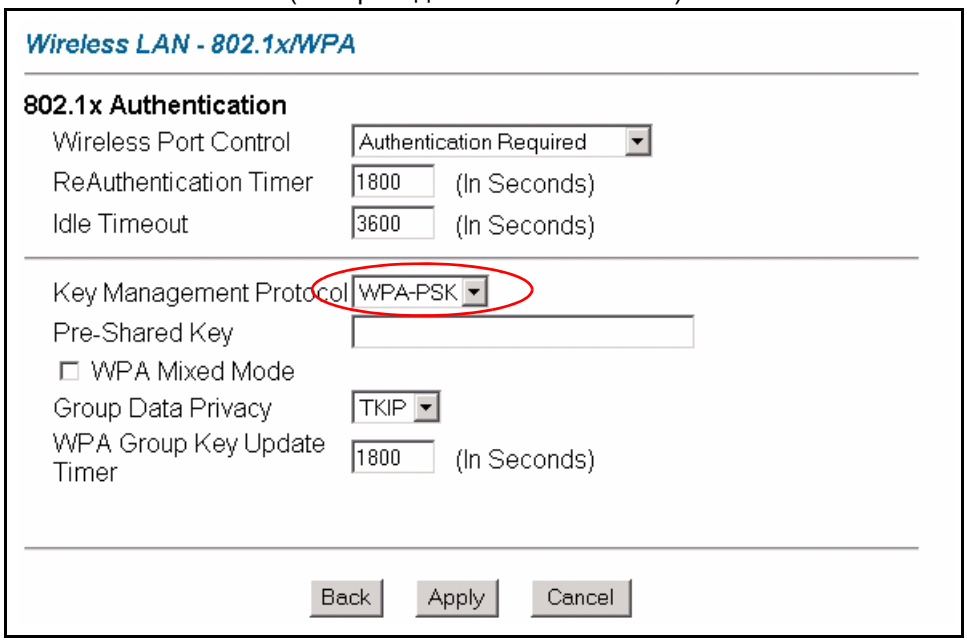
ПОЛЕ	ОПИСАНИЕ
WPA Group Key Update Timer (Таймер обновлений групповых ключей WPA)	**WPA Group Key Update Timer** — это периодичность, с которой точка доступа (если используется управление ключами **WPA-PSK**) или сервер RADIUS (если используется управление ключами **WPA**) отправляет новый групповой ключ всем клиентам. Процесс повторной настройки по ключу является WPA-эквивалентом автоматической замены ключей WEP для точки доступа и всех устройств беспроводной локальной сети на периодической основе. Настройка **WPA Group Key Update Timer** поддерживается и в режиме WPA-PSK. По умолчанию в интернет-центре установлено значение времени в 1800 секунд (30 минут).
Authentication Databases (Базы данных аутентификации)	Если для **WPA (Защищенного беспроводного доступа)** используется **Протокол управления ключами (Key Management Protocol),** то в качестве **Баз данных аутентификации (Authentication Databases)** должен использоваться только сервер **RADIUS**. Опцию **Local User Database Only (Только встроенная база пользователей)** можно использовать только с протоколом управления ключами **802.1x Key Management Protocol**.

5.7.4 Authentication Required (Требуется аутентификация): WPA-PSK

Выберите **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа)** и **WPA-PSK** в поле **Key Management Protocol (Протокол управления ключами)** — откроется следующее окно.

Более подробную информацию см. в Разд. 5.6 на с. 86.

Рис. 29 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA:WPA-PSK



В приведенной ниже таблице даны описания полей, не рассматривавшихся ранее.

Табл. 18 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: WPA-PSK

ПОЛЕ	ОПИСАНИЕ
Key Management Protocol (Протокол управления ключами)	В данном поле выберите **WPA-PSK** .
Pre-Shared Key (Предварительно согласованный ключ)	Механизмы шифрования, используемые для **WPA** и **WPA-PSK,** одинаковы. Разница между WPA и WPA-PSK состоит в том, что **WPA-PSK** использует единственный предварительно согласованный ключ (пароль) для аутентификации всех пользователей, в то время как WPA предполагает наличие индивидуального пароля у каждого пользователя. Введите предварительно согласованный ключ длиной от 8 до 63 печатных знаков (включая пробелы и с учетом регистра для букв алфавита).
WPA Mixed Mode (Смешанный режим WPA)	Интернет-центр может функционировать в режиме **WPA Mixed Mode**, который обеспечивает работу в одной сети Wi-Fi как клиентов, использующих WPA, так и клиентов, использующих динамический обмен ключами WEP при помощи 802.1x. Поставьте флажок для включения режима **WPA mixed**, или уберите флажок и заполните поле **Group Data Privacy (Конфиденциальность данных группы)**.

Табл. 18 Wireless LAN (Беспроводная локальная сеть): 802.1x/WPA: WPA-PSK

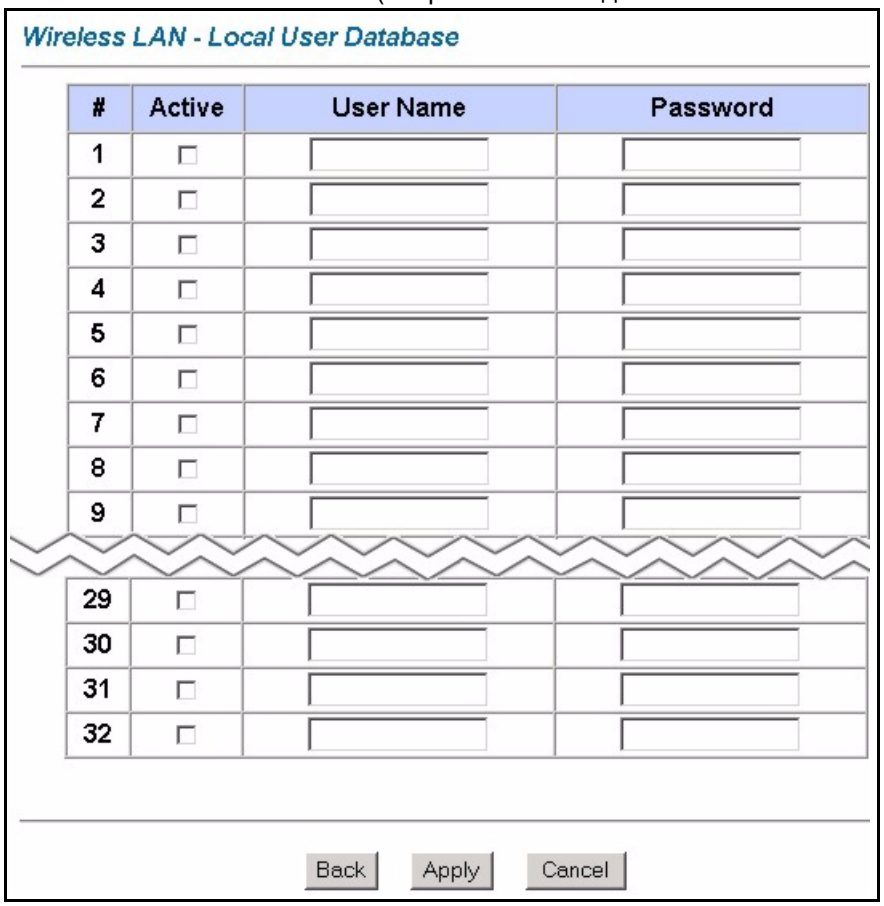
ПОЛЕ	ОПИСАНИЕ
Group Data Privacy (Конфиденциальность данных группы)	В поле **Group Data Privacy** можно выбрать **TKIP** (рекомендуется) или **WEP** для широковещательного и многоадресного ("группового") трафика, если в **Key Management Protocol** выбран **WPA,** а **WPA Mixed Mode** — отключен. При включении **смешанного режима WPA (WPA Mixed Mode) WEP** задействуется автоматически. При выборе **протокола управления ключами WPA** или **WPA-PSK**, весь одноадресный трафик автоматически шифруется методом **TKIP**.
Authentication Databases (Базы данных аутентификации)	Данное поле доступно только при включенном режиме **WPA Mixed Mode**.

5.8 Настройка локальной аутентификации пользователей

Благодаря локальному сохранению пользовательских профилей, интернет-центр способен определять подлинность беспроводных пользователей, не взаимодействуя с сетевым сервером RADIUS. Однако существует ограничение на число пользователей, которых можно аутентифицировать таким образом.

Для изменения встроенной базы данных пользователей интернет-центра нажмите **Wireless LAN**, **Local User Database**. При этом откроется показанное ниже окно.

Рис. 30 Local User Database (Встроенная база данных пользователей)



В следующей таблице даны описания полей этого окна.

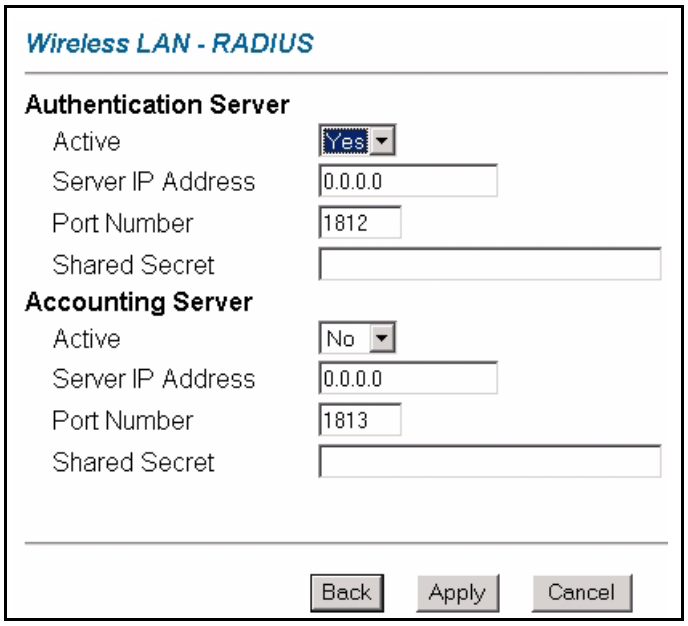
Табл. 19 Local User Database (Встроенная база данных пользователей)

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер локальной учетной записи пользователя.
Active (Активировать)	Поставьте галочку в этом поле для включения данной пользовательской настройки
Имя пользователя	Введите имя пользователя, длиной до 31 буквенно-цифрового символа (с учетом регистра; допускаются дефисы '-' и '_'), если Вы используете шифрование MD5, и до 14 символов, если Вы используете PEAP.
Пароль	Введите пароль длиной не более 31 печатного знака ASCII (включая пробелы и с учетом регистра для букв алфавита), если Вы используете шифрование MD5, и до 14 символов, если Вы используете PEAP.
Back (Назад)	Нажмите **Back**, чтобы вернуться к экрану основного меню настроек беспроводной локальной сети.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

5.9 Настройка сервера RADIUS

Для создания в интернет-центре настроек сервера RADIUS нажмите **WIRELESS LAN**, **RADIUS**. При этом откроется показанное ниже окно.

Рис. 31 RADIUS



В следующей таблице даны описания полей этого окна.

Табл. 20 RADIUS

ПОЛЕ	ОПИСАНИЕ
Authentication Server (Сервер аутентификации)	
Active (Активировать)	Выберите **Yes** из раскрывающегося списка для включения аутентификации пользователей с помощью сервера внешней аутентификации.
Server IP Address (IP-адрес сервера)	Введите в этом поле IP-адрес внешнего сервера аутентификации в десятичном виде с разделительными точками.
Номер порта	По умолчанию, для сервера аутентификации RADIUS устанавливается порт **1812**. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.
Shared Secret (Общий секретный ключ)	Введите пароль (до 31 буквенно-цифрового символа) в качестве ключа, общего для внешнего сервера аутентификации и точек доступа. Этот ключ не передается по сети. Интернет-центр и внешний сервер аутентификации должны использовать один и тот же ключ.
Accounting Server (Сервер учета)	
Active (Активировать)	Выберите **Yes** из раскрывающегося списка для включения аутентификации пользователей с помощью сервера учета.

Табл. 20 (продолжение)RADIUS

ПОЛЕ	ОПИСАНИЕ
Server IP Address (IP-адрес сервера)	Введите в этом поле IP-адрес внешнего сервера учета в десятичном виде с разделительными точками.
Номер порта	По умолчанию, для сервера учета RADIUS устанавливается порт **1813**. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.
Shared Secret (Общий секретный ключ)	Введите пароль (до 31 буквенно-цифрового символа) в качестве ключа, общего для внешнего сервера учета и точек доступа. Этот ключ не передается по сети. Интернет-центр и внешний сервер учета должны использовать один и тот же ключ.
Back (Назад)	Нажмите **Back**, чтобы вернуться к экрану основного меню настроек беспроводной локальной сети.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

Глава 6
Настройка глобальной сети

В этой главе описывается настройка глобальной сети.

6.1 Общая информация о глобальной сети

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

6.1.1 Инкапсуляция

Убедитесь, что используется метод инкапсуляции, предписанный Вашим Интернет-провайдером. Интернет-центр P–660HT/HTW EE поддерживает следующие методы.

6.1.1.1 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 транспортные 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.

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

Протокол PPPoE обеспечивает функции учета и управления доступом аналогично услуге доступа по коммутируемой линии с использованием протокола PPP. Интернет-центр инициирует PPP-сеанс (PPP поверх Ethernet, RFC 2516) с сервером провайдера через мост по постоянному виртуальному каналу ATM PVC (Permanent Virtual Circuit — PVC), который соединяется с DSL-коммутатором. Один постоянный виртуальный канал (PVC) может поддерживать любое количество сеансов PPP из локальной сети. Для получения дополнительной информации по PPPoE, см. приложения.

6.1.1.3 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 функционирует подобно коммутируемому подключению к Интернет. Интернет-центр инкапсулирует сеанс связи PPP на основе RFC1483 и пересылает его по постоянному виртуальному каналу ATM (PVC) к DSL-коммутатору Интернет-провайдера. Для получения дополнительной информации по PPPoA см. комментарий RFC 2364. Для информации по PPP см. комментарий RFC 1661.

6.1.1.4 RFC 1483

RFC 1483 описывает два способа многопротокольной инкапсуляции на уровне 5 адаптации ATM (AAL5). Первый метод обеспечивает мультиплексирование 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.

6.1.2 Мультиплексирование

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

6.1.2.1 Мультиплексирование на базе VC

При таком способе мультиплексирования, по предварительному взаимному соглашению, за каждым протоколом закрепляется конкретный виртуальный канал, например, по VC1 передается IP, и т. д. Мультиплексирование на базе VC может быть основным методом в сетевом окружении, где динамическое создание большого числа виртуальных каналов ATM является более быстрым и экономичным.

6.1.2.2 Мультиплексирование на базе LLC

При таком способе мультиплексирования по одному виртуальному каналу передается несколько протоколов с идентифицирующей информацией, которая содержится в заголовке каждого пакета. Несмотря на передачу дополнительных данных и затраты на обработку служебной информации, этот метод может оказаться предпочтительнее там, где иметь отдельный виртуальный канал для каждого передаваемого протокола нерационально, например, если оплата во многом зависит от количества одновременно функционирующих виртуальных каналов.

6.1.3 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 номеров VPI — от 0 до 255, а для VCI — от 32 до 65535 (номера от 0 до 31 зарезервированы для локального управления трафиком ATM). Более подробную информацию см. в приложении.

6.1.4 Назначение IP-адреса

Статический IP-адрес — это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является постоянным. В этом случае Интернет-провайдер каждый раз назначает новый IP-адрес. Функция учетной записи одиночного пользователя может быть включена или отключена, если вы имеете динамический или статический IP-адрес. Однако назначенный метод инкапсуляции влияет на выбор IP-адреса и шлюза ENET ENCAP.

6.1.4.1 Назначение IP с инкапсуляцией 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)**.

6.1.4.2 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.

6.1.4.3 Назначение IP с инкапсуляцией ENET ENCAP

В этом случае можно иметь как статический, так и динамический IP-адрес. 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 WAN-порт интернет-центра функционирует как клиент DHCP и, следовательно, поля **IP Address (IP-адрес)** и **ENET ENCAP Gateway (Шлюз ENET ENCAP)** являются недоступными (N/A), так как эти параметры для интернет-центра назначает сервер DHCP.

6.1.5 Постоянное соединение (по протоколу "точка-точка" — PPP)

Постоянное соединение — это коммутируемая линия с постоянно установленным соединением независимо от необходимости передачи трафика. При выборе постоянного соединения интернет-центр выполняет следующее: во-первых, отключает время простоя, во-вторых, восстанавливает соединение каждый раз при включении питания и после разрыва соединения. По очевидным причинам постоянное соединение может быть очень дорогим.

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

6.1.6 NAT (Трансляция сетевых адресов)

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.

6.2 Метрика

Метрика представляет собой "стоимость передачи данных". Маршрутизатор определяет наилучший маршрут для передачи, выбирая путь с самой низкой "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве единицы "стоимости", минимальное значение которой равно 1 и соответствует прямому соединению между сетями. Число, определяющее стоимость, должно лежать в интервале от "1" до "15"; значение больше "15" означает, что канал не работает. Чем меньше число, тем ниже "стоимость".

Метрика устанавливает приоритет для маршрутов в Интернете. Если какие-либо два маршрута по умолчанию имеют одинаковую метрику, интернет-центр использует следующие заранее установленные приоритеты:

- Стандартный маршрут: назначается Интернет-провайдером (см. Разд. 6.7 на с. 108)
- Маршрут перенаправления трафика (см. Разд. 6.8 на с. 112)
- Резервный маршрут WAN, известный также как резервирование коммутируемыми каналами (см. Разд. 6.9 на с. 113)

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 установить подключение к Интернету, тогда интернет-центр пытается использовать маршрут перенаправления трафика. Аналогичным образом, если соединение не удалось установить с помощью маршрута перенаправления трафика, интернет-центр использует резервный маршрут.

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.

6.3 Инкапсуляция PPPoE

Интернет-центр поддерживает протокол PPPoE (Point-to-Point Protocol over Ethernet — Протокол "точка-точка" поверх Ethernet). PPPoE — это проект стандарта IETF (RFC 2516), который определяет порядок взаимодействия персонального компьютера (PC) с широкополосным модемным (DSL, кабельным, беспроводным и т.д.) соединением. Протокол **PPPoE** предназначен для коммутируемого соединения с использованием PPPoE.

Для провайдера услуг протокол PPPoE обеспечивает метод доступа и аутентификации, который работает с существующими системами управления доступом (например, RADIUS). PPPoE также обеспечивает способ регистрации и аутентификации, поддерживаемый программным обеспечением для удаленного доступа в сеть от компании Microsoft, поэтому для пользователей Windows не требуется освоения новых методик.

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.

В случае установки PPPoE интернет-центром (а не на отдельных компьютерах), установка программного обеспечения PPPoE на компьютерах локальной сети не требуется, поскольку эта часть задачи выполняется интернет-центром. Кроме того, при включении функции NAT доступ будут иметь все компьютеры локальной сети.

6.4 Ограничение трафика

Ограничение трафика — это соглашение между оператором связи и абонентом, предназначенное для регулирования средней скорости и колебаний скорости передачи данных по сети ATM. Такое соглашение помогает устранить перегрузку каналов, 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 1 ячейки ATM равен 53 байта (424 бита), таким образом, при максимальной скорости передачи 832 кбит/с, максимальная скорость PCR равна 1962 ячеек/с. Однако эта скорость не гарантирована, так как зависит от скорости передачи в линии.

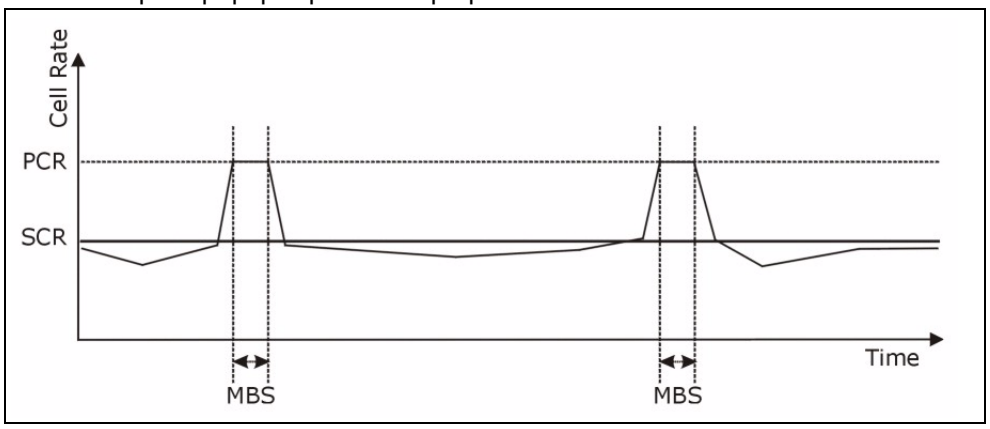
SCR (Sustained Cell Rate — Поддерживаемая скорость ячеек) — это средняя скорость ячеек каждого источника пульсирующего трафика. Она определяет максимальную среднюю скорость, с которой ячейки могут передаваться по виртуальному соединению. SCR не может быть больше, чем PCR.

MBS (Maximum Burst Size — Максимальный размер пакета) — это максимальное количество ячеек, которые можно передать со скоростью PCR. После достижения MBS, скорость ячеек падает ниже SCR, пока в среднем снова ее не достигнет. С этого момента снова может быть передано большее количество ячеек (до MBS) со скоростью 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. 32 Пример формирования трафика



6.5 Доступ в Интернет с использованием автоматической настройки модема (Zero Configuration)

После включения питания и подключения интернет-центра к телефонной розетке, устройство автоматически определяет настройки подключения к Интернету (такие как номер VCI/VPI и метод инкапсуляции) через Интернет-провайдера и выполняет необходимые изменения в конфигурации. В случае, если требуется ввод данных учетной записи Интернет (таких как имя пользователя и пароль) или если интернет-центр не может подключиться к оборудованию Интернет-провайдера, на экране появляется окно(а) для ввода регистрационной информации или поиска и устранения неисправностей.

Автоматическая настройка отключается, если:

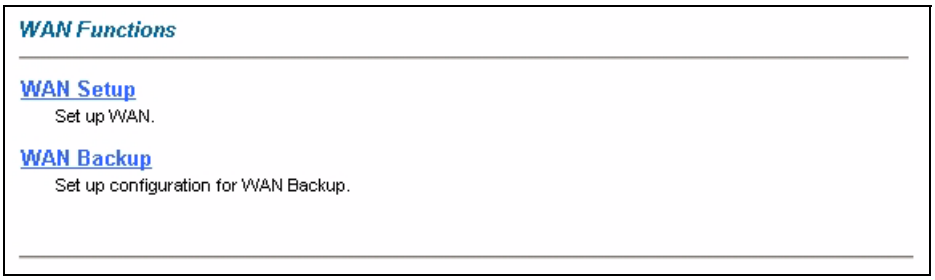
- Интернет-центр работает в режиме моста
- Интернет-центру назначен статический (постоянный) IP-адрес в глобальной сети.

6.6 Главное окно WAN

Нажмите **WAN** на панели навигации, чтобы открыть главное окно **WAN**.

Более подробную информацию см. в Разд. 6.1 на с. 102.

Рис. 33 WAN (Глобальная сеть)



В следующей таблице даны описания ссылок в этом окне.

Табл. 21 WAN

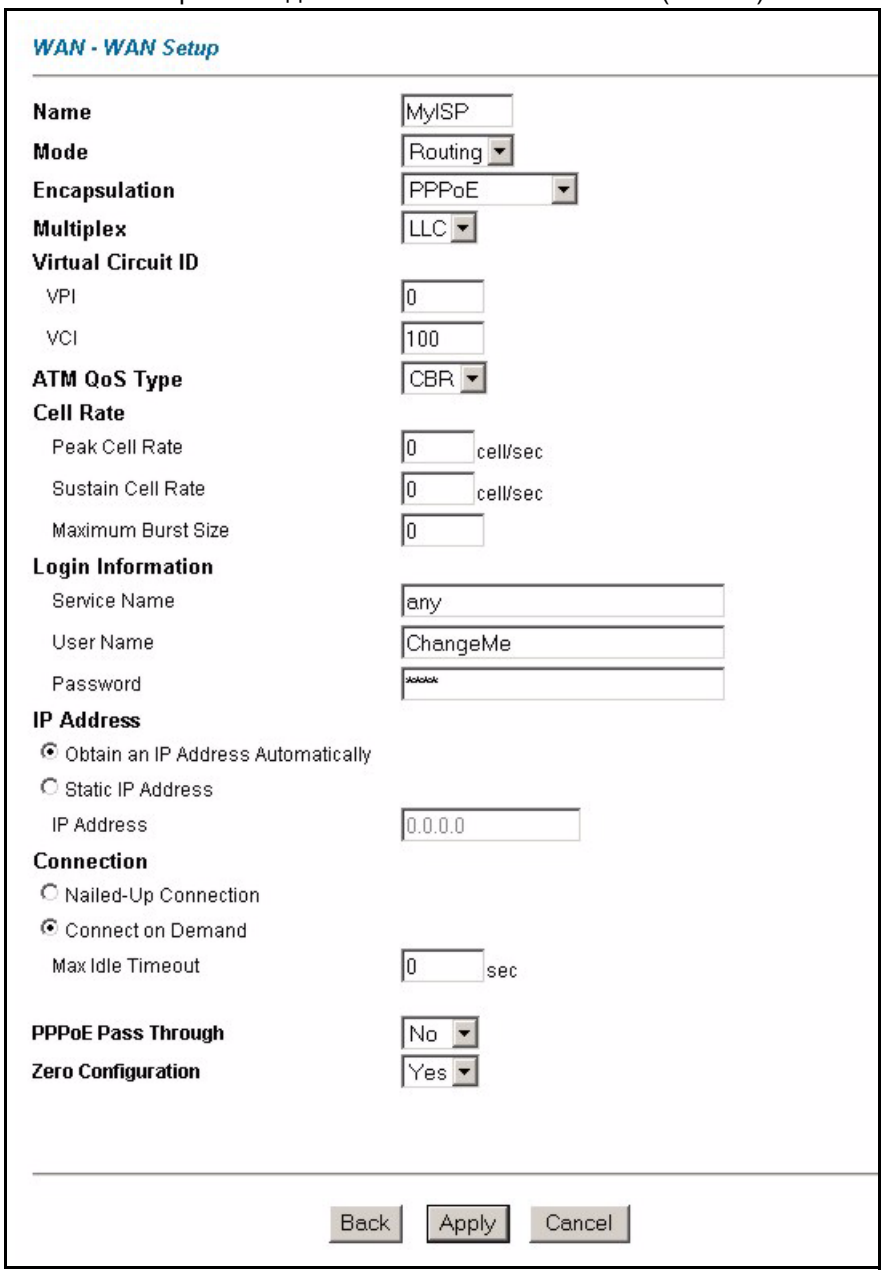
ССЫЛКА	ОПИСАНИЕ
WAN Setup (Настройка глобальной сети)	Щелкните по этой ссылке для перехода к окну, где можно настроить интернет-центр для подключения к Интернет.
WAN Backup (Резервирование глобальной сети)	Щелкните по этой ссылке для перехода к окну, где можно настроить резервные соединения с глобальной сетью (перенаправление трафика и резервное соединение через модем).

6.7 Настройка подключения к глобальной сети

Для изменения в интернет-центре настроек доступа в глобальную сеть нажмите **WAN (Глобальная сеть)** и **WAN Setup (Настройка глобальной сети)**. Появится окно, вид которого зависит от типа инкапсуляции.

Более подробную информацию см. в Разд. 6.1 на с. 102.

Рис. 34 Настройка подключения к глобальной сети (PPPoE)



В следующей таблице даны описания полей этого окна.

Табл. 22 WAN Setup (Настройка глобальной сети)

ПОЛЕ	ОПИСАНИЕ
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 использовать одни учетные данные для подключения к Интернету нескольких компьютеров. В противном случае выберите **Bridge (Мост)**.

Табл. 22 WAN Setup (Настройка глобальной сети) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Encapsulation (Инкапсуляция)	Выберите из раскрывающегося списка метод инкапсуляции, используемый вашим Интернет-провайдером. Опции в списке зависят от режима, установленного в поле **Mode (Режим)**. Если в поле **Mode (Режим)** вы установили **Bridge (Мост)**, то выберите **PPPoA** или **RFC 1483**. Если в поле **Mode (Режим)** вы установили **Routing (Маршрутизация)**, то выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
Multiplex (Мультиплексирование)	Выберите из раскрывающегося списка метод мультиплексирования, используемый вашим Интернет-провайдером. Вариантами являются **VC** или **LLC**.
Virtual Circuit ID (Идентификатор виртуальной линии передачи)	VPI (Virtual Path Identifier — Идентификатор виртуального пути) и VCI (Virtual Channel Identifier — Идентификатор виртуального канала) определяют виртуальную линию передачи. Более подробную информацию см. в приложении.
VPI	Допустимый диапазон для VPI равен от 0 до 255. Введите назначенный вам номер VPI.
VCI	Допустимый диапазон для VCI равен от 32 до 65535 (номера от 0 до 31 зарезервированы для локального управления трафиком ATM). Введите назначенный вам номер VCI.
ATM QoS Type (Тип качества обслуживания ATM)	Выберите **CBR** (Постоянная скорость передачи) для установки постоянной (всегда доступной) пропускной способности для трафика речи или данных. Выберите **UBR** (Unspecified Bit Rate — Неопределенная скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите **VBR** (Variable Bit Rate — Переменная скорость передачи) для пульсирующего трафика и разделения пропускной способности с другими приложениями.
Cell Rate (Скорость ячеек)	Настройка скорости ячеек часто помогает устранить перегрузку в сети, которая снижает скорость передачи данных в реальном времени, таких как аудио и видео трафик.
Peak Cell Rate (Пиковая скорость ячеек)	Чтобы найти PCR (Peak Cell Rate — Пиковая скорость ячеек), разделите скорость DSL линии (бит/с) на 424 (размер ячейки ATM). Это 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.
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).
Login Information (Регистрационные данные)	(Только для инкапсуляции PPPoA и PPPoE)
Service Name (Имя услуги)	(Только для PPPoE) Введите имя услуги PPPoE в это поле.

Табл. 22 WAN Setup (Настройка глобальной сети) (продолжение)

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 вводите оба элемента имени в полном соответствии с данными от провайдера.
Password (Пароль)	Введите пароль для данного имени пользователя.
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 постоянным. В этом случае Интернет-провайдер будет назначать новый адрес при каждом подключении к Интернету. Выберите **Obtain an IP Address Automatically (Получить IP-адрес автоматически)**, если у вас динамический IP-адрес; или выберите **Static IP Address (Статический IP-адрес)** и введите предоставленный Интернет-провайдером IP-адрес в расположенное ниже текстовое поле "IP Address".
Connection (Подключение) (Только для инкапсуляции PPPoA и PPPoE)	Правило(а) расписания связи в меню SMT 26 имеет приоритет над настройками полей **Connection (Подключение)**.
Nailed-Up Connection (Постоянное соединение)	Выберите **Nailed-Up Connection (Постоянное соединение)**, если требуется постоянное соединение. При разрыве соединения интернет-центр будет автоматически пытаться его восстановить.
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 Интернет не будет разрываться .
PPPoE Pass Through (Транзит PPPoE-соединений) (Только для инкапсуляции PPPoE)	Это поле доступно, если вы выбрали инкапсуляцию **PPPoE**. В дополнение к встроенному в интернет-центр клиенту PPPoE, вы можете включить функцию транзита PPPoE-соединений, чтобы разрешить до 10 узлам локальной сети использовать программное обеспечение клиента PPPoE для подключения к Интернет-провайдеру через интернет-центр. 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.
Subnet Mask (Маска подсети) (Только для инкапсуляции ENET ENCAP)	Введите маску подсети в десятичном формате с разделительными точками. Если требуется создание подсетей, см. приложения для расчета маски подсети.

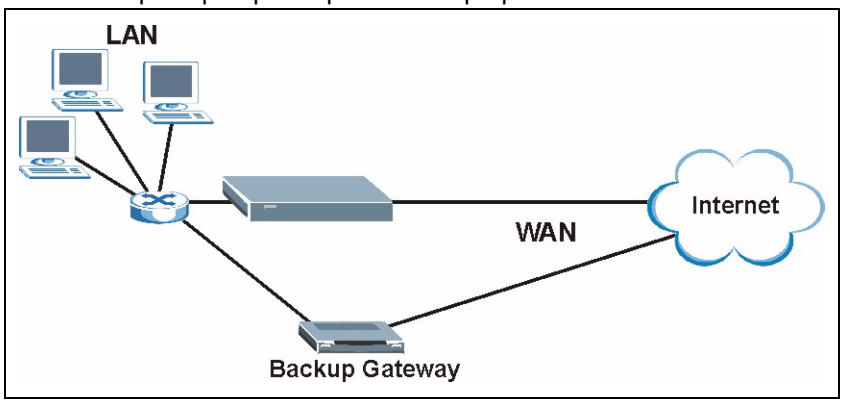
Табл. 22 WAN Setup (Настройка глобальной сети) (продолжение)

ПОЛЕ	ОПИСАНИЕ
ENET ENCAP Gateway (Шлюз ENET ENCAP) (Только для инкапсуляции ENET ENCAP)	Необходимо указать IP-адрес шлюза (предоставленный вашим Интернет-провайдером), если в поле **Encapsulation (Инкапсуляция)** установлен тип инкапсуляции **ENET ENCAP**.
Zero Configuration (Автоматическая настройка на провайдера)	Эта функция не применяется/недоступна, если в конфигурации интернет-центра используется статический IP-адрес глобальной сети или режим моста. Выберите **Yes (Да)**, чтобы интернет-центр автоматически определял настройки подключения к Интернету (такие как номера VCI/VPI и метод инкапсуляции) через Интернет-провайдера и выполнял необходимые изменения в конфигурации. Выберите **No (Нет)** для отключения этой функции. Вам придется вручную настраивать интернет-центр для получения доступа в Интернет.
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 заново начать настройку в этом окне.

6.8 Перенаправление трафика (Traffic Redirect)

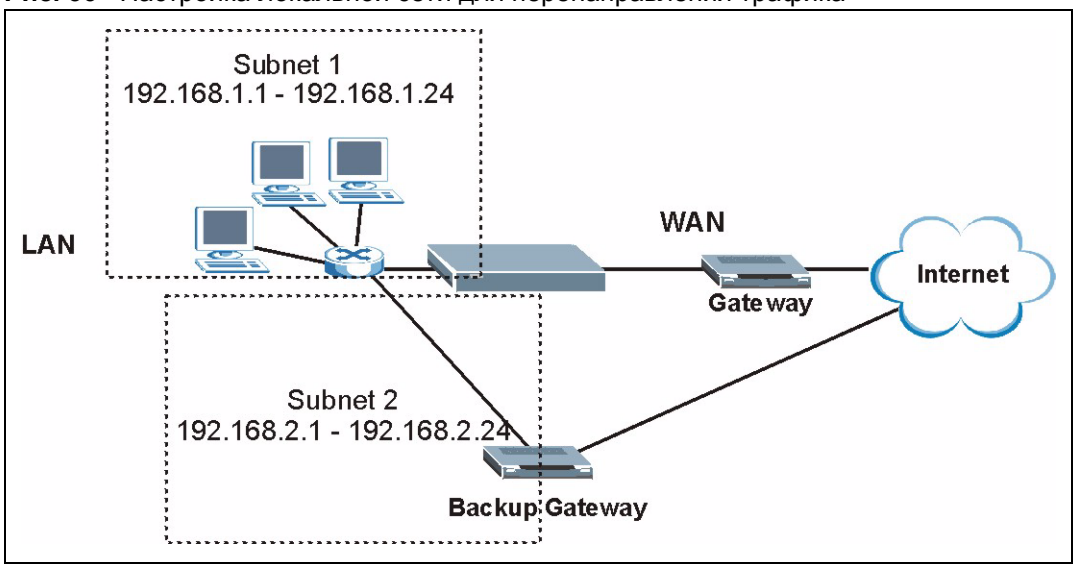
Функция перенаправления трафика пересылает трафик на резервный шлюз, если интернет-центр не может подключиться к Интернету. Пример показан на следующем рисунке.

Рис. 35 Пример перенаправления трафика



Следующая топология сети позволяет избежать проблем безопасности при треугольном маршруте, если к локальной сети подключен резервный шлюз. С помощью псевдонимов IP локальная сеть разделяется на две или три логических сети, где интернет-центр является шлюзом для каждой логической локальной сети. Поместите защищенную локальную сеть в одну подсеть (Подсеть 1 на следующем рисунке), а резервный шлюз — в другую подсеть (Подсеть 2). Настройте фильтры, которые пропускают пакеты от защищенной локальной сети (Подсеть 1) к резервному шлюзу (Подсеть 2).

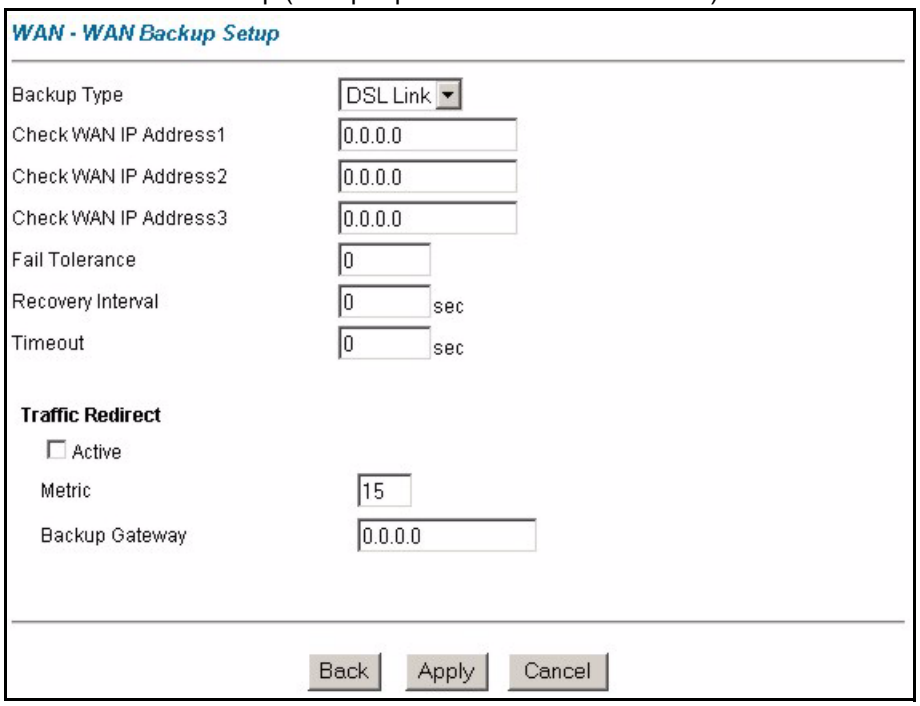
Рис. 36 Настройка локальной сети для перенаправления трафика



6.9 Настройка резервного соединения с глобальной сетью

Для изменения настроек интернет-центра, связанных с резервированием порта WAN, нажмите **WAN (Глобальная сеть)**, затем **WAN Backup (Резервирование глобальной сети)**. При этом откроется показанное ниже окно.

Рис. 37 WAN Backup (Резервирование глобальной сети)



В следующей таблице даны описания полей этого окна.

Табл. 23 Резервирование глобальной сети

ПОЛЕ	ОПИСАНИЕ
Backup Type (Тип резервирования)	Выберите метод, который интернет-центр будет использовать для проверки соединения DSL. Выберите **DSL Link** (**Канал DSL)**, чтобы интернет-центр проверял, установлено ли подключение к DSL-коммутатору. Выберите **ICMP** (Internet Control Message Protocol — Протокол управляющих сообщений в сети Интернет), чтобы интернет-центр периодически выполнял эхо-тестирование IP-адресов, введенных в полях **Check WAN IP Address (Проверять IP-адрес глобальной сети)**.
Check WAN IP Address1-3 (Проверять IP-адреса глобальной сети 1-3)	Заполните эти поля, чтобы интернет-центр 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 с глобальной сетью интернет-центр периодически проводит эхо-тестирование заданных здесь адресов и, если не получает ответа, использует другое резервное соединение (если таковое настроено).
Fail Tolerance (Допустимое число отсутствий ответов)	Введите число (рекомендуется 2), которое показывает, сколько раз интернет-центр будет выполнять эхо-тестирование IP-адресов, введенных в поле **Check WAN IP Address (Проверять IP-адреса глобальной сети)** при отсутствии ответа, прежде чем переключиться на какое-либо из резервных соединений.

Табл. 23 Резервирование глобальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
Recovery Interval (Интервал восстановления)	Когда интернет-центр использует соединение с более низким приоритетом (обычно резервное соединение с глобальной сетью), устройство периодически проверяет, можно или нет перейти на соединение с более высоким приоритетом. Введите интервал между проверками в секундах (рекомендуется 30). Увеличьте время, если в устройстве с IP-адресом получателя обрабатывается большой объем трафика.
Timeout (Время ожидания)	Введите время в секундах (рекомендуется 3), в течение которого интернет-центр ожидает ответ на эхо-запрос от одного из IP-адресов, введенных в поле **Check WAN IP Address (Проверять IP-адреса глобальной сети)**, прежде чем повторить запрос. Подключение к глобальной сети рассматривается как "недоступное", после того как интернет-центр выполнил проверки, число которых установлено в поле **Fail Tolerance (Допустимое число отсутствий ответов)**. Установите в этом поле большее значение, если ваша сеть очень занята или перегружена.
Traffic Redirect (Перенапра-вление трафика)	Функция перенаправления трафика пересылает трафик на резервный шлюз, если интернет-центр не может подключиться к Интернету.
Active (Активировать)	Поставьте в этом поле флажок, чтобы интернет-центр использовал перенаправление трафика, в случае если основное подключение к глобальной сети не работает. **ПРИМЕЧАНИЕ:** При включении функции перенаправления трафика, необходимо настроить хотя бы одно поле Check WAN IP Address (Проверять IP-адреса глобальной сети).
Metric (Метрика)	В этом поле устанавливается приоритет маршрутов, которые использует интернет-центр. Метрика представляет собой "стоимость передачи данных". Маршрутизатор определяет наилучший маршрут для передачи, выбирая путь с самой низкой "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве единицы "стоимости", минимальное значение которой равно 1 и соответствует прямому соединению между сетями. Число, определяющее стоимость, должно лежать в интервале от "1" до "15"; значение больше "15" означает, что канал не работает. Чем меньше число, тем ниже "стоимость".
Backup Gateway (Резервный шлюз)	Введите IP-адрес резервного шлюза в десятичном формате с разделительными точками. Интернет-центр автоматически пересылает трафик на этот IP-адрес при разрыве подключения к Интернету.
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 заново начать настройку в этом окне.

Глава 7
Окна NAT (Трансляция сетевых адресов)

В данной главе описывается настройка функции NAT в интернет-центре.

7.1 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.

7.1.1 Определения NAT

Определение внутренний/внешний означает местоположение узла относительно интернет-центра, например, компьютеры абонентов являются внутренними узлами, тогда как web-серверы в Интернете 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. 24 Определения NAT

ПАРАМЕТР	ОПИСАНИЕ
Inside (Внутренний)	Относится к узлу в локальной сети.
Outside (Внешний)	Относится к узлу в глобальной сети.

Табл. 24 Определения NAT (продолжение)

ПАРАМЕТР	ОПИСАНИЕ
Local (Локальный)	Относится к адресу пакета (источника или адресата), когда пакет перемещается в локальной сети.
Global (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.

7.1.2 Назначение NAT

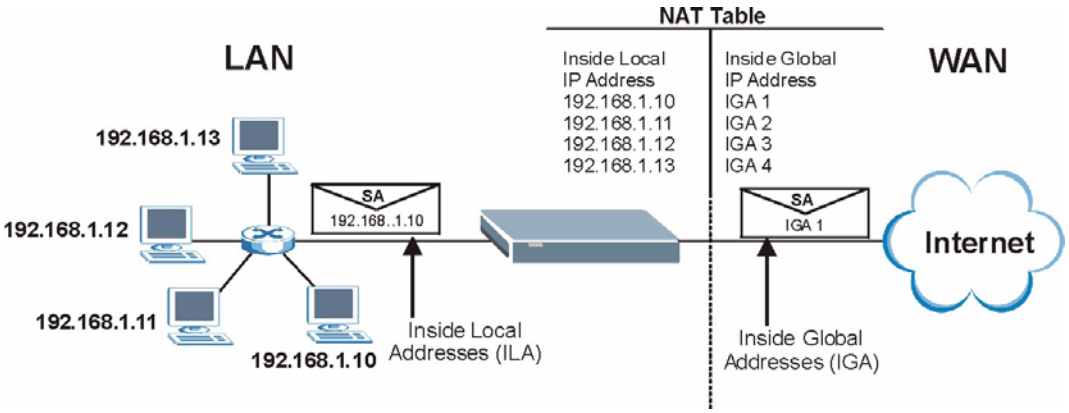
В простейшем случае NAT изменяет IP-адрес источника в пакете, принятом от абонента (внутренний локальный адрес) на другой (внутренний глобальный адрес) перед передачей пакета в глобальную сеть. При получении ответа NAT преобразовывает адрес получателя (внутренний глобальный адрес) обратно во внутренний 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 перекрытием — см. Табл. 25 на с. 119), NAT предлагает дополнительное преимущество защиты сети с помощью межсетевого экрана. Если серверы не определены, интернет-центр будет отфильтровывать все входящие запросы, предотвращая проверку вашей сети на уязвимость злоумышленниками. Дополнительные сведения о трансляции IP-адресов см. Комментарий *RFC 1631*, *"Трансляция сетевых IP-адресов (NAT)*".

7.1.3 Как работает NAT

Каждый пакет имеет два адреса — адрес источника и адрес назначения. Для исходящих пакетов, внутренний локальный адрес (ILA) является адресом источника в локальной сети, а внутренний глобальный адрес (IGA) — адресом источника в глобальной сети. Для входящих пакетов, ILA — это адрес получателя в локальной сети, а IGA — адрес получателя 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. Интернет-центр сохраняет исходные адреса и номера портов, чтобы входящие ответные пакеты могли содержать восстановленные первоначальные значения. Это показано на следующем рисунке.

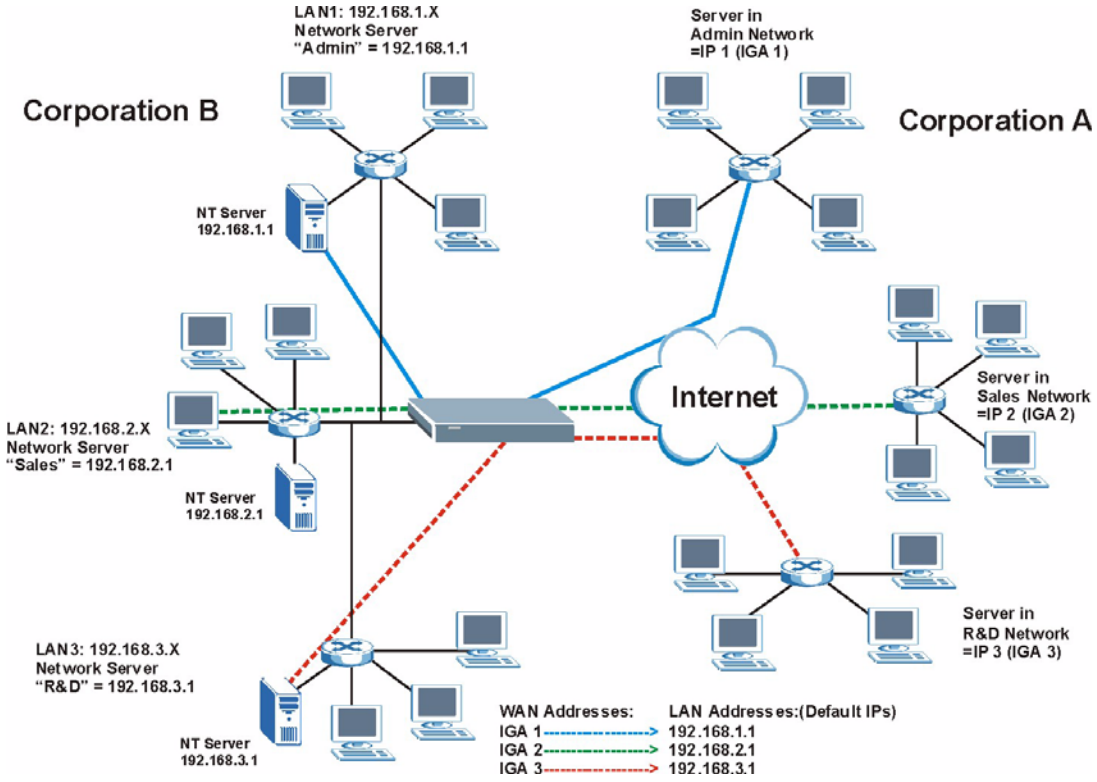
Рис. 38 Как работает NAT



7.1.4 Применение NAT

На следующем рисунке приведен вариант применения NAT, где три внутренних локальных сети (логические локальные сети, образованные с помощью псевдонимов IP), находящиеся за интернет-центром, могут взаимодействовать с тремя отдельными глобальными сетями. Дополнительные примеры приведены в конце данной главы.

Рис. 39 Применение NAT с использованием псевдонимов IP



7.1.5 Типы отображения NAT

NAT поддерживает пять типов отображения IP-адресов/портов. Используются следующие типы:

- **One to One (Один-к-одному)**: в режиме один-к-одному интернет-центр отображает один локальный IP-адрес на один глобальный IP-адрес.
- **Many to One (Много-к-одному)**: в режиме много-к-одному интернет-центр отображает несколько локальных IP-адресов на 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).
- **Many to Many Overload (Много-ко-многим с перекрытием)**: в режиме много-ко-многим с перекрытием интернет-центр отображает множество локальных IP-адресов в несколько совместно используемых глобальных IP-адресов.
- **Many-to-Many No Overload (Много-ко-многим без перекрытия)**: в режиме много-ко-многим без перекрытия интернет-центр отображает каждый локальный IP-адрес в уникальный глобальный IP-адрес.
- **Server (Сервер)**: этот режим позволяет определить внутренние серверы для различных служб, находящихся 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. 25 Типы отображения NAT

ТИП	ОТОБРАЖЕНИЕ IP	СОКРАЩЕНИЕ SMT
Один-к-одному	ILA1←→ IGA1	1:1
Много-к-одному (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M:1
Много-ко-многим с перекрытием	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M:M Ov
Много-ко-многим без перекрытия	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M:M No OV
Сервер	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Сервер

7.2 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)**. Интернет-центр, кроме этого, поддерживает **Full Feature (Полный набор функциональных возможностей)** NAT для отображения нескольких глобальных IP-адресов на несколько частных локальных IP-адресов клиентов или серверов с использованием типов отображения, как показано в Табл. 25 на с. 119.

- Выберите **SUA Only (Только SUA)**, если интернет-центр имеет только один общедоступный IP-адрес в глобальной сети.
- Выберите **Full Feature (Полный набор функциональных возможностей)**, если интернет-центр имеет несколько общедоступных IP-адресов в глобальной сети.

7.3 Сервер SUA

Сервер SUA — это список внутренних серверов (расположенных в локальной сети за NAT), например, web или FTP, которые вы можете сделать видимыми для внешних пользователей, несмотря на то, что функция SUA представляет всю вашу внутреннюю сеть для внешних пользователей, как одиночный компьютер.

Вы можете указать для переадресации один номер порта или диапазон номеров портов, а также локальный IP-адрес требуемого сервера. Номер порта идентифицирует службу; например, служба web имеет 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.

7.3.1 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 не назначен IP-адрес для **Server Set 1 (Набор серверов 1)** (сервер по умолчанию), интернет-центр будет сбрасывать все пакеты, принятые для портов, не указанных здесь или в настройках удаленного управления.

7.3.2 Переадресация портов: службы и номера портов

В следующей таблице приведены наиболее часто используемые номера портов. Для дополнительной информации о номерах портов см. RFC 1700.

Табл. 26 Службы и номера портов

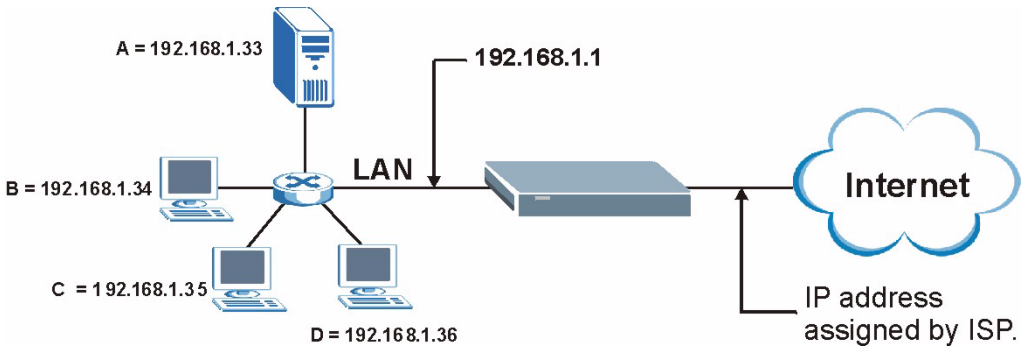
СЛУЖБЫ	НОМЕР ПОРТА
ECHO	7
FTP (File Transfer Protocol — Протокол передачи файлов)	21
SMTP (Simple Mail Transfer Protocol — Простой протокол электронной почты)	25
DNS (Domain Name System — Система доменных имен)	53
Finger (Указатель)	79
HTTP (Hyper Text Transfer Protocol — Протокол передачи гипертекста или WWW — "всемирная паутина")	80
POP3 (Post Office Protocol — Почтовый протокол)	110
NNTP (Network News Transfer Protocol — Сетевой протокол передачи новостей)	119
SNMP (Simple Network Management Protocol — Простой протокол управления сетью).	161
SNMP trap (Прерывание SNMP)	162
PPTP (Point-to-Point Tunneling Protocol — Протокол туннелирования "точка-точка")	1723

7.3.3 Настройка серверов, расположенных за SUA (пример)

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.

IP-адрес назначается Интернет-провайдером.

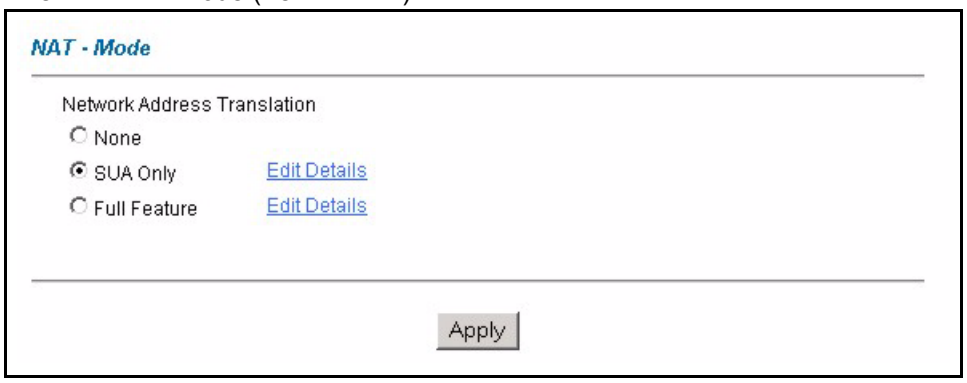
Рис. 40 Пример: несколько серверов расположены за NAT



7.4 Выбор режима NAT

Необходимо создать правило межсетевого экрана в дополнение к созданию SUA/NAT для того, чтобы трафик из глобальной сети пересылался через интернет-центр. Нажмите **NAT** для отображения следующего окна.

Рис. 41 NAT Mode (Режим NAT)



В следующей таблице даны описания полей этого окна.

Табл. 27 NAT Mode (Режим NAT)

ПОЛЕ	ОПИСАНИЕ
None (Отключить)	Выберите эту опцию для отключения NAT.
SUA Only (Только SUA)	Выберите эту опцию, если интернет-центр имеет только один общедоступный IP-адрес в глобальной сети. Интернет-центр будет использовать Набор отображения адресов 1 (Address Mapping Set 1), установленный в окне **NAT — Edit SUA/NAT Server Set (Редактировать набор серверов SUA/NAT)**.
Edit Details (Редактировать параметры)	Щелкните по этой ссылке для перехода к окну **NAT — Edit SUA/NAT Server Set (Редактировать набор серверов SUA/NAT)**.
Full Feature (Полный набор функциональных возможностей)	Выберите эту опцию, если интернет-центр имеет несколько общедоступных IP-адресов в глобальной сети.

Табл. 27 NAT Mode (Режим NAT) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Edit Details (Редактировать параметры)	Щелкните по этой ссылке для перехода к окну **NAT — Address Mapping Rules (Правила отображения адресов)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить конфигурациию.

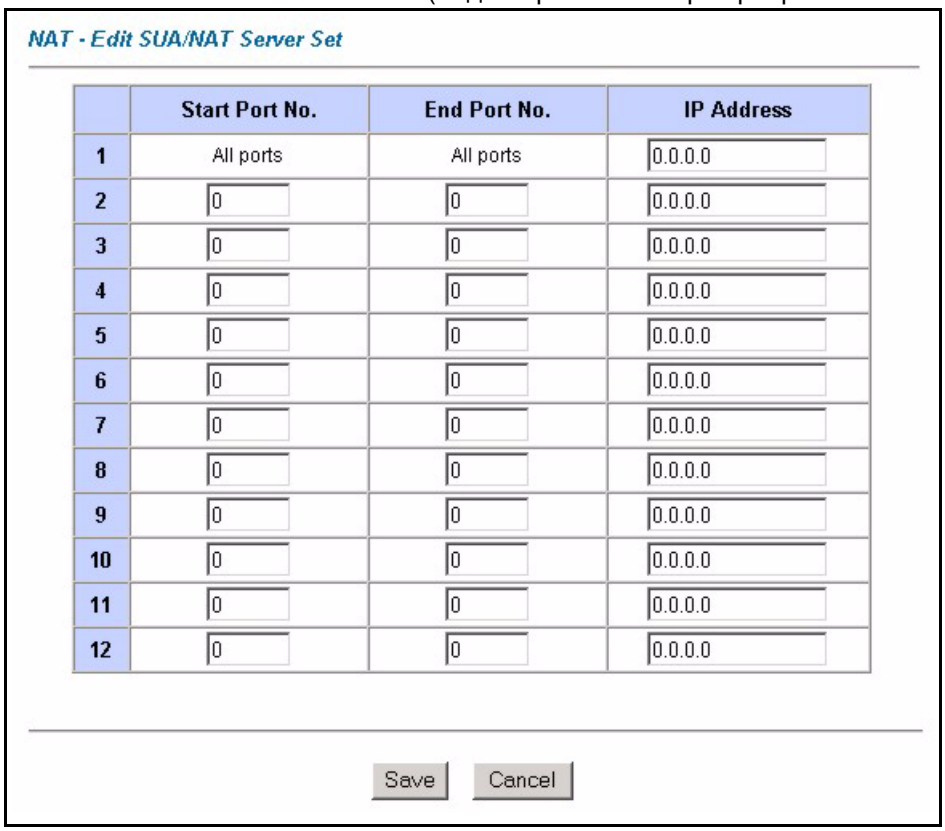
7.5 Настройка серверов SUA

Если не назначен IP-адрес для **Server Set 1 (Набор серверов 1)** (сервер по умолчанию), интернет-центр будет сбрасывать все пакеты, принятые для портов, не указанных здесь или в настройках удаленного управления.

Нажмите **NAT**, выберите **SUA Only (Только SUA)** и затем нажмите **Edit Details (Редактировать параметры)** для отображения следующего окна.

Более подробную информацию см. в Разд. 7.3 на с. 120. См. Табл. 26 на с. 121 для справки по номерам портов, обычно используемых для конкретных служб.

Рис. 42 Edit SUA/NAT Server Set (Редактировать набор серверов SUA/NAT)



В следующей таблице даны описания полей этого окна.

Табл. 28 Редактировать набор серверов SUA/NAT

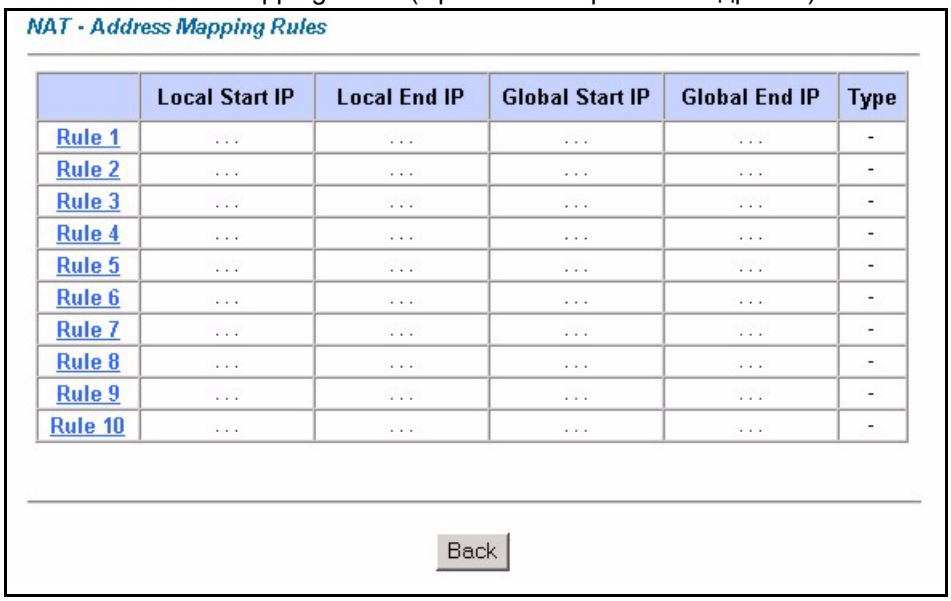
ПОЛЕ	ОПИСАНИЕ
Start Port No. (Номер начального порта диапазона)	Введите в это поле номер порта. Для пересылки пакетов только одного порта введите его номер еще раз в поле **End Port No. (Номер конечного порта диапазона)**. Для пересылки пакетов ряда портов введите здесь номер начального порта, а номер конечного порта в поле **End Port No. (Номер конечного порта диапазона)**.
End Port No. (Номер конечного порта диапазона)	Введите в это поле номер порта. Для пересылки пакетов только одного порта введите его номер в поле **Start Port No. (Номер начального порта диапазона)**, расположенное выше, а затем введите тот же номер еще раз в это поле. Для пересылки пакетов ряда портов введите здесь номер конечного порта в серии портов с начальным номером, указанным в поле **Start Port No. (Номер начального порта диапазона)**.
Server IP Address (IP-адрес сервера)	Введите в этом поле IP-адрес сервера.
Save (Сохранить)	Нажмите кнопку **Save (Сохранить)**, чтобы сохранить конфигурацию интернет-центра.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы вернуться к предыдущей конфигурации.

7.6 Настройка правил отображения адресов

Порядок следования правил имеет большое значение, поскольку интернет-центр применяет правила в указанном порядке. Когда текущий пакет соответствует какому-либо правилу, интернет-центр 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, вы уже настроили правила с 1-го по 6-е в текущем наборе и теперь хотите настроить правило 9. В общем окне набора правил новое правило будет иметь номер 7, но 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 настроек отображения адресов интернет-центра, нажмите **NAT**, выберите **Full Feature (Полный набор функциональных возможностей)** и затем щелкните по ссылке **Edit Details (Редактировать параметры)**, чтобы отобразить следующее окно.

Рис. 43 Address Mapping Rules (Правила отображения адресов)



В следующей таблице даны описания полей этого окна.

Табл. 29 Address Mapping Rules (Правила отображения адресов)

ПОЛЕ	ОПИСАНИЕ
Local Start IP (Начальный локальный IP-адрес)	Это начальный внутренний локальный IP-адрес (начальный ILA). Локальные IP-адреса недоступны (**N/A**)для типа отображения портов **Server (Сервер)**.
Local End IP (Конечный локальный IP-адрес)	Это конечный внутренний локальный IP-адрес (конечный 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 **один-к-одному** и **сервер**.
Global Start IP (Начальный глобальный IP-адрес)	Это начальный внутренний глобальный IP-адрес (начальный IGA). Если вы используете динамический IP-адрес, назначаемый Интернет-провайдером, введите в это поле 0.0.0.0. В этом случае используются только отображения **много-к-одному** и **сервер**.
Global End IP (Конечный глобальный IP-адрес)	Это конечный внутренний глобальный IP-адрес (конечный IGA). В этом поле отображается **N/A (Не применяется)** для типов отображения **один-к-одному**, **много-к-одному** и **сервер**.

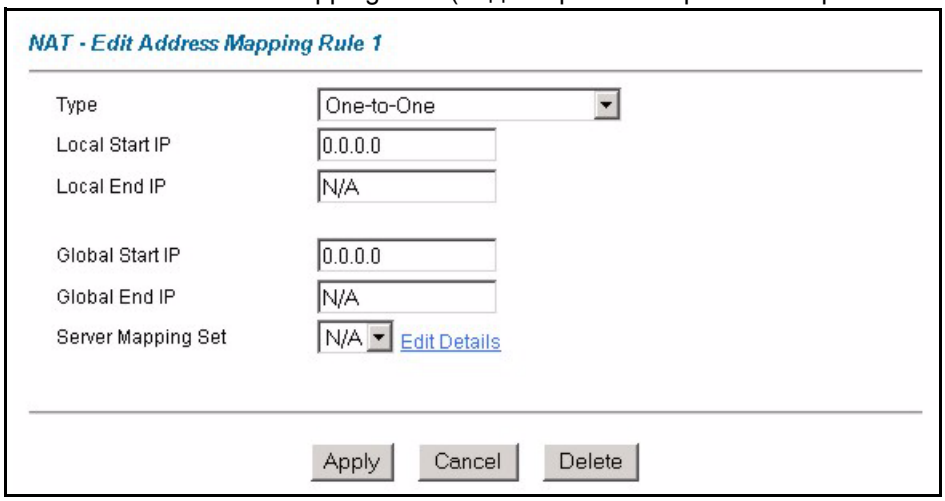
Табл. 29 Address Mapping Rules (Правила отображения адресов) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	**1-1**: в режиме 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 много-к-одному несколько локальных IP-адресов отображаются на один глобальный IP-адрес. Этот режим аналогичен SUA (т.е., 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 много-ко-многим с перекрытием несколько локальных IP-адресов отображаются на несколько совместно используемых глобальных IP-адресов. **MM No** (No Overload): в режиме много-ко-многим без перекрытия каждый локальный IP-адрес отображается на уникальный глобальный IP-адрес. **Server (Сервер)**: этот режим позволяет определить внутренние серверы для различных служб, находящихся за NAT, и сделать их доступными для внешних пользователей.
Back (Назад)	Нажмите кнопку **Back (Назад)** для возврата к окну **NAT Mode (Режим NAT)**.

7.7 Редактирование правил отображения адресов

Для редактирования правила отображения адресов, щелкните по ссылке этого правила в окне **NAT Address Mapping Rules (NAT — Правила отображения адресов)**, чтобы отобразить следующее окно.

Рис. 44 Edit Address Mapping Rule (Редактирование правил отображения адресов)



В следующей таблице даны описания полей этого окна.

Табл. 30 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 режиме 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. • **Many-to-One (Много к одному)**: в режиме много-к-одному несколько локальных IP-адресов отображаются на один глобальный IP-адрес. Этот режим аналогичен SUA (т.е., 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 перекрытием)**: в режиме много-ко-многим с перекрытием несколько локальных IP-адресов отображаются на несколько совместно используемых глобальных IP-адресов. • **Many-to-Many No Overload (Много-ко-многим без перекрытия)**: в режиме много-ко-многим без перекрытия каждый локальный IP-адрес отображается на уникальный глобальный IP-адрес. • **Server (Сервер)**: этот режим позволяет определить внутренние серверы для различных служб, находящихся за NAT, и сделать их доступными для внешних пользователей.
Local Start IP (Начальный локальный IP-адрес)	Это начальный локальный IP-адрес (начальный ILA). Локальные IP-адреса недоступны (**N/A**)для типа отображения портов **Server (Сервер)**.
Local End IP (Конечный локальный IP-адрес)	Это конечный локальный IP-адрес (конечный 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 **один-к-одному** и **сервер**.

Табл. 30 Edit Address Mapping Rule (Редактирование правил отображения адресов)

ПОЛЕ	ОПИСАНИЕ
Global Start IP (Начальный глобальный IP-адрес)	Это начальный глобальный IP-адрес (начальный IGA). Если вы используете динамический IP-адрес, назначаемый Интернет-провайдером, введите в это поле 0.0.0.0.
Global End IP (Конечный глобальный IP-адрес)	Это конечный глобальный IP-адрес (конечный IGA). В этом поле отображается **N/A (Не применяется)** для типов отображения **один-к-одному**, **много-к-одному** и **сервер**.
Server Mapping Set (Набор отображения серверов)	Это поле доступно, только если в поле **Type (Тип)** установлено значение **Server (Сервер)**. Выберите число из раскрывающегося списка для установки набора серверов в окне **NAT — Address Mapping Rules (NAT — Правила отображения адресов)**.
Edit Details (Редактировать параметры)	Щелкните по этой ссылке для перехода к окну **NAT — Edit SUA/NAT Server Set (NAT — Редактировать набор серверов SUA/NAT)**, чтобы изменить набор серверов, который вы выбрали в поле **Server Mapping Set (Набор отображения серверов)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.
Delete (Удалить)	Нажмите кнопку **Delete (Удалить)**, чтобы выйти из этого окна без сохранения настроек.

Глава 8 Настройка динамической системы доменных имен (DYNDNS)

В этой главе описывается настройка интернет-центра для использования динамической DNS (DYNDNS).

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 получить учетную запись динамической 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 Шаблоны DYNDNS

Включение функции шаблонов позволяет соотносить имена вида *.yourhost.dyndns.org с тем же IP-адресом, что и имя 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.

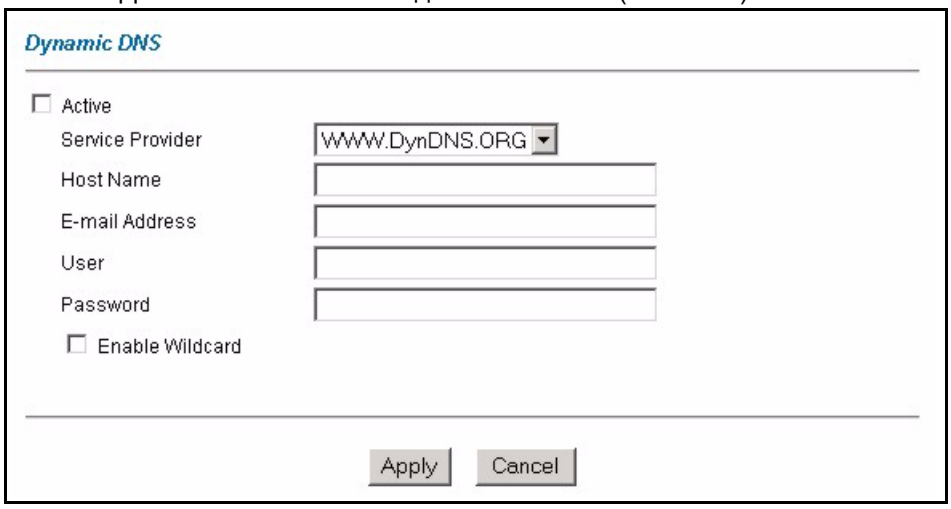
Инструкции по настройке см. в Разд. 8.2 на с. 131.

8.2 Настройка динамической DNS (DYNDNS)

Для изменения настроек DYNDNS интернет-центра, выберите **Dynamic DNS (Динамическая DNS)**. При этом откроется показанное ниже окно.

Более подробную информацию см. в Разд. 8.1 на с. 130.

Рис. 45 Динамическая система доменных имен (DYNDNS)



В следующей таблице даны описания полей этого окна.

Табл. 31 Динамическая система доменных имен (DYNDNS)

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Установите этот флажок для использования динамической службы доменных имен.
Service Provider (Провайдер услуг)	Это имя провайдера услуг динамической DNS.
Host Name (Имя узла)	Введите доменное имя, назначенное интернет-центру провайдером услуг динамической DNS.
E-mail Address (Адрес электронной почты)	Введите адрес электронной почты.
User (Пользователь)	Введите имя пользователя.
Password (Пароль)	Введите назначенный пароль.
Enable Wildcard (Включить шаблоны)	Установите этот флажок для включения шаблонов DYNDNS.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

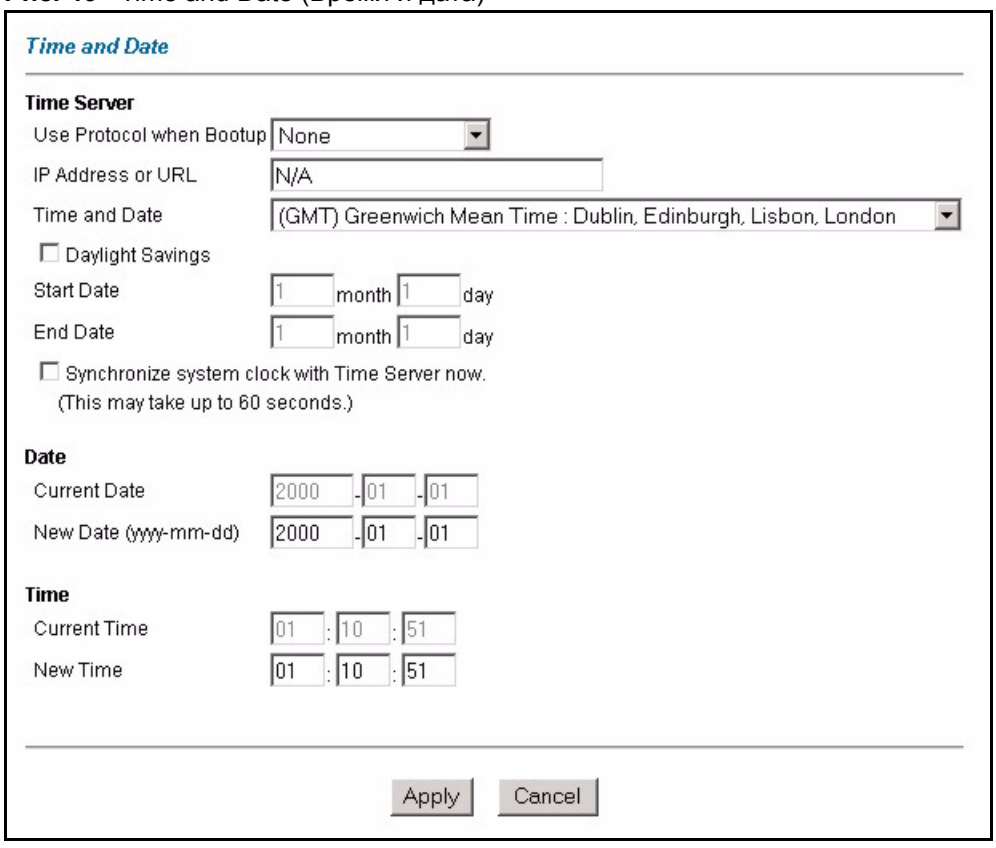
Глава 9
Время и дата

Это окно доступно не во всех моделях. Оно используется для установки времени и даты в интернет-центре.

9.1 Установка времени и даты

Для изменения времени и даты в интернет-центре, нажмите **Time And Date (Время и дата)**. При этом откроется показанное ниже окно. Это окно используется для установки времени в интернет-центре в соответствии с вашим часовым поясом.

Рис. 46 Time and Date (Время и дата)



В следующей таблице даны описания полей этого окна.

Табл. 32 Время и дата

ПОЛЕ	ОПИСАНИЕ
Time Server (Сервер точного времени)	
Use Protocol when Bootup (Использовать протокол при загрузке)	Введите сервисный протокол, с помощью которого ваш сервер времени посылает данные при включении интернет-центра. Не все серверы времени поддерживают любые протоколы, поэтому следует проконсультироваться с Интернет-провайдером/сетевым администратором, или попытаться определить работающий протокол методом проб и ошибок. Основные различия между ними заключаются в формате представления времени. Формат **Daytime (RFC 867)** содержит 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. Формат **NTP (RFC 1305)** аналогичен формату **Time (RFC 868)**. Выберите **None (Нет)** для установки времени и даты вручную.
IP Address or URL (IP-адрес или URL)	Введите IP-адрес или URL сервера времени. Если вы не обладаете этой информацией, следует обратиться к Интернет-провайдеру/сетевому администратору.
Time and Date (Время и дата)	Выберите часовой пояс вашего местонахождения. Это поле устанавливает разницу между вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time — GMT).
Daylight Savings (Переход на летнее время)	Выберите эту опцию, если вы используете 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.
Start Date (Дата начала)	Введите месяц и день, когда начинается летнее время, если выбрана опция **Daylight Savings (Переход на летнее время)**.
End Date (Конечная дата)	Введите месяц и день, когда заканчивается летнее время, если выбрана опция **Daylight Savings (Переход на летнее время)**.
Synchronize system clock with Time Server now (Синхронизировать системные часы с сервером времени).	Выберите эту опцию, чтобы интернет-центр использовал время, полученное от сервера времени (настроенного выше), для настройки своих внутренних системных часов. Подождите примерно 60 секунд, пока интернет-центр обнаружит сервер времени. Если интернет-центр не смог обнаружить сервер времени, проверьте используемый сервисный протокол и IP-адрес сервера времени. Если IP-адрес установлен правильно, протестируйте соединение, например, с помощью команды "ping".
Date (Дата)	
Current Date (Текущая дата)	В этом поле отображается дата в интернет-центре. Каждый раз при загрузке этой страницы, интернет-центр синхронизирует время с сервером времени.
New Date (yyyy-mm-dd) (Новая дата (гггг-мм-дд)	В этом поле отображается последняя обновленная дата от сервера времени. Если в поле **Use Protocol when Bootup (Использовать протокол при загрузке)** установлено **None (Нет)**, введите вручную новую дату в этом поле и затем нажмите **Apply (Применить)**.
Time (Время)	
Current Time (Текущее время)	В этом поле отображается время в интернет-центре. Каждый раз при загрузке этой страницы, интернет-центр синхронизирует время с сервером времени.

Табл. 32 Время и дата (продолжение)

ПОЛЕ	ОПИСАНИЕ
New Time (Новое время)	В этом поле отображается последнее обновленное время от сервера времени. Если в поле **Use Protocol when Bootup (Использовать протокол при загрузке)** установлено **None (Нет)**, введите вручную новое время в этом поле и затем нажмите **Apply (Применить)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

Глава 10
Межсетевые экраны

В этой части дается вводная информация о межсетевых экранах в целом и о межсетевом экране интернет-центра P–660HT/HTW EE.

10.1 Межсетевой экран — общая информация

Первоначально термин *firewall* относился к технологии строительства, разработанной в целях предотвращения распространения огня между помещениями. Сетевой термин “firewall” означает систему или группу систем, определяющих политику управления доступом между двумя сетями. Его также можно определить как механизм защиты надежной (в отношении безопасности) сети от ненадежной. Безусловно, межсетевые экраны не решают все проблемы безопасности. Межсетевой экран (другое его название — брандмауэр) — это лишь *один* из механизмов, предназначенных для создания внешнего периметра защиты сети в рамках политики безопасности сети. Он не должен быть *единственным* применяемым механизмом или способом. Успешная работа межсетевого экрана возможна только как результат правильной его разработки и установки. Это требует включения межсетевого экрана в общую политику защиты информации. Кроме того, необходимо внедрить определенные политики в рамках собственно межсетевой защиты.

Настройки межсетевого экрана по умолчанию — см. Разд. 11.5 на с. 156.

Просмотр правил межсетевых экранов — см. Разд. 11.6 на с. 157.

Настройка правил межсетевых экранов — см. Разд. 11.6.1 на с. 159.

Настройка пользовательских служб — см. Разд. 11.7 на с. 162.

Настройка порогов межсетевых экранов — см. Разд. 11.12.3 на с. 174.

10.2 Типы межсетевых экранов

Существует три основных вида межсетевых экранов:

- Межсетевые экраны с фильтрацией пакетов
- Межсетевые экраны на уровне приложений
- Межсетевые экраны с инспекцией пакетов с учетом состояния

10.2.1 Межсетевые экраны с фильтрацией пакетов

Межсетевой экран с фильтрацией пакетов ограничивает доступ в зависимости от сетевого адреса источника/получателя пакета и типа приложения.

10.2.2 Межсетевые экраны на уровне приложений

Межсетевые экраны на уровне приложений ограничивают доступ, выступая в качестве прокси-серверов для внешних серверов. В связи с тем, что они используют программы, написанные для конкретных служб Интернет, таких как HTTP, FTP и telnet, они могут инспектировать пакеты на предмет достоверности относящихся к приложению данных. У шлюзов приложений имеется ряд преимуществ общего характера по сравнению с режимом (по умолчанию) разрешения передачи трафика приложений непосредственно к внутренним узлам:

Функция намеренного скрытия информации не позволяет внешним системам получить имена внутренних узлов через DNS, так как шлюз приложения — это единственный узел, имя которого должно быть известно внешним системам.

Надежная система аутентификации и протоколирования предварительно аутентифицирует трафик приложения до того, как он достигает внутренних узлов и обеспечивает более эффективное ведение протокола по сравнению с регистрацией обычными средствами узла. Правила фильтрации в маршрутизаторе с фильтрацией пакетов могут быть проще, чем в случае фильтрации маршрутизатором трафика приложений и пересылки его нескольким конкретным системам. Задача маршрутизатора в данном случае состоит лишь в том, чтобы переназначать трафик приложений шлюзу приложений и запретить весь остальной.

10.2.3 Межсетевые экраны с инспекцией пакетов с учетом состояния

Межсетевые экраны с инспекцией пакетов с учетом состояния ограничивают доступ путем отбраковки пакетов, не удовлетворяющих установленным правилам доступа. Решения о доступе принимаются в зависимости от IP-адреса и протокола. Такие межсетевые экраны также "инспектируют" данные сеансов связи для обеспечения целостности соединения и адаптации к динамическим протоколам. Как правило, такие экраны обеспечивают лучшую скорость и прозрачность, однако проигрывают в таких аспектах как управление доступом на уровне приложений и кэширование, которые поддерживаются некоторыми прокси. Для получения более подробной информации об инспекции пакетов с учетом состояния см. Разд. 10.5 на с. 144.

Межсетевые экраны того или иного типа сегодня являются неотъемлемой частью стандартных решений систем безопасности для предприятий.

10.3 Знакомство с межсетевым экраном ZyXEL

Межсетевой экран интернет-центра P–660HT/HTW EE представляет собой межсетевой экран с функцией инспекции пакетов с учетом состояния, предназначенный, при его активации (в меню SMT 21.2 или в Web-конфигураторе), для защиты от атак типа "Отказ в обслуживании" (DoS). Задача интернет-центра — обеспечить безопасное подключение частной локальной вычислительной сети (LAN) к Интернет. Интернет-центр может предотвращать хищение, уничтожение и изменение данных, а также регистрировать события, которые могут иметь важное значение для безопасности сети. Интернет-центр P–660HT/HTW EE имеет также возможности фильтрации пакетов.

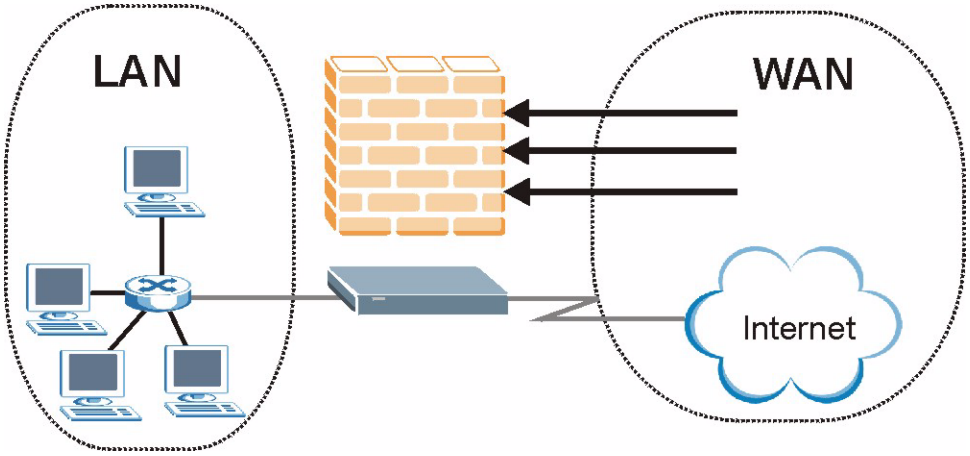
Интернет-центр устанавливается между LAN и Интернетом. Это позволяет ему выступать в качестве безопасного шлюза для данных, пересылаемых из локальной сети в Интернет и наоборот.

Интернет-центр P–660HT/HTW EE имеет один порт DSL/ISDN и несколько портов LAN Ethernet. DSL-порт и LAN-порты физически разделяют сеть на две области.

- Порт DSL/ISDN подключается к Интернету.
- Порт локальной сети подключается к компьютерной сети, для которой необходимо обеспечить защиту от внешнего мира. Компьютеры сети будут иметь доступ к Интернет-службам, таким как электронная почта, FTP, и WWW. Однако, “входящий доступ” не будет разрешен, если не настроено удаленное управление или не создано правило межсетевого экрана, позволяющее удаленному узлу использовать конкретную службу.

10.3.1 Атаки типа "Отказ в обслуживании" (DoS)

Рис. 47 Применение межсетевого экрана интернет-центра P–660HT/HTW EE



10.4 Отказ в обслуживании (DoS)

Атаки типа "Отказ в обслуживании" (DoS) нацелены на устройства и сети, подключенные к Интернету. Эти атаки нацелены не на несанкционированное получение информации, а имеют своей целью вывести из строя какое-либо устройство или сеть, таким образом лишая пользователя дальнейшего доступа к ресурсам сети. Интернет-центр P–660HT/HTW EE изначально настроен на автоматическое обнаружение и предотвращение всех известных атак DoS.

10.4.1 Основные сведения

Компьютеры обмениваются информацией через Интернет, используя общий "универсальный язык" под названием TCP/IP. TCP/IP, в свою очередь, представляет собой набор протоколов уровня приложений, выполняющих определенные функции. “Добавочный номер”, называемый "порт TCP" или "порт UDP" идентифицирует эти протоколы, а именно HTTP (Web), FTP (File Transfer Protocol/Протокол передачи файлов), POP3 (E-mail) и т. д. Например, Web-трафик по умолчанию использует порт 80 TCP.

При взаимодействии компьютеров в Интернете используется модель клиент-сервер, при которой сервер "прослушивает" через конкретный порт TCP/UDP запросы на информацию, поступающие от удаленных клиентских компьютеров сети. Например, web-сервер обычно "слушает" через порт 80. Следует отметить, что на данном компьютере может быть задействован не единственный порт (например, порт 80 для web), но и остальные тоже будут активны. При недостаточной осторожности лица, осуществляющего настройку и управление данным компьютером, компьютер может подвергнуться атаке хакера через незащищенный порт.

Некоторые наиболее общепринятые порты IP:

Табл. 33 Общепринятые порты IP

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

10.4.2 Типы атак DoS

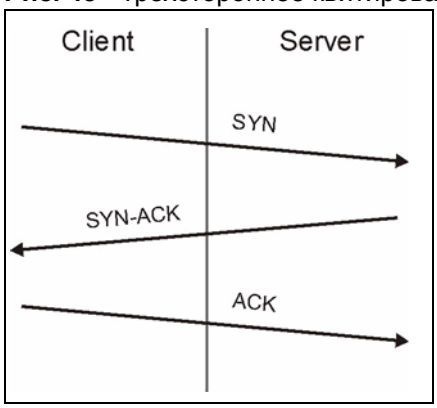
Существуют четыре категории атак типа DoS:

1. Атаки, использующие недостатки реализации TCP/IP.
2. Атаки, использующие слабые места спецификации TCP/IP.
3. Атаки грубой силой, наполняющие сеть бесполезными данными.
4. Подстановка IP-адреса (IP Spoofing)
5. Атаки "**Ping of Death**" и "**Teardrop**" используют недостатки реализации TCP/IP на различных компьютернах и узлах.

- Атака "Ping of Death" использует утилиту эхо-тестирования ("ping") для создания IP-пакета, превышающего максимальный размер в 65,536 байт, разрешенный спецификацией IP. Пакет большого размера посылается в систему, что вызывает ее отказ, повисание или перезагрузку.
- Атака "Teardrop" использует слабости в перекомпоновке фрагментов пакета IP. При передаче данных в сети IP-пакеты разбиваются на более мелкие фрагменты. Каждый фрагмент выглядит как первоначальный пакет IP, но содержит поле смещения, несущее информацию, например, о том, что "Данный фрагмент несет байты с 200 по 400 первоначального (нефрагментированного) пакета IP." Программа Teardrop создает серию IP-фрагментов с перекрывающимися полями смещения. Когда при достижении адресата пакет восстанавливается из фрагментов, это может привести к остановке, зависанию и перезагрузке системы.

6. Слабости в спецификации TCP/IP оставляют ее открытой для атак "**SYN Flood**" и "**LAND**". Эти атаки происходят во время квитирования, инициирующего сеанс связи между двумя приложениями.

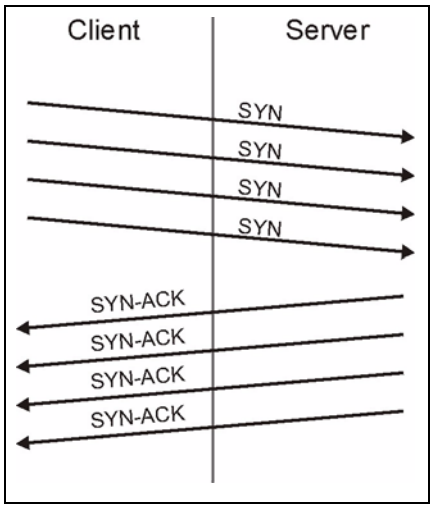
Рис. 48 Трехстороннее квитирование



В обычных обстоятельствах приложение, инициирующее сеанс связи, посылает пакет SYN (синхронизации) серверу-получателю. Получатель отправляет назад пакет ACK (подтверждения) и собственный SYN, на который инициатор отвечает ACK (подтверждением). После такого подтверждения связи устанавливается соединение.

- **Атака SYN** "переполняет" систему-получатель SYN-пакетами. Каждый пакет побуждает атакуемую систему выдавать ответ SYN-ACK. Пока система ожидает получения ACK в ответ на SYN-ACK, все остальные запросы SYN-ACK становятся в очередь (backlog queue). Запросы SYN-ACK удаляются из очереди только после получения ответного ACK или в случае прекращения трехстороннего обмена по истечении определенного времени ожидания (относительно долгого). Переполнение очереди приводит к тому, что система игнорирует очередные поступающие запросы SYN, и становится недоступной для легальных пользователей.

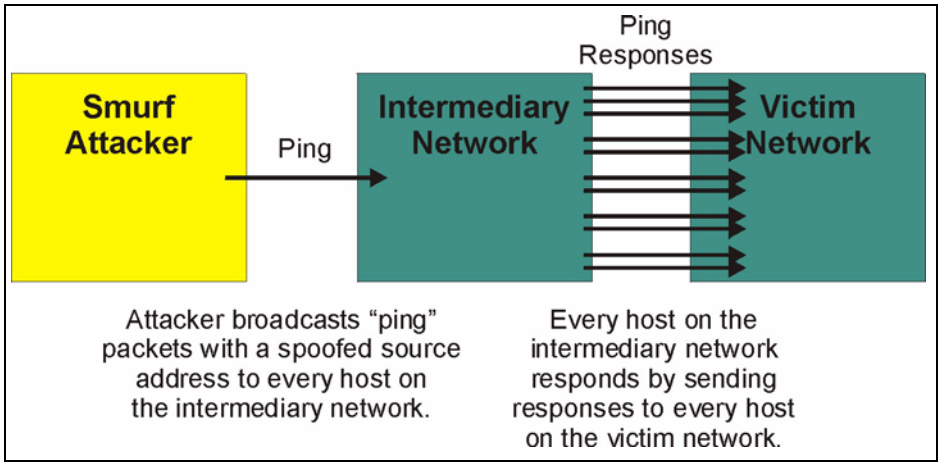
Рис. 49 SYN Flood



- Используя **атаку "LAND"**, хакер переполняет сеть SYN-пакетами с ложным IP-адресом источника, равным IP-адресу атакуемой системы. В результате компьютер-узел посылает пакеты сам себе, и система становится недоступной, пытаясь отвечать на запросы самой себе.

7 Атака **"грубой силой"**, например "Smurf", использует особенность спецификации IP, известную как направленная рассылка или циркулярная рассылка для подсети, для того, чтобы переполнить атакуемую сеть бесполезными данными. Хакер, использующий этот вид атаки, переполняет маршрутизатор пакетами — эхо-запросами протокола ICMP (протокол управляющих сообщений в сети Интернет). Так как IP-адрес получателя каждого пакета является широковещательным адресом сети, маршрутизатор рассылает такой пакет ICMP всем узлам сети. Если узлов много, это приводит к большому объему трафика состоящего из запросов и ответов ICMP. Если хакер решает подменить IP-адрес источника эхо-запроса ICMP, то в результате трафик ICMP не только переполнит сеть-"посредник", но и перегрузит сеть подмененного IP-адреса, именуемую сетью-"жертвой". Такое переполнение широковещательным трафиком использует весь имеющийся ресурс пропускной способности, делая связь с системой недоступной.

Рис. 50 Атака Smurf



10.4.2.1 Уязвимость ICMP

ICMP является протоколом с оповещением об ошибках, работающим совместно с IP. Следующие типы ICMP выдают предупреждение:

Табл. 34 Команды ICMP, выдающие предупреждение

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

10.4.2.2 Недопустимые команды (NetBIOS и SMTP)

Единственно допустимыми командами NetBIOS являются приведенные ниже, все остальные — недопустимы.

Табл. 35 Команды NetBIOS

MESSAGE:
REQUEST:
POSITIVE:
VE:
RETARGET:
KEEPALIVE:

За исключением приведенных в следующей таблице, все другие команды SMTP запрещены.

Табл. 36 Команды SMTP

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

10.4.2.3 Traceroute

Traceroute — это утилита, предназначенная для определения маршрута, проходимого пакетом между двумя конечными точками. Иногда при некорректной установке межсетевого экрана у хакера появляется возможность проследить его путь и получить данные о топологии сети, находящейся за экраном.

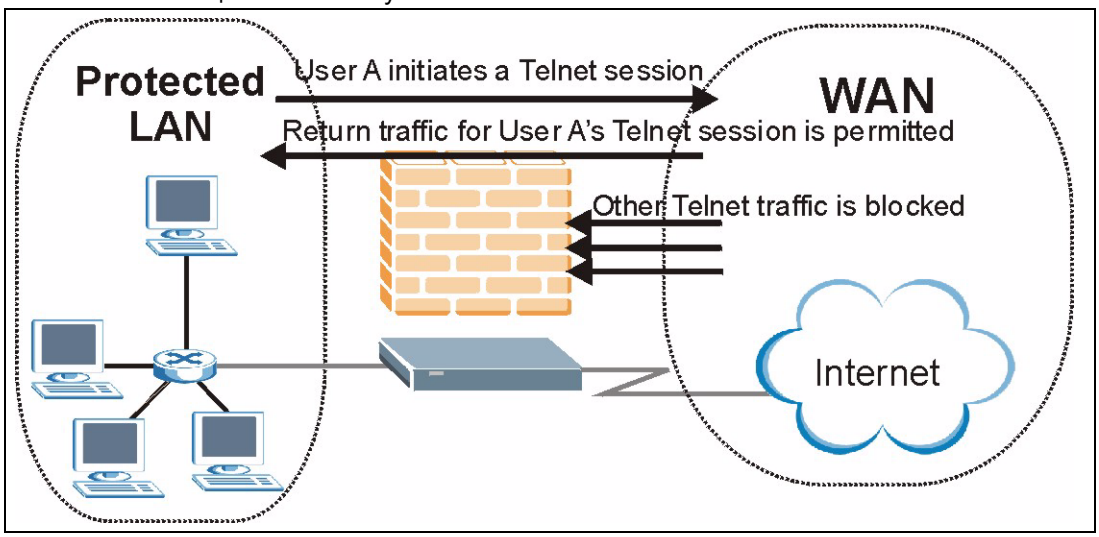
Часто, многие атаки DoS также применяют, как часть своей атаки метод, известный как "**IP Spoofing**" (подстановка IP-адреса). Подстановка IP-адреса может использоваться с целью проникновения в системы, чтобы исключить возможность идентифицировать хакера или увеличить эффект атаки DoS. "IP Spoofing" применяется для получения несанкционированного доступа к компьютерам путем создания ситуации, когда межсетевой экран или маршрутизатор получают информацию о том, что обмен данными происходит якобы с надежной (в отношении безопасности) сетью. При использовании данного способа хакер должен видоизменить заголовки пакетов так, чтобы складывалось впечатление, что пакеты поступают с надежного (доверенного) узла и должны беспрепятственно пропускаться сетевым экраном или маршрутизатором. Интернет-центр P–660HT/HTW EE блокирует все попытки получения доступа обманным путем с использованием ложного IP-адреса.

10.5 Инспекция пакетов с учетом состояния

Инспекция с учетом состояния означает, что поля пакетов сравниваются с теми пакетами, которые уже считаются достоверными. Например, при доступе к внешнему серверу прокси-сервер запоминает параметры первоначального запроса, такие как номер порта и адрес источника и получателя. Такое "запоминание" называется *сохранением состояния*. Когда внешняя система отвечает на запрос, межсетевой экран сравнивает параметры получаемых пакетов с параметрами сохраненного состояния и принимает решение о допуске. Интернет-центр P–660HT/HTW EE использует инспекцию пакетов с учетом состояния для защиты частной LAN от хакеров и вандалов в Интернете. Установленная по умолчанию, функция инспекции пакетов с учетом состояния пропускает все данные, идущие в Интернет из LAN, и блокирует весь трафик в LAN, исходящий из Интернета. В целом, функция инспекции пакетов с учетом состояния:

- Разрешает все сеансы связи с глобальной сетью (Интернет, WAN) со стороны локальной (LAN).
- Запрещает сеансы связи с локальной сетью со стороны глобальной.

Рис. 51 Инспекция пакетов с учетом состояния



Данная схема демонстрирует установленные по умолчанию правила межсетевого экрана интернет-центра P–660HT/HTW EE в действии, а также показывает, как работает инспекция пакетов с учетом состояния. Пользователь A может инициировать Telnet-соединение из локальной сети, и ответы на его запросы разрешаются. Однако всякий иной трафик Telnet, поступающий из глобальной сети, блокируется.

10.5.1 Действие функции инспекции пакетов с учетом состояния

В данном примере иллюстрируется последовательность событий, имеющих место после того, как пакет TCP покидает локальную сеть через порт WAN межсетевого экрана. Этот пакет TCP является первым в сеансе, а протокол уровня приложений данного пакета настроен на проверку на соответствие одному из правил сетевого экрана:

1. Пакет поступает из локальной сети (где находится сетевой экран) в глобальную сеть.
2. Происходит проверка пакета по существующему списку контроля исходящего доступа для данного порта и дается разрешение (недопущенный пакет сбрасывается уже на данном этапе).
3. Происходит инспекция пакета в соответствии с правилом сетевого экрана для выявления и записи информации о состоянии подключения для данного пакета. Эта информация записывается в виде нового элемента таблицы состояний, созданной для данного подключения. Если для данного пакета нет соответствующего правила межсетевого экрана и он не является атакой, то действия в отношении этого пакета будут определяться настройками в окне **Правило по умолчанию**.
4. В зависимости от полученной информации о состоянии, правило межсетевого экрана создает временную запись в списке контроля доступа, которая вставляется в начало расширенного списка контроля входящего доступа для порта WAN. Эта временная запись в списке контроля доступа предназначена для разрешения пропуска входящих пакетов с того же соединения, что и уже проинспектированные исходящие пакеты.
5. Исходящий пакет пересылается через данный порт.
6. Далее, входящий пакет достигает порта. Этот пакет является частью соединения уже установленного исходящим пакетом. Происходит сверка входящего пакета со списком контроля входящего доступа и дается разрешение, так как ранее была добавлена временная запись в список контроля доступа.
7. Пакет проверяется на соответствие правилом межсетевого экрана, а таблица состояний для данного соединения по необходимости обновляется. На основании обновленной информации о состоянии временные записи расширенного списка контроля входящего доступа могут быть изменены, чтобы разрешать только пропуск пакетов, действительных для текущего состояния данного соединения.
8. Проверяются дополнительные входящие или исходящие пакеты для данного соединения, таким образом обновляется таблица состояний и, соответственно, временные записи в списке контроля исходящего доступа; пакеты пересылаются через порт.
9. При прекращении связи или истечении времени ожидания, таблица состояний для данного соединения и временные записи в списке контроля доступа удаляются.

10.5.2 Реализация функции в модели P–660HT/HTW EE

Дополнительные правила могут расширять или замещать установленные по умолчанию. Например, можно создать правило, которое будет выполнять следующее:

- Блокировать трафик определенного типа, например IRC (Internet Relay Chat), исходящий из локальной сети в Интернет.
- Разрешить трафик определенного типа из Интернета к конкретным компьютерам-узлам локальной сети.
- Разрешить доступ к web-серверу всем, кроме конкурентов.
- Разрешить использование определенных протоколов, например Telnet, лишь полномочным пользователям локальной сети.

Эти определяемые пользователями правила работают, используя принцип проверки IP-адреса источника и IP-адреса получателя сетевого трафика, типа протокола IP, и сравнения с правилами, установленными администратором.

ПРИМЕЧАНИЕ: Возможность устанавливать правила межсетевого экрана является очень мощным инструментом. С помощью этих правил можно отключить межсетевой экран или полностью заблокировать доступ в Интернет. Создание и удаление правил межсетевого экрана требует большой осторожности. После создания новых правил необходимо проверить их на правильность работы.

Ниже дается краткое техническое описание отслеживания таких соединений. Соединения могут определяться или протоколами верхнего уровня (например, TCP) или самим интернет-центром (как и в случае "виртуальных соединений", создаваемых для UDP и ICMP).

10.5.3 Безопасность TCP

Интернет-центр P–660HT/HTW EE использует информацию о состоянии, встроенную в пакеты TCP. В первом пакете нового соединения флаг SYN установлен, а флаг ACK снят; это — "пакеты-инициаторы". Пакеты, не содержащие таких флажков, называются "последующими", так как несут данные, возникающие затем в потоке TCP.

Если пакет-инициатор исходит из глобальной сети, это значит, что кто-то в Интернете пытается установить соединение с локальной сетью. За исключением особых случаев (см. далее "протоколы верхнего уровня"), такие пакеты сбрасываются и вносятся в журнал.

Если пакет-инициатор исходит из локальной сети, это означает, что кто-то из локальной сети пытается установить соединение с Интернет. Полагая, что это допустимо в рамках политики безопасности (а именно такова политика по умолчанию), соединение будет разрешено. В кэш будет помещена информация о соединении, т. е. IP-адреса, порты TCP, порядковые номера и т. д.

Если интернет-центр получает последующий пакет (из Интернета или из LAN), то информация о подключении извлекается и проверяется по кэшу. Прохождение пакета разрешается только если он соответствует данному соединению (то есть, если он является ответом на запрос соединения из локальной сети).

10.5.4 Безопасность UDP/ICMP

Пакеты UDP и ICMP не содержат информации о соединении (такой как порядковые номера). Однако они как минимум содержат пару IP-адресов (источника и получателя). UDP также содержит данные обоих портов, а ICMP — тип и код. Все эти данные анализируются для построения "виртуальных соединений" в кэше.

Например, пакет UDP, исходящий из локальной сети, создает запись в кэше. Записываются его IP-адрес и оба порта. На короткое время пакеты UDP из глобальной сети с совпадающими IP и UDP посылаются обратно через сетевой экран.

Подобная ситуация справедлива и для ICMP, за исключением того, что для них интернет-центр вводит больше ограничений. В частности, лишь в ответ на исходящие эхо-запросы разрешены входящие эхо-отклики, на исходящий запрос маски подсети — входящий ответ, а входящий ответ временной метки разрешен только на исходящий запрос. Межсетевой экран не пропускает никакие другие пакеты ICMP, так как они представляют собой большую опасность и содержат слишком мало информации о маршруте. Например, прием ICMP-пакетов переадресации запрещен, так как с их помощью можно перенаправить трафик через атакующие компьютеры.

10.5.5 Протоколы верхнего уровня

Некоторые протоколы верхнего уровня (такие как FTP и RealAudio) используют несколько сетевых соединений одновременно. Говоря простыми словами, они обычно используют "управляющее соединение" для посылки команд между оконечными точками, и "соединения передачи данных", используемые для передачи больших объемов информации.

Рассмотрим протокол FTP. Пользователь в локальной сети устанавливает управляющее соединение с сервером в Интернете и запрашивает файл. В ответ на него удаленный сервер создаст соединение для передачи данных из Интернета. Для нормальной работы FTP это соединение должно получить разрешение доступа, даже если обычно такие подключения из Интернета запрещены.

Для этого интернет-центр контролирует данные FTP уровня приложений. В частности, ищет выходную команду "PORT", и если таковая имеется, добавляет в кэш запись об ожидаемом соединении для передачи данных. Эта операция безопасна, поскольку команда PORT содержит адрес и порт, по которым идентифицируется соединение.

Любой протокол, работающий таким образом, необходимо поддерживать по принципу case-by-case. Для этого можно использовать функцию Custom Ports (пользовательские порты) Web-конфигуратора.

10.6 Методы усиления безопасности при помощи межсетевого экрана

- Измените пароль по умолчанию при помощи SMT или Web-конфигуратора.
- Ограничьте круг лиц, имеющих право telnet-подключения к маршрутизатору.
- Не подключайте неиспользуемые локальные службы (SNMP или NTP). Любое такое лишнее подключение может представлять потенциальную угрозу безопасности. Находчивый хакер может отыскать оригинальные способы злоупотребления подключенными службами для получения доступа к межсетевому экрану или сети.
- Подключенные локальные серверы необходимо обезопасить. Защита обеспечивается путем ограничения взаимодействия до конкретных клиентских устройств и назначения правил блокировки пакетов, поступающих через конкретный порт.
- Активированный межсетевой экран обеспечит защиту от подмены IP-адресов.
- Само устройство межсетевого экрана должно находиться в недоступном (закрытом) помещении.

10.6.1 Общая безопасность

Предусмотреть все возможные случаи невозможно. Многие факторы, контроль над которыми выходит за пределы возможностей межсетевого экрана, фильтрации или трансляции сетевых адресов, могут создать бреши в системе защиты. Ниже приводятся некоторые общие рекомендации, выполнение которых позволит свести риск к минимуму.

- Организация/компания должна разработать комплексный план по защите. Качественное сетевое администрирование предполагает учет возможностей хакеров и предвидение атак. Лучшей защитой от хакеров и взломщиков является информированность. Все сотрудники компании должны быть осведомлены о том, как важна безопасность и как минимизировать риск. Рекомендуется составить перечни, подобные этому.
- Подключения с помощью DSL или кабельного модема являются соединениями типа “always-on” ("всегда включено") и особенно уязвимы, так как предоставляют хакерам возможность взлома системы. Компьютеры, не используемые в данный момент, необходимо выключать.
- Никогда не сообщайте пароль или другие секретные данные, отвечая на телефонные звонки или сообщения по электронной почте от неизвестных лиц.
- Никогда не отправляйте секретные сведения, такие как пароли, данные о кредитных картах и т. д. в незашифрованном виде.
- Не публикуйте секретные данные на веб-страницах, если веб-сайт не использует безопасные подключения. Безопасное подключение можно идентифицировать по иконке в виде ключа в нижней панели браузера (Internet Explorer версии 3.02 и выше или Netscape версии 3.0 и выше). Если веб-сайт использует безопасное подключение, предоставление информации безопасно. Безопасные веб-транзакции довольно сложно взламывать.

- Не сообщайте IP-адрес и прочие системные данные о сети людям, не имеющим отношения к вашей организации. Обращайте внимание на файлы, присылаемые по электронной почте неизвестными отправителями. Общеизвестный способ получения вируса BackOrifice — получение его в составе другого файла в качестве "троянского коня".
- Время от времени меняйте пароли. Используйте пароли, которые невозможно угадать. Наиболее трудно взламывать пароли, содержащие буквы нижнего и верхнего регистров, числа и символы типа % или # одновременно.
- Регулярно обновляйте программное обеспечение. Многие старые версии программ, особенно Web-браузеры, имеют недостатки в системе защиты. Последние версии программ, как правило, содержат самые последние обновления и исправления.
- При участии в “chat rooms” (чатах) или сеансах IRC необходимо тщательно следить за информацией, сообщаемой незнакомым людям.
- При подозрительном поведении системы необходимо обратиться к своему Интернет-провайдеру. Некоторые хакеры используют средства, заставляющие систему со временем становиться все менее устойчивой или прекращать нормальное функционирование.
- Уничтожайте документы, содержащие конфиденциальную информацию, особенно о компьютере, перед тем как их выбросить. Некоторые хакеры могут получить нужную им информацию, исследуя выбрасываемые организацией или отдельными людьми ненужные документы.

10.7 Сравнение функций фильтрации пакетов и межсетевого экрана

Ниже представлено сравнение функций фильтрации и функций межсетевого экрана интернет-центра.

10.7.1 Фильтрация пакетов

- Маршрутизатор производит фильтрацию пакетов во время их прохождения через порт маршрутизатора в соответствии с назначенными правилами фильтрации.
- Фильтрация пакетов является мощным инструментом, однако, могут возникнуть сложности с ее настройкой и управлением, особенно если нужно задать цепочку правил для фильтрации какой-либо службы.
- Фильтрация пакетов проверяет лишь заголовки пакетов IP.

10.7.1.1 Случаи использования фильтрации

- Для блокировки/допуска пакетов LAN по их MAC-адресам.
- Для блокировки/допуска пакетов с особым IP, не являющихся пакетами TCP, UDP, или ICMP.

- Для блокировки/допуска как входящего (из WAN в LAN), так и исходящего (из LAN в WAN) трафика между конкретным внутренним узлом/сетью "A" и внешним узлом/сетью "B". Если фильтр блокирует трафик из A в B, то также блокируется и трафик из B в A. Фильтры не могут различать трафик, исходящий от внутреннего или внешнего узла по IP-адресу.
- Для блокировки/допуска отслеживания маршрута по сети IP.

10.7.2 Межсетевой экран

- Межсетевой экран проверяет содержание пакетов и адреса их источника и получателя. Экраны такого типа используют модуль контроля, подходящий ко всем протоколам, и распознающий данные пакета разных уровней, от сетевого уровня (заголовки IP) до уровня приложений.
- Межсетевой экран выполняет инспекцию пакетов с учетом состояния. Он учитывает состояние обрабатываемых подключений, например, легальный входящий пакет можно сопоставить с исходящим запросом на этот пакет и разрешить его получение. Напротив, входящий пакет, маскирующийся под ответ на несуществующий исходящий запрос, блокируется.
- Межсетевой экран применяет фильтрацию сеансов связи, т. е. использует сложные правила, расширяющие процесс фильтрации с проверки отдельных пакетов в рамках сеанса связи до контроля сеанса связи в целом.
- Межсетевой экран имеет службу электронной почты, с помощью которой отсылаются отчеты и извещения.

10.7.2.1 Случаи использования межсетевого экрана

- Для защиты от атак типа DoS и предотвращения проникновения в сеть хакеров.
- Возможность в рамках одного правила задать ряд IP-адресов источника и получателя, а также номера портов делает использование экрана более предпочтительным в случаях, когда необходимы сложные правила.
- Для выборочной блокировки/допуска входящего и исходящего трафика между внутренними и внешними узлами/сетями. Напомним, что фильтры не в состоянии отличать трафик, исходящий от внутреннего или внешнего узла, по IP-адресу.
- Межсетевой экран предпочтительнее, чем фильтрация, если необходима проверка на соответствие нескольким правилам.
- Лучше использовать межсетевой экран, если есть необходимость получать плановые отчеты о системе или сообщения об атаках по электронной почте.
- Межсетевой экран позволяет блокировать трафик от конкретного URL при появении такового. Указатели URL сохраняются в базе данных списка контроля доступа.

Глава 11
Настройка межсетевого экрана

В этой главе описывается включение и настройка межсетевого экрана интернет-центра P–660HT/HTW EE.

11.1 Способы настройки

Web-конфигуратор, несомненно, является наиболее полным средством настройки межсетевого экрана интернет-центра P–660HT/HTW EE. Поэтому рекомендуется настраивать межсетевой экран с помощью web-конфигуратора. Активировать межсетевой экран можно с помощью экранов SMT. Команды CLI дают ограниченный выбор настроек и рекомендованы только для опытных пользователей.

11.2 Обзор правил межсетевого экрана

Правила межсетевого экрана группируются по направлениям движения пакетов, к которым они применяются.

- Соединение одной ЛВС с другой (LAN–LAN) или с маршрутизатором
- LAN to WAN (ЛВС — глобальная сеть)
- WAN to LAN (глобальная сеть — ЛВС)
- Соединение одной глобальной сети с другой (WAN–WAN) или с маршрутизатором

ПРИМЕЧАНИЕ: Локальная сеть включает в себя как порт LAN, так и порт WLAN.

По умолчанию выполняемая интернет-центром инспекция пакетов с учетом состояния пропускает пакеты в следующих направлениях:

- Соединение одной ЛВС с другой (LAN–LAN) или с маршрутизатором

  Это позволяет компьютерам в локальной сети управлять интернет-центром и обмениваться данными с сетями и подсетями, подключенными к порту локальной сети.
- LAN to WAN (ЛВС — глобальная сеть)

По умолчанию выполняемая интернет-центром инспекция пакетов с учетом состояния блокирует пакеты в следующих направлениях:

- WAN to LAN (глобальная сеть — ЛВС)
- Соединение одной глобальной сети с другой (WAN–WAN) или с маршрутизатором

Это не дает компьютерам из глобальной сети (WAN) использовать интернет-центр в качестве шлюза для обмена данными с другими компьютерами в WAN и/или управлять устройством.

Можно определить дополнительные правила и установить или модифицировать существующие, но соблюдайте при этом крайнюю осторожность.

ПРИМЕЧАНИЕ: Вы можете неумышленно подвергнуть межсетевой экран и защищенную сеть риску, если попытаетесь настроить правила, не имея четкого представления о том, как они работают. После настройки правила необходимо протестировать.

Например, можно назначить следующие правила:

- Блокировать трафик определенного типа, например IRC (Internet Relay Chat), исходящий из локальной сети в Интернет.
- Разрешить трафик определенного типа (например, синхронизация записей баз данных), поступающий от конкретных узлов в Интернете на конкретные серверы локальной сети.
- Разрешить доступ к web-серверу всем, кроме конкурентов.
- Разрешить использование определенных протоколов, например Telnet, лишь полномочным пользователям локальной сети.

Эти определяемые пользователем правила работают на основе принципа проверки IP-адреса источника, IP-адреса получателя сетевого трафика и типа протокола IP на соответствие правилам, установленным администратором. Правила, установленные пользователем, имеют очередность и могут иметь приоритет над установленными по умолчанию правилами.

11.3 Обзор логики правил

ПРИМЕЧАНИЕ: Прежде чем назначать правила необходимо тщательно изучить данные указания.

11.3.1 Список вопросов для составления правил

Сформулировать смысл данного правила. Например:“ограничить доступ IRC из локальной сети в сеть Интернет”. Или: “позволить удаленному серверу Lotus Notes синхронизацию с внутренним сервером Notes через Интернет.”

1. Правило должно пересылать или блокировать трафик?
2. К какому направлению трафика применяется правило?
3. Какие службы IP попадут под действие правила?
4. На каких компьютерах локальной сети отразится выполнение этого правила?

5 На каких компьютерах в Интернете отразится выполнение этого правила? Эти сведения должны быть по возможности конкретны. Например, если разрешается пересылка трафика из сети Интернет в локальную сеть, лучше указать определенные серверы в Интернете, которые будут иметь доступ к локальной сети.

11.3.2 Правила с точки зрения безопасности

1 Когда правило составлено, очень важно рассмотреть те последствия, которые оно будет иметь для безопасности сети.

2 Не мешает ли данное правило пользователям локальной сети иметь доступ к каким-либо важным ресурсам Интернета? Например, если блокируется IRC, есть ли пользователи, которым необходима эта служба?

3 Нельзя ли видоизменить правило так, чтобы оно стало более конкретным? Например, если IRC заблокирован для всех пользователей, возможно, будет целесообразнее задать правило, которое блокирует доступ только для определенных пользователей.

4 Не является ли правило, позволяющее пользователям Интернета иметь доступ к ресурсам локальной сети, причиной появления слабых мест в системе защиты? Например, если соединение с локальной сетью через порт FTP (TCP 20, 21) возможно из Интернета, пользователи Интернета могут получить доступ к работающим FTP-серверам.

5 Нет ли конфликта между данным правилом и другими имеющимися правилами?

6 Если ответы на эти вопросы известны, то добавление правил сведется к простому внесению данных в нужные поля в окнах Web-конфигуратора.

11.3.3 Основные поля для настройки правил

11.3.3.1 Action (Действие)

Какое должно быть действие **Block** (блокировать) или **Forward** (пересылать)? “Block” означает, что межсетевой экран сбрасывает пакет без уведомления.

11.3.3.2 Service (Служба)

Выберите службу из прокручиваемого окна списка **Service** (служба). Если нужной службы нет в списке, необходимо сначала ее определить. Для получения более подробной информации о предварительно заданных службах см. Разд. 11.10 на с. 168.

11.3.3.3 Source Address (Адрес источника)

Каков адрес источника соединения: в локальной или глобальной сети? Это одиночный IP-адрес, диапазон IP-адресов или подсеть?

11.3.3.4 Destination Address (Адрес получателя)

Каков адрес получателя соединения; в локальной или глобальной сети? Это одиночный IP-адрес, диапазон IP-адресов или подсеть?

11.4 Направление связи

В этом разделе приведены примеры правил межсетевого экрана для соединений LAN–WAN и WAN–LAN.

Правила для соединений из LAN в LAN/маршрутизатор, из WAN в WAN/маршрутизатор применяются к пакетам, поступающим на соответствующий порт (LAN, WAN). "LAN–LAN/маршрутизатор" — это правила для соединений "LAN-интернет-центр" (правила для управления интернет-центром через порт LAN) и правила для соединений "LAN–LAN" (правила для управления маршрутизацией между двумя подсетями в локальной сети). Аналогично, правила для соединений "WAN–WAN/маршрутизатор" применяются к портам WAN.

11.4.1 Правила LAN–WAN

Правило, устанавливаемое по умолчанию для трафика направлением LAN–WAN, разрешает всем пользователям в локальной сети неограниченный доступ к глобальной. Назначение правил "LAN–WAN" обычно подразумевает запрет для некоторых или всех пользователей доступа к определенным службам глобальной сети.

11.4.2 Правила WAN–LAN

Правило, устанавливаемое по умолчанию для трафика направлением WAN–LAN блокирует все входящие соединения (из глобальной сети в локальную). Чтобы разрешить отдельным пользователям глобальной сети доступ к локальной, необходимо создать дополнительные правила.

11.4.3 Предупреждения

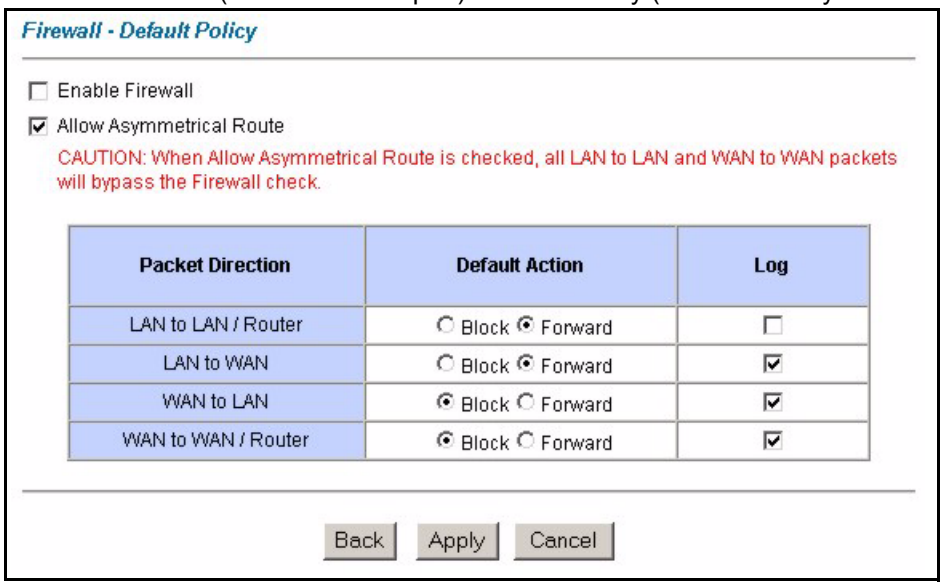
Предупреждения — это сообщения о событиях (таких как атаки), информация о которых может быть необходима пользователю немедленно. Вы можете активировать генерирование предупреждений при обнаружении атаки либо при удовлетворении условиям правила в окне **Edit Rule (Редактировать правило)** (отметьте флажком окошко "**Send Alert Message to Administrator When Matched**" — "**Отправлять сообщение администратору при совпадении**"). Если событие генерирует предупреждение, сообщение незамедлительно отправляется по адресу электронной почты, который указан в экране **Log Settings (Настройки журналов)** (см. главу о журнальной регистрации).

11.5 Настройка политики межсетевого экрана по умолчанию

Нажмите **Firewall**, а затем **Default Policy** для отображения следующего окна. Активируйте межсетевой экран, поставив флажок напротив **Firewall Enabled** (см. ниже).

Более подробную информацию см. в Разд. 10.1 на с. 136.

Рис. 52 Firewall (Межсетевой экран): Default Policy (Политика по умолчанию)



В следующей таблице даны описания полей этого окна.

Табл. 37 Firewall (Межсетевой экран): Default Policy (Политика по умолчанию)

ПОЛЕ	ОПИСАНИЕ
Firewall Enabled (Межсетевой экран включен)	Выберите эту опцию, чтобы включить межсетевой экран. При включенном экране интернет-центр будет осуществлять управление доступом и защищать от атак типа "Отказ в обслуживании" (DoS).
Allow Asymmetrical Route (Разрешить асимметричные маршруты)	Поставьте метку в этом окошке, чтобы межсетевой экран интернет-центра допускал использование треугольной топологии сетевых маршрутов. Дополнительную информацию о треугольной топологии маршрутов см. в *приложении*.
Packet Direction (Направление пакетов)	Это направление движения пакетов: **LAN to LAN/Router (LAN–LAN/ Маршрутизатор), LAN to WAN (LAN–WAN)**, **WAN to WAN/Router (LAN–WAN/Маршрутизатор)**, **WAN-LAN**). Правила межсетевого экрана группируются по направлениям движения пакетов, к которым они применяются. Например, **LAN–LAN/ Маршрутизатор** означает пакеты, которые перемещаются из компьютера/ подсети локальной сети к другому компьютеру/подсети порта ЛВС интернет-центра или к самому интернет-центру.
Default Action (Действия по умолчанию)	Выберите при помощи переключателей, следует ли блокировать (**Block**) или разрешить (**Forward**) пересылку пакетов, которые движутся в выбранном направлении.

Табл. 37 Firewall (Межсетевой экран): Default Policy (Политика по умолчанию)

ПОЛЕ	ОПИСАНИЕ
Log (Регистрационный журнал)	Отметьте эту опцию, чтобы создать журнал регистрации осуществления определенных выше действий для пакетов, которые движутся в выбранном направлении и не соответствуют определенным ниже правилам.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

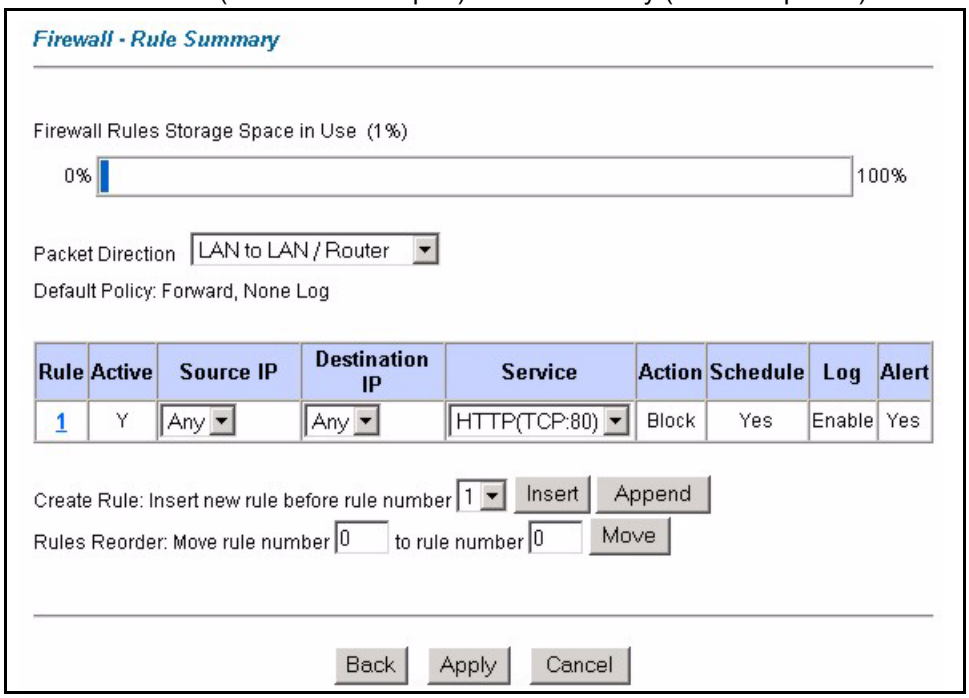
11.6 Список правил

ПРИМЕЧАНИЕ: Очередность правил очень важна, так как правила применяются одно за другим.

Более подробную информацию см. в Разд. 10.1 на с. 136.

Нажмите **Firewall (Межсетевой экран)**, затем **Rule Summary (Список правил)** для вызова следующего окна. На экране появится список существующих правил. Следует обратить внимание на порядок, в котором они перечислены.

Рис. 53 Firewall (Межсетевой экран): Rule Summary (Список правил)



В следующей таблице даны описания полей этого окна.

Табл. 38 Rule Summary (Список правил)

ПОЛЕ	ОПИСАНИЕ
Firewall Rules Storage Space in Use (Память, занятая правилами межсетевого экрана)	Этот информационный индикатор показывает, какая часть памяти интернет-центра, предназначенная для записи правил межсетевого экрана используется в данный момент. Если занято 80% или менее доступной памяти, индикатор остается зеленым. Если занято более 80% памяти, индикатор становится красным.
Packet Direction (Направление пакетов)	Выберите из раскрывающегося списка направление движения пакетов, для которого вы хотите определить правила межсетевого экрана.
Default Policy (Политика по умолчанию)	В этом поле отображается действие по умолчанию и политика регистрации, выбранные в окне **Default Rule** для направления пакетов, определенного в предыдущем поле.
	Следующие поля, предназначенные только для чтения, содержат информацию о правилах, определенных для трафика в выбранном направлении. Установленные правила межсетевого экрана (описанные ниже) имеют приоритет перед общими настройками межсетевого экрана (указаны выше).
Rule (Правило)	Номер правила. Порядок расположения правил имеет большое значение, так как правила выполняются по очереди. Выберите номер правила, чтобы перейти к окну **Firewall Edit Rule (Редактировать правило)** и настроить или изменить правило межсетевого экрана.
Active (Активировать)	В этом поле отображается состояние межсетевого экрана: включен (**Y**) или выключен (**N**).

Табл. 38 Rule Summary (Список правил) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Source IP (IP-адрес источника)	Этот раскрывающийся список содержит адреса или диапазоны адресов источника, к которым применяется данное правило межсетевого экрана. Заметьте, что отсутствие адреса источника или получателя эквивалентно выбору **Any (Любой)**.
Destination IP (IP-адрес получателя)	Этот раскрывающийся список содержит адреса или диапазоны адресов получателя, к которым применяется данное правило межсетевого экрана. Заметьте, что отсутствие адреса источника или получателя эквивалентно выбору **Any (Любой)**.
Service (Служба)	Этот раскрывающийся список содержит службы, к которым применяется данное правило межсетевого экрана. Заметьте, что отсутствие типа службы эквивалентно выбору **Any (Любой)**. Более подробную информацию см. в Разд. 11.10 на с. 168.
Action (Действие)	Определяет действие для данного правила, возможнные варианты **Block** (блокировать) или **Forward** (пересылать). Заметим, что включение опции **Block** означает, что межсетевой экран просто сбрасывает пакет.
Schedule (Расписание)	Это поле показывает, определено (**Yes**) или нет (**No**) расписание.
Log (Регистрационный журнал)	Это поле показывает, создается ли журнальная запись, если пакеты соответствуют данному правилу: **Enabled (Создается)** или **Disable (Не создается)**.
Alert (Предупреждение)	Это поле показывает, выдается (**Yes**) или нет (**No**) предупреждение, если условия данного правила выполняются.
Insert/Append (Вставить/добавить)	Введите номер, под которым вы хотите определить правило. Например, если вы введете “6”, новое правило получит номер 6, а старое правило под номером 6 (если такое было) получит номер 7. Нажмите **Insert**, чтобы добавить новое правило межсетевого экрана перед указанным номером. Нажмите **Append**, чтобы добавить новое правило межсетевого экрана после указанного номера.
Move (Переместить)	Введите номер правила и номер, на который вы хотите его переместить. Нажмите **Move** (переместить), чтобы перенести это правило на введенный номер. Порядок расположения правил имеет большое значение, так как правила выполняются по очереди.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

11.6.1 Настройка правил межсетевого экрана

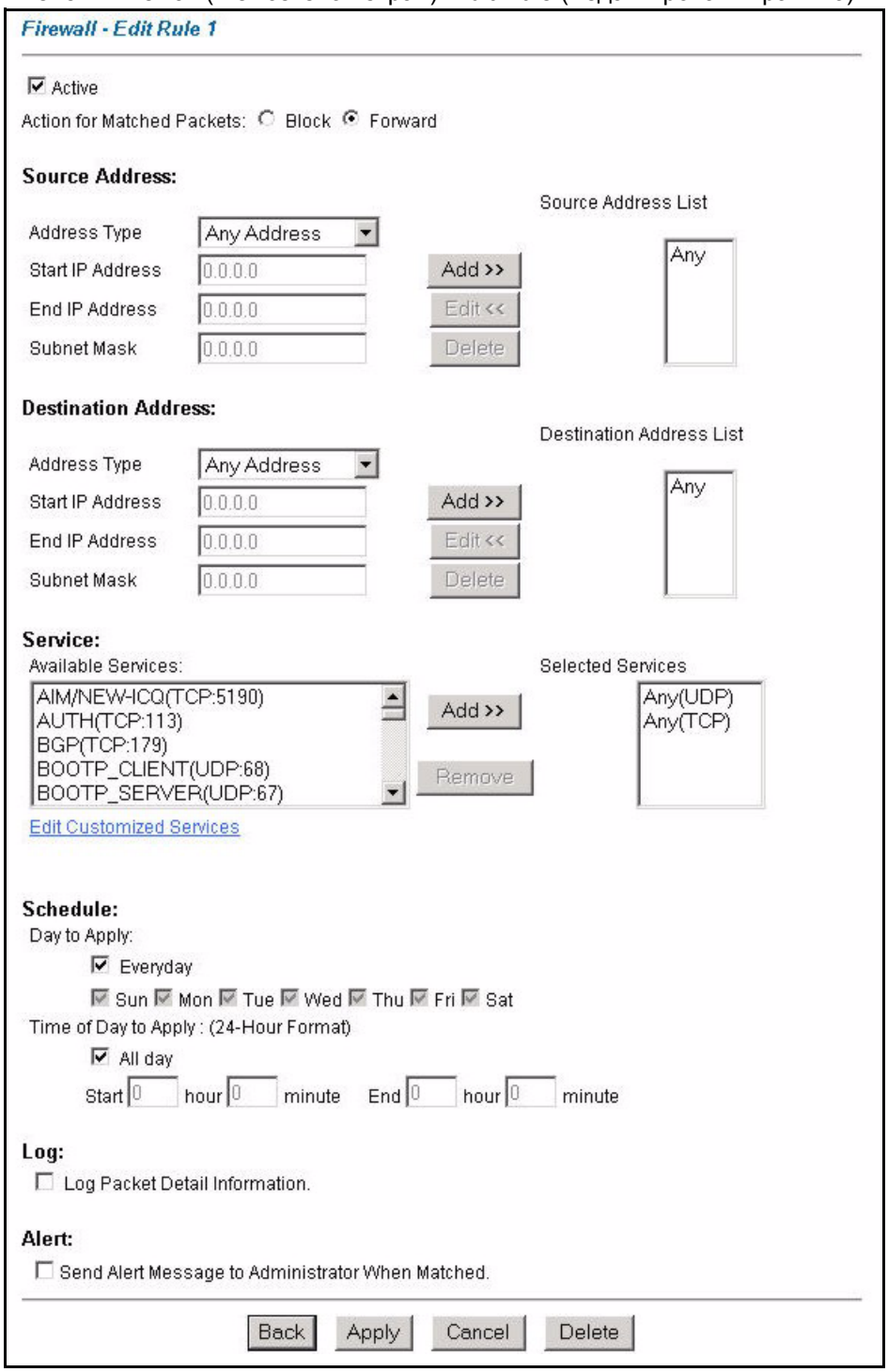
Более подробную информацию см. в Разд. 10.1 на с. 136.

Для создания нового правила выполните следующие действия.

1 В окне **Rule Summary (Список правил)** введите номер, под которым должно значиться данное правило. Например, если вы введете “6”, новое правило получит номер 6, а старое правило под номером 6 (если такое было) получит номер 7.

2 Нажмите кнопку **Insert** для отображения этого окна, информацию о полях см. в приведенной ниже таблице.

Рис. 54 Firewall (Межсетевой экран): Edit Rule (Редактировать правило)



В следующей таблице даны описания полей этого окна.

Табл. 39 Firewall (Межсетевой экран): Edit Rule (Редактировать правило)

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Выберите эту опцию, чтобы задействовать данное правило межсетевого экрана.
Action for Matched Packet (Действие для соответствующего пакета)	Выберите при помощи переключателей, следует ли блокировать (**Block**) или разрешить (**Forward**) пересылку пакетов, соответствующих данному правилу.
Source/Destination Address (Адрес источника/получателя)	
Address Type (Тип адреса)	Хотите ли вы, чтобы это правило применялось к пакетам с (одним) определенным IP-адресом, любым из диапазона IP-адресов (например, от 192.168.1.10 до 192.169.1.50), подсети или любому IP-адресу? Выберите нужную опцию из раскрывающегося списка, в который входят: **Single Address (Один адрес)**, **Range Address (Диапазон адресов)**, **Subnet Address (Адрес подсети)** и **Any Address (Любой адрес)**.
Start IP Address(Начальный IP-адрес)	Ввести одиночный IP-адрес или начальный IP-адрес группы.
End IP Address (Конечный IP-адрес)	Ввести конечный IP-адрес группы.
Subnet Mask (Маска подсети)	Введите маску подсети, если таковая имеется.
Add (Добавить)	Нажмите на **Add**, чтобы добавить новый адрес в поле **Source Address** или **Destination Address**. Добавлять можно группы адресов, диапазоны адресов и/или подсети.
Edit (Редактировать)	Чтобы отредактировать существующий адрес источника или получателя, выберите его в соответствующем поле и нажмите на **Edit**.
Delete (Удалить)	Выделите существующий адрес источника или получателя в поле **Source Address** или **Destination Address** и нажмите на **Delete**, чтобы удалить его.
Services (Службы)	
Available/Selected Services (Доступные/ Выбранные службы)	Более подробную информацию об имеющихся службах см. Разд. 11.10 на с. 168. Выделите одну из служб в списке **Available Services** слева, затем нажмите **Add>>**, чтобы добавить ее в список **Selected Services** справа. Чтобы удалить службу, выделите ее в списке **Selected Services** справа и нажмите **Remove**.
Edit Customized Service (Редактирование пользовательских служб)	Щелкните по ссылке **Edit Customized Services**, чтобы открыть окно, позволяющее настроить новую службу, отсутствующую в стандартном списке служб.
Schedule (Расписание)	
Day to Apply (День применения)	Выберите, должно ли правило прменяться каждый день (Everyday) или в определенные дни недели.
Time of Day to Apply (24-Hour Format) (Время применения в 24-часовом формате)	Выберите **All Day (Круглосуточно)** или введите время начала и окончания применения правила в часах и минутах.

Табл. 39 Firewall (Межсетевой экран): Edit Rule (Редактировать правило)

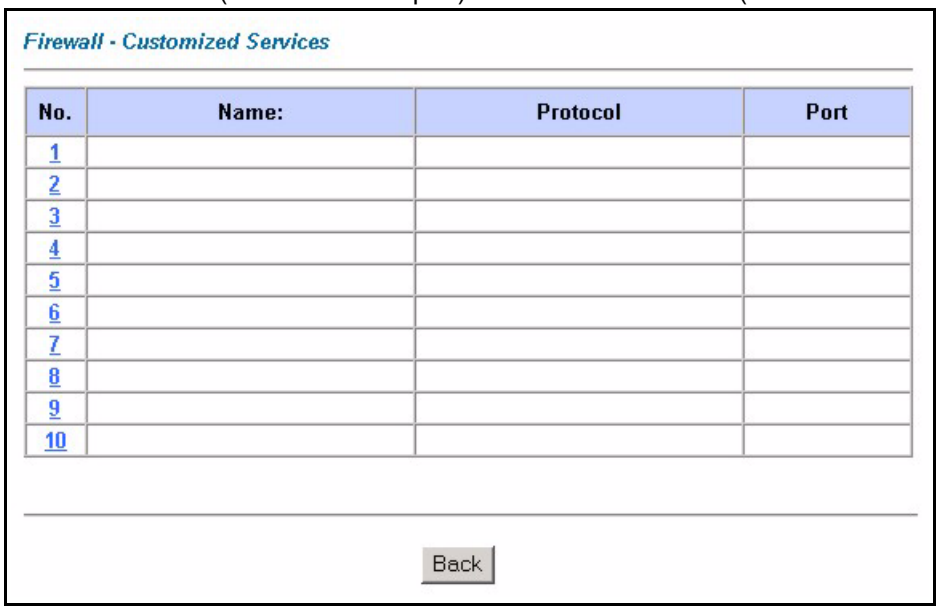
ПОЛЕ	ОПИСАНИЕ
Log (Регистрационный журнал)	
Log Packet Detail Information (Регистрировать подробную информацию о пакете)	Это поле определяет, создается (**Enabled**) или нет (**Disable**) журнальная запись для пакетов, соответствующих данному правилу. Перейдите на страницу **Log Settings (Настройки журналов)** и выберите категорию **Access Control (Управление доступом)**, чтобы включить ведение этих журналов интернет-центром.
Alert (Предупреждение)	
Send Alert Message to Administrator When Matched (Посылать администратору предупреждение при совпадении)	Выберите эту опцию, чтобы интернет-центр выдавал предупреждение в случае выполнения условий данного правила.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel**, чтобы выйти из этого окна без сохранения изменений.
Delete (Удалить)	Нажмите кнопку **Delete (Удалить)**, чтобы удалить данное правило межсетевого экрана и вернуться к окну **Firewall Rule Summary (Межсетевой экран: список правил)**.

11.7 Пользовательские службы

Позволяет настроить пользовательские службы и номера портов, не определенные в интернет-центре изначально. Полный перечень номеров портов и служб приведен на сайте IANA (Internet Assigned Number Authority — Агентство по назначению имен и уникальных параметров протоколов Интернет). Дополнительную информацию по службам см. в Разд. 11.10 на с. 168. Чтобы настроить порт пользовательской службы при редактировании правила межсетевого экрана щелкните по ссылке **Customized Services (Пользовательские службы)**.При этом откроется следующее окно.

Более подробную информацию см. в Разд. 10.1 на с. 136.

Рис. 55 Firewall (Межсетевой экран): Customized Services (Пользовательские службы)



В следующей таблице даны описания полей этого окна.

Табл. 40 Customized Services (Пользовательские службы)

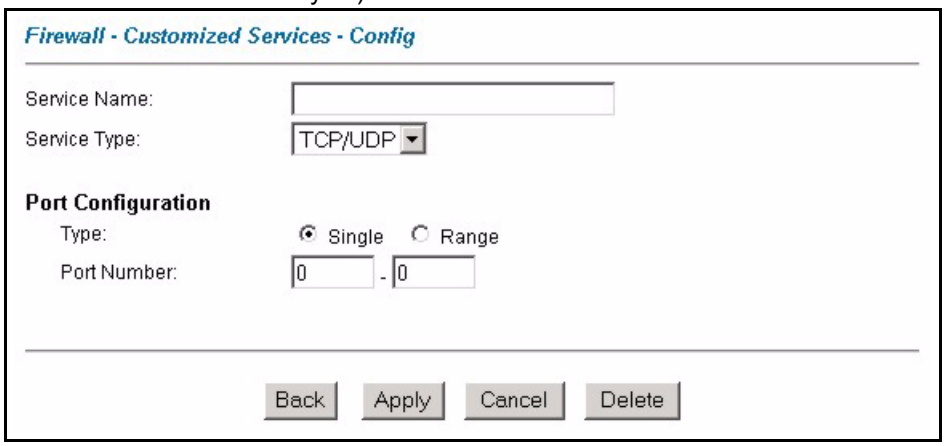
ПОЛЕ	ОПИСАНИЕ
No. (Номер)	Номер дополнительно назначаемого пользовательского порта. Выберите номер правила для службы, чтобы вызвать экран **Firewall Customized Services Config** и настроить или отредактировать пользовательскую службу.
Name (Имя)	В этом поле отображается название пользовательской службы.
Protocol (Протокол)	В этом поле отображается протокол IP (**TCP**, **UDP** или **TCP/UDP**), определяющий пользовательскую службу.
Port (Порт)	В этом поле отображается номер порта или диапазон, определяющий пользовательскую службу.
Back (Назад)	Нажмите кнопку **Back** для возвращения к экрану **Firewall Edit Rule**.

11.8 Настройка пользовательских служб

Выберите номер правила в окне **Firewall Customized Services**, чтобы создать новый пользовательский порт или отредактировать существующий. Появится следующий экран.

Более подробную информацию см. в Разд. 10.1 на с. 136.

Рис. 56 Firewall (Межсетевой экран): Configure Customized Services (Настройка пользовательских служб)



В следующей таблице даны описания полей этого окна.

Табл. 41 Firewall (Межсетевой экран): Configure Customized Services (Настройка пользовательских служб)

ПОЛЕ	ОПИСАНИЕ
Service Name (Имя службы)	Введите уникальное имя для пользовательского порта.
Service Type (Тип службы)	Выберите из раскрывающегося списка порт IP (**TCP**, **UDP** или **TCP/UDP**) для пользовательского порта.
Port Configuration (Настройка порта)	
Type (Тип)	Выберите **Single** для одного порта или **Range** для диапазона из нескольких портов, связанных с пользовательской службой.
Port Number (Номер порта)	Введите один номер или диапазон номеров портов, связанных с пользовательской службой.
Back (Назад)	Нажмите кнопку **Back** для возвращения к экрану **Firewall Edit Rule**.
Apply (Применить)	Нажмите кнопку **Apply**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.
Delete (Удалить)	Нажмите кнопку **Delete**, чтобы удалить текущее правило.

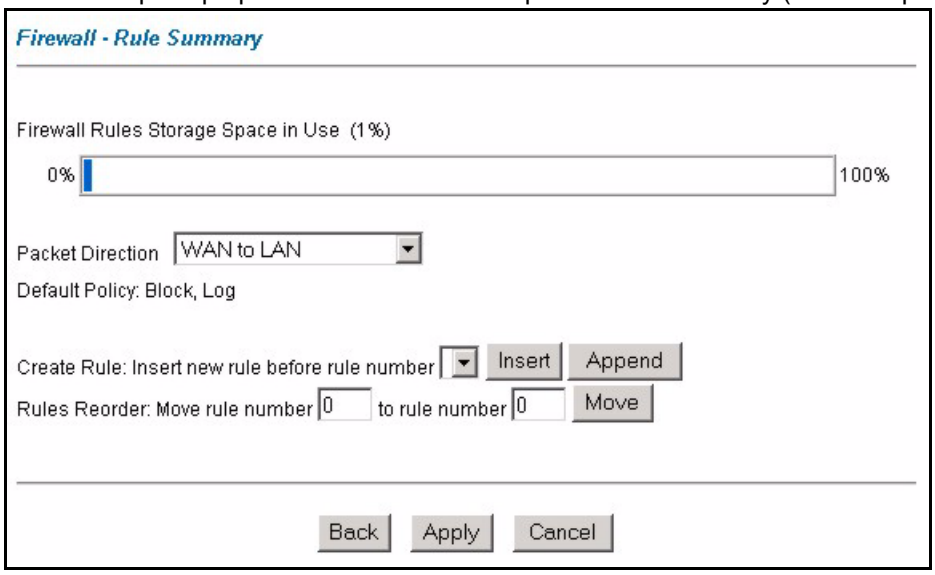
11.9 Пример правила межсетевого экрана

Следующий пример правила межсетевого экрана разрешает гипотетическое соединение “My Service”, инициируемое из Интернета.

1 Нажмите кнопку **Firewall (Межсетевой экран)** на навигационной панели и затем по **Rule Summary (Список правил)**.

2 Выберите **WAN to LAN** в поле **Packet Direction (Маршрут пакета)**.

Рис. 57 Пример правила межсетевого экрана: Rule Summary (Список правил)



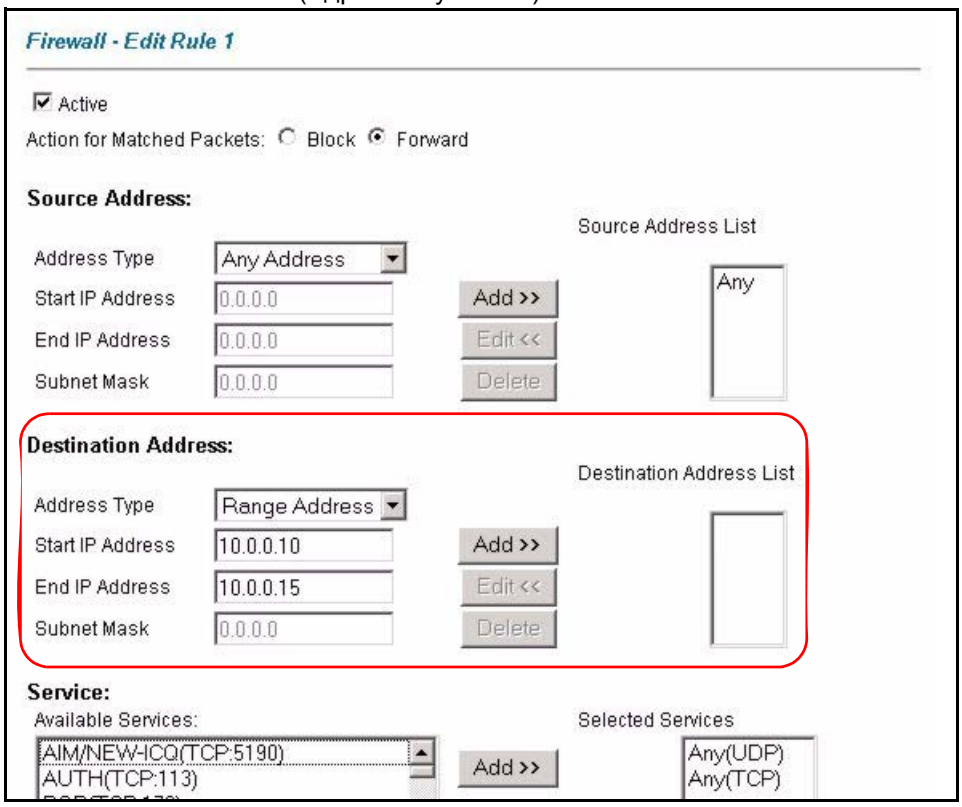
3 В окне **Rule Summary (Список правил)** введите номер, под которым должно значиться данное правило. Например, если вы введете “6”, новое правило получит номер 6, а старое правило под номером 6 (если такое было) получит номер 7.

4 Нажмите кнопку **Insert** для отображения окна "Firewall rule configuration" (Настройка правила межсетевого экрана).

5 В окне **Destination Address (Адрес получателя)** выберите **Any (любой)**, а затем нажмите **Delete**.

6 Выполните настройки в окне "Адрес получателя", как показано ниже и нажмите кнопку **Add**.

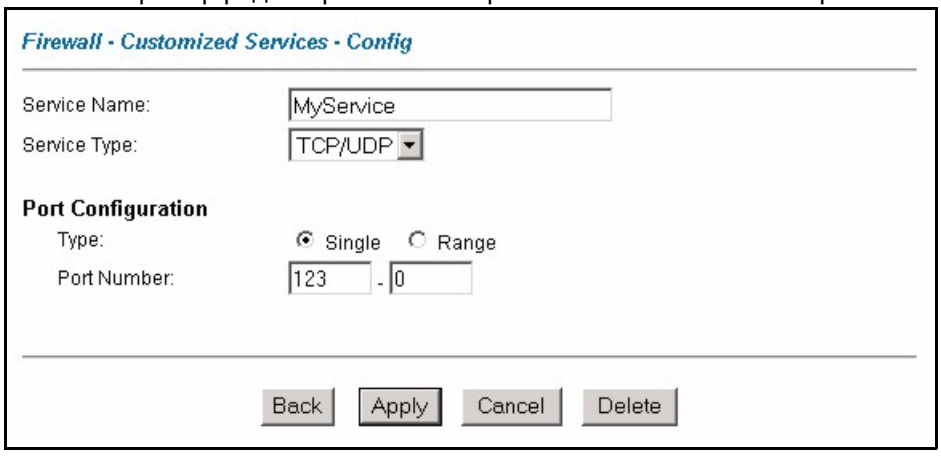
Рис. 58 Пример правила межсетевого экрана: Edit Rule (Редактировать правило): Destination Address (Адрес получателя)



7 В окне **Edit Rule** щелкните по ссылке **Customized Services**, при этом откроется окно **Customized Service (Пользовательские службы)**.

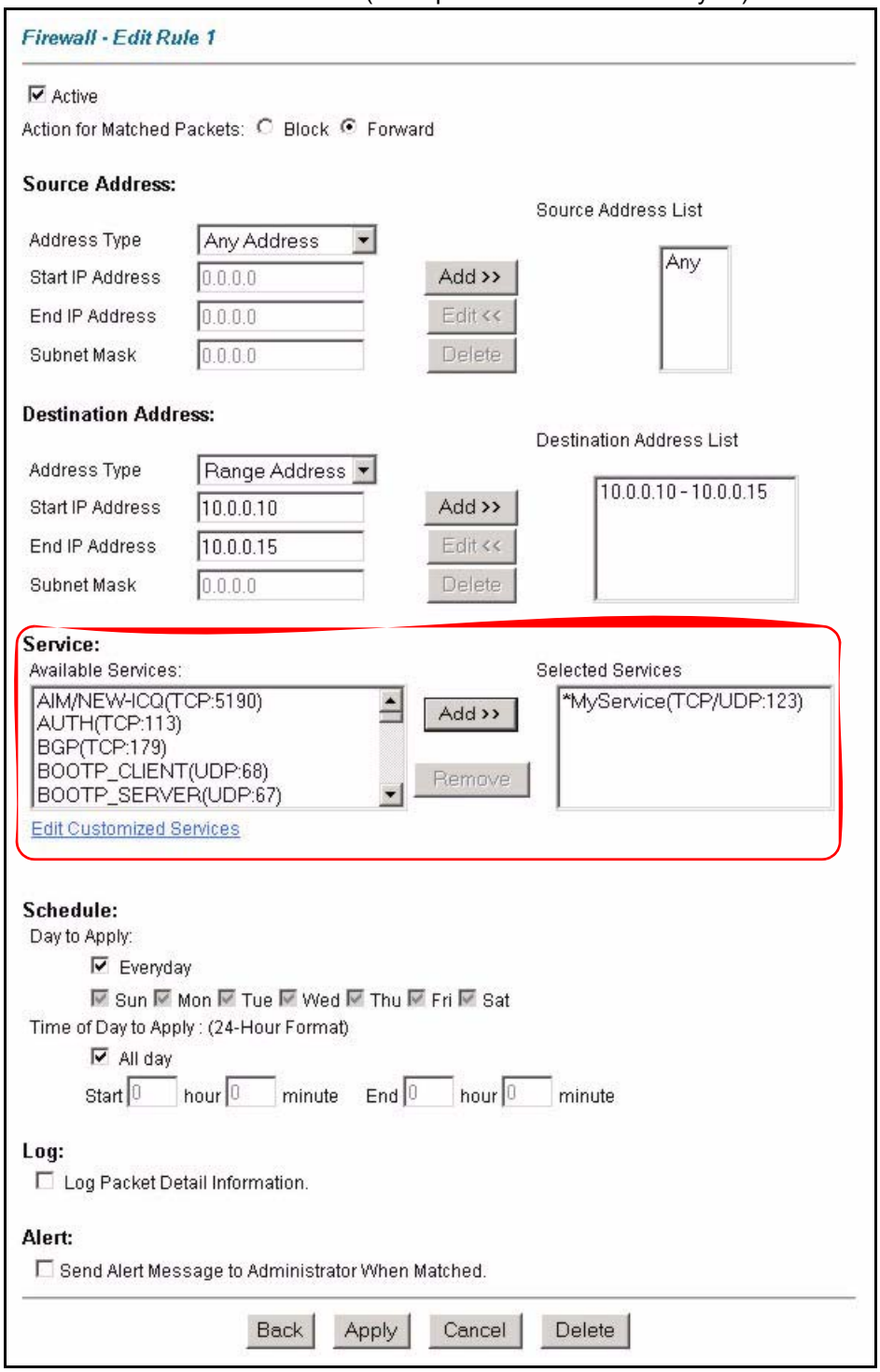
8 Выберите номер правила, при этом откроется окно **Customized Services -Config (Пользовательские службы — настройка)**, выполните в нем показанные ниже настройки и нажмите **Apply (Применить)**.

Рис. 59 Пример редактирования настроек пользовательского порта



9 В окне **Edit Rule** с помощью кнопок **Add (Добавить)>>** и **Remove (Удалить)** между перечнями **Available Services (Имеющиеся службы)** и **Selected Services (Выбранные службы)** выполните показанные ниже настройки. По окончании нажмите **Apply (Применить)**.

Рис. 60 Пример правила межсетевого экрана: Edit Rule (Редактировать правило): Select Customized Services (Выбор пользовательских служб)

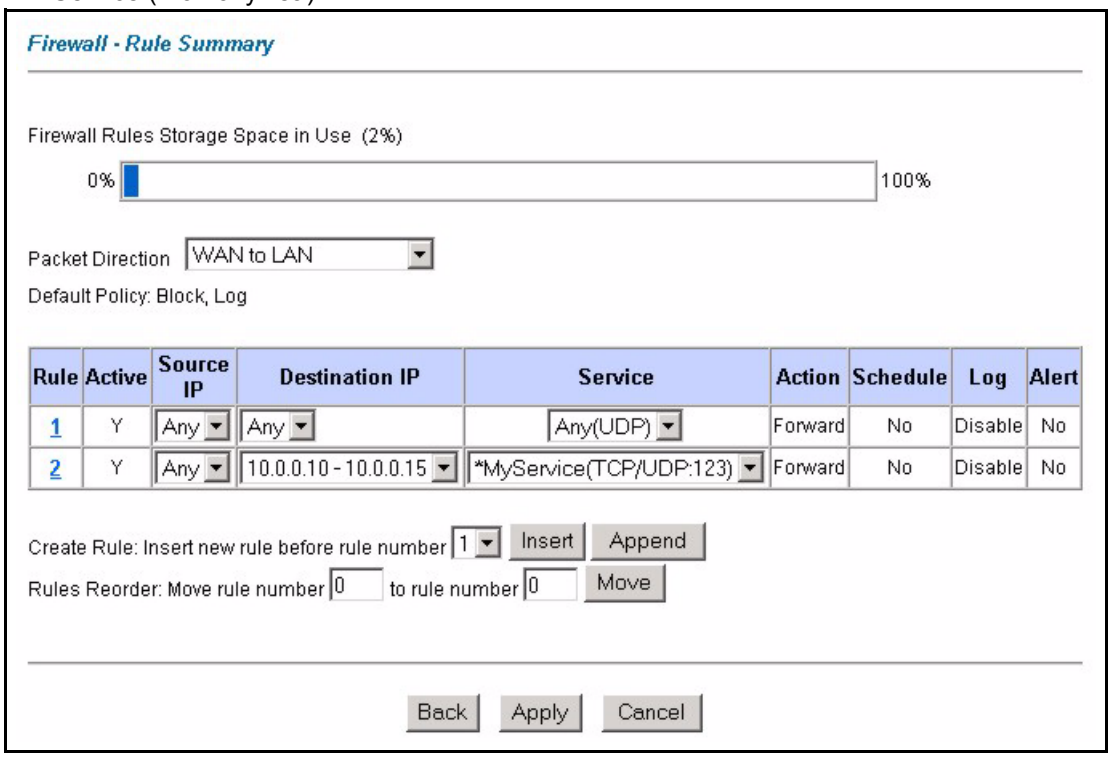


ПРИМЕЧАНИЕ: В окне "Services list" (Перечень служб) и **Rule Summary (Список правил)** появятся наименования пользовательских портов со звездочками (“*”) перед ними. После создания порта нажмите кнопку **Apply (Применить)**.

По завершении процедуры настройки правила межсетевого экрана Интернет, окно **Rule Summary** должно выглядеть следующим образом (см. ниже).

Правило 2 разрешает соединение “My Service” (Моя служба) от WAN к IP-адресам 10.0.0.10–10.0.0.15 в локальной сети.

Рис. 61 Пример правила межсетевого экрана: Rule Summary (Список правил): My Service (Моя служба)



11.10 Предварительно настроенные службы

Список **Available Services** в окне **Edit Rule** (см. Разд. 11.6.1 на с. 159) отображает все предварительно настроенные службы, которые интернет-центр уже поддерживает. Рядом с названием службы помещаются два поля в скобках. В первом поле указывается тип протокола IP (TCP, UDP, или ICMP). Во втором — номер порта IP для данной службы. Следует учесть, что тип протокола IP может быть не один. Например, взгляните

на конфигурацию по умолчанию, обозначенную “(**DNS**)”. **(UDP/TCP:53)** означает UDP-порт 53 и TCP-порт 53. Возможно до 128 записей. Порты пользовательских служб можно настроить также с помощью функции **Edit Customized Services**, о которой было рассказано выше.

Табл. 42 Предварительно настроенные службы

СЛУЖБА	ОПИСАНИЕ
AIM/NEW_ICQ(TCP:5190)	Система пересылки сообщений в сети Интернет, предоставляемая корпорацией AOL, используется службой ICQ как "слушающий" порт.
AUTH(TCP:113)	Протокол аутентификации, используемый 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(UDP/TCP:53)	Сервер имен доменов — служба, определяющая соответствие web-имен (например, www.zyxel.com) номерам IP.
FINGER(TCP:79)	Finger — команда для UNIX или Интернет, используемая для проверки вхождения пользователя в сеть.
FTP(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 уровня клиент/сервер для WWW.
HTTPS	Протокол защищенной передачи текстов, часто используемый в Интернет-коммерции.
ICQ(UDP:4000)	Популярная система интерактивного общения в Интернет.
IPSEC_TRANSPORT/ TUNNEL(AH:0)	Туннелирующий протокол IPSEC AH (заголовок аутентификации).
IPSEC_TUNNEL(ESP:0)	Эту службу использует протокол туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).
IRC(TCP/UDP:6667)	Еще одна программа интерактивного общения в Интернет.
MSN Messenger(TCP:1863)	Протокол для передачи сообщений в сетях Microsoft.
MULTICAST(IGMP:0)	Широковещательный протокол взаимодействия групп в сети Интернет, используется для рассылки пакетов определенным группам узлов.
NEWS(TCP:144)	Протокол для групп новостей.
NFS(UDP:2049)	Сетевая файловая система — NFS, распределенная файловая система клиент/сервер, обеспечивающая прозрачное совместное использование файлов в сетевом окружении.
NNTP(TCP:119)	Сетевой протокол передачи новостей, система доставки для групп новостей USENET.
PING(ICMP:0)	Packet INternet Groper (Пакетное эхо-тестирование в Интернет) — это протокол, который посылает эхо-запросы ICMP для проверки достижимости удаленного узла.

Табл. 42 Предварительно настроенные службы (продолжение)

СЛУЖБА	ОПИСАНИЕ
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)	Протокол туннелирования между узлами, обеспечивает безопасную передачу данных в общедоступных сетях. Это — канал управления.
PPTP_TUNNEL(GRE:0)	Протокол туннелирования между узлами, обеспечивает безопасную передачу данных в общедоступных сетях. Это — канал 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 сетевой доступ по Telnet.
RTSP(TCP/UDP:554)	Протокол передачи мультимедийных потоков (RTSP), обеспечивает удаленное управление потоками аудио/видео данных в сети Интернет.
SFTP(TCP:115)	Простой протокол передачи файлов.
SMTP(TCP:25)	Простой протокол электронной почты, стандартный протокол обмена сообщениями для сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой.
SNMP(TCP/UDP:161)	Простой протокол сетевого управления.
SNMP-TRAPS (TCP/ UDP:162)	Система регистрации событий в потоке SNMP (RFC:1215).
SQL-NET(TCP:1521)	Язык структурированных запросов, интерфейс доступа к системам баз данных различного типа, в том числе супер-ЭВМ, ЭВМ средней производительности, системам UNIX и сетевым серверам.
SSDP(UDP:1900)	Протокол упрощенной службы обнаружения (SSDP) — это служба обнаружения, отыскивающая устройства типа Plug and Play в домашней сети или шлюзы в Интернете для предачи данных при помощи порта 1900 протокола DUDP.
SSH(TCP/UDP:22)	Программа безопасной удаленной регистрации.
STRMWORKS(UDP:1558)	Протокол передачи потоков Stream Works.
SYSLOG(UDP:514)	Системный журнал — позволяет отправлять журналы системы серверу UNIX.
TACACS(UDP:49)	Протокол регистрации узла, используемый для системы управления доступом на основе контроллера доступа к терминалу.
TELNET(TCP:23)	Telnet — протокол регистрации и эмуляции терминала, общий для среды Интернет и UNIX. Он работает в сетях TCP/IP. Его главная задача состоит в том, чтобы позволить пользователям регистрироваться на удаленных узлах.
TFTP(UDP:69)	Упрощенный протокол передачи файлов, протокол передачи файлов, подобный FTP, но использующий протокол UDP (протокол передачи дейтаграмм пользователя), а не TCP (протокол управления передачей).
VDOLIVE(TCP:7000)	Еще одна программа для видеоконференций.

11.11 Anti-Probing (Блокирование эхо-тестирования)

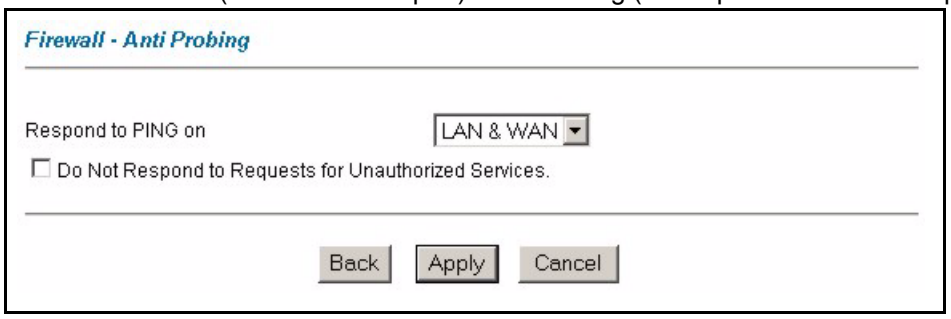
Если внешний пользователь попробует прозондировать порт вашего интернет-центра, ему будет автоматически отправлен ответный пакет ICMP. Это позволяет внешнему пользователю узнать о существовании интернет-центра. Модель P–660HT/HTW EE поддерживает функцию блокирования эхо-тестирования, предотвращающую отправку ответного пакета ICMP и, соответственно, обнаружение устройства при эхо-тестировании портов извне.

Протокол управляющих сообщений в сети Интернет (ICMP) является протоколом управляющих сообщений и сообщений об ошибках между сервером-узлом и шлюзом выхода в Интернет. ICMP использует дейтаграммы Интернет-протокола (IP), но сообщения обрабатываются программным обеспечением TCP/IP, и невидимы для пользователей приложений.

Более подробную информацию см. в Разд. 10.1 на с. 136.

Нажмите кнопку **Firewall** на навигационной панели и затем **Anti Probing (Блокирование эхо-тестирования)**, при этом появится показанное ниже окно.

Рис. 62 Firewall (Межсетевой экран): Anti Probing (Блокирование эхо-тестирования)



В следующей таблице даны описания полей этого окна.

Табл. 43 Firewall (Межсетевой экран): Anti Probing (Блокирование эхо-тестирования)

ПОЛЕ	ОПИСАНИЕ
Respond to PING on (Отвечать на PING-запросы)	Интернет-центр не отвечает на входящие Ping-запросы (зондирующие запросы извне), если выбрана опция **Disable (Выкл.)**. 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.
Do not respond to requests for unauthorized services (Не отвечать на запросы для запрещеных служб).	Выберите эту опцию, чтобы предотвратить обнаружение интернет-центра хакерами путем эхо-тестирования неиспользуемых портов. Если Вы выберете эту опцию, то интернет-центр не будет отвечать на запросы о неиспользуемых портах, таким образом делая неиспользуемые порты и интернет-центр невидимыми. По умолчанию эта опция не отмечена и интернет-центр отвечает на эхо-тестирование неиспользуемых портов UDP ответными ICMP-пакетами "Port Unreachable" (Порт недоступен), а на эхо-тестирование неиспользуемых портов TCP-пакетами "TCP Reset" (Сброс TCP). Обратите внимание, что прежде чем зондирующие пакеты дойдут до механизма блокирования эхо-тестирования, они должны сначала пересечь механизм межсетевого экрана. Поэтому если механизм межсетевого экрана заблокирует зондирующий пакет, то интернет-центр отреагирует в зависимости от политики межсетевого экрана, которая по умолчанию отправляет пакет сброса TCP для заблокированного пакета TCP. Для изменения этой политики Вы можете использовать команду "sys firewall tcprst rst [on|off]". Когда механизм межсетевого экрана блокирует пакет UDP, он удаляет его, не отправляя ответного пакета.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

11.12 Допустимые пороги для атак "Отказ в обслуживании" (DoS)

Для атак типа DoS, интернет-центр использует допустимые пороги, определяющие, когда необходимо удалить сеанс связи, установленный не полностью. Данные допустимые пороги относятся в целом ко всем сессиям.

Можно использовать значения допустимых порогов по умолчанию или установить собственные в соответствиями с требованиями безопасности.

Настройка порогов — см. Разд. 11.12.3 на с. 174.

11.12.1 Значения допустимых порогов

Если что-то не работает и счетчики сетевого экрана проверены, необходимо настроить данные параметры. Значения, установленные по умолчанию, хорошо подходят для небольших офисов. Выбор значений допустимых порогов зависит от следующих величин:

- Максимальное количество открытых сессий.
- Минимальное количество возможных незавершенных заданий на сервере локальной сети.
- Возможности центральных процессоров серверов локальной сети.
- Пропускная способность сети.
- Тип трафика для отдельных серверов.

Если по причинам, зависящим от каких-то из вышеперечисленных факторов, сеть работает медленнее, чем обычно (особенно если имеются медленные серверы или серверы, обрабатывающие большое количество задач, которые часто перегружены), значения по умолчанию необходимо уменьшить.

Изменять значения допустимых порогов необходимо до продолжения работы по настройке параметров межсетевого экрана.

11.12.2 Полуоткрытые сеансы связи

Слишком большое количество полуоткрытых сеансов связи (выраженное конкретным числом или в виде частоты поступлений) может означать наличие атаки Do S. Применительно к TCP, "полуоткрытые" сеансы — это сеансы связи, не дошедшие до состояния установленных, т.е. когда не завершено трехстороннее квитирование по TCP (см. Рис. 48 на с. 141). Для UDP, "полуоткрытое" состояние означает, что межсетевой экран не обнаружил ответный трафик.

Интернет-центр P–660HT/HTW EE измеряет как общее число существующих полуоткрытых сеансов связи, так и интенсивность попыток установления сеанса связи. Для обоих типов соединений, TCP и UDP, считается количество полуоткрытых соединений и интенсивность поступлений. Подсчеты производятся поминутно.

Когда число существующих полуоткрытых сеансов связи превышает верхний допустимый порог (**max-incomplete high**), интернет-центр начинает удалять полуоткрытые сеансы связи для осуществления новых запросов на соединение. Интернет-центр продолжает удалять полуоткрытые запросы по мере необходимости, до тех пор, пока число существующих полуоткрытых сеансов связи не упадет ниже другого допустимого порога (**max-incomplete low**).

Когда интенсивность новых попыток соединения (в минуту) превышает допустимый порог (**one-minute high**), интернет-центр начинает удалять полуоткрытые сеансы связи для осуществления новых запросов на соединение. Интернет-центр продолжает удалять полуоткрытые сеансы связи по мере необходимости, до тех пор, пока интенсивность попыток нового соединения не упадет ниже другого допустимого порога (**one-minute low**). Частота соединений — это количество новых попыток, обнаруженное за последний установленный период выборки длительностью в одну минуту.

11.12.2.1 Максимум неполных TCP-соединений и время блокирования

Слишком большое количество полуоткрытых соединений с одним и тем же адресом узла получателя может означать атаку DoS, направленную на данный компьютер-узел.

Всякий раз, когда число полуоткрытых сеансов связи с одинаковым адресом узла получателя превышает допустимый порог (**TCP Maximum Incomplete — Максимум неполных TCP**), интернет-центр начинает удалять полуоткрытые сеансы связи согласно одному из следующих методов:

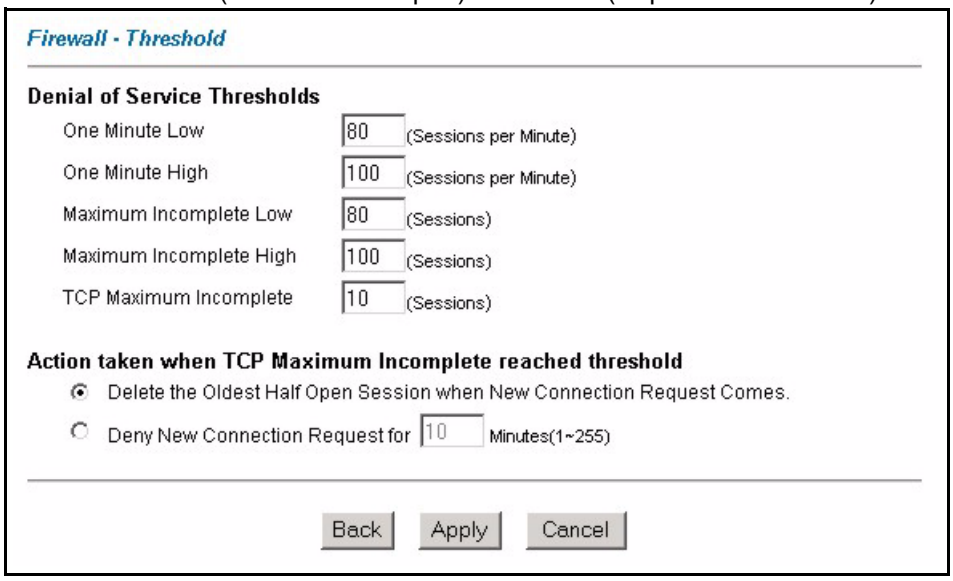
- Если время простоя **Blocking Time (Время блокирования)** равно 0 (по умолчанию), тогда интернет-центр удаляет самые старые существующие полуоткрытые сеансы связи узла для каждого нового запроса на соединение с узлом. В этом случае количество полуоткрытых соединений для данного узла не может превысить допустимый порог.
- Если интервал простоя **Blocking Time (Время блокирования)** выше 0, тогда интернет-центр блокирует все новые запросы на соединение с узлом, предоставляя серверу время на обработку текущих соединений. Интернет-центр продолжает блокировать все новые запросы соединения до тех пор, пока не истечет **Blocking Time (Время блокирования)**.

11.12.3 Настройка порогов межсетевого экрана

Интернет-центр также посылает извещения, всякий раз, когда превышено значение **TCP Maximum Incomplete**. Глобальные значения допустимого порога и времени ожидания действительны для всех TCP-соединений.

Нажмите кнопку **Firewall**, а затем **Threshold**, чтобы открыть следующее окно.

Рис. 63 Firewall (Межсетевой экран): Threshold (Пороговое значение)



В следующей таблице даны описания полей этого окна.

Табл. 44 Firewall (Межсетевой экран): Threshold (Пороговое значение)

ПОЛЕ	ОПИСАНИЕ	ЗНАЧЕНИЯ ПО УМОЛЧАНИЮ
Denial of Service Thresholds (Значения допустимых порогов для атак DoS)		
One Minute Low (Нижний порог интенсивности)	Частота появления новых полуоткрытых соединений, при которой межсетевой экран прекращает удалять полуоткрытые соединения. Интернет-центр продолжает удалять полуоткрытые сеансы связи по мере необходимости, до тех пор, пока интенсивность новых попыток соединения не упадет до этого значения.	80 существующих полуоткрытых соединений.
One Minute High (Верхний порог интенсивности)	Частота появления новых полуоткрытых соединений, при которой межсетевой экран начинает удалять полуоткрытые соединения. Когда интенсивность попыток нового соединения превышает это число, интернет-центр начинает удалять полуоткрытые сеансы связи для осуществления новых соединений.	100 полуоткрытых соединений в минуту. Указанные выше величины означают, что интернет-центр начнет удалять полуоткрытые соединения, как только в течении последней минуты будет зафиксировано более ста попыток установки соединения, и прекратит удалять полуоткрытые соединения, когда в течение последней минуты будет зафиксировано менее 80 попыток.

Табл. 44 Firewall (Межсетевой экран): (продолжение)Threshold (Пороговое значение)

ПОЛЕ	ОПИСАНИЕ	ЗНАЧЕНИЯ ПО УМОЛЧАНИЮ
Maximum Incomplete Low (Максимум незавершенных — нижний порог)	Количество существующих полуоткрытых соединений при котором межсетевой экран прекращает удалять полуоткрытые соединения. Интернет-центр продолжает удалять полуоткрытые сеансы связи по мере необходимости, до тех пор, пока число существующих полуоткрытых сеансов связи не упадет ниже этого значения.	80 существующих полуоткрытых соединений.
Maximum Incomplete High (Максимум незавершенных — верхний порог)	Количество существующих полуоткрытых соединений, при котором межсетевой экран начинает удалять полуоткрытые соединения. Когда число существующих полуоткрытых сеансов связи превышает это значение, интернет-центр начинает удалять полуоткрытые сеансы связи для осуществления новых соединений. Нельзя устанавливать значение **Maximum Incomplete High** ниже текущего значения **Maximum Incomplete Low**.	100 существующих полуоткрытых соединений. Указанные выше величины означают, что интернет-центр начнет удалять полуоткрытые соединения, как только количество существующих полуоткрытых соединений превысит 100, и прекратит удалять полуоткрытые соединения, если количество имеющихся в настоящий момент меньше 80.
Максимум неполных TCP (TCP Maximum Incomplete)	Количество существующих полуоткрытых соединений через TCP с одним и тем же IP-адресом получателя, при котором межсетевой экран начинает сбрасывать полуоткрытые соединения с адресатом по данному IP-адресу. Введите число от 1 до 256. Обычно в случае небольшой сети, медленной системы или ограниченной пропускной способности выбирается небольшое количество	30 существующих полуоткрытых TCP-соединений.
Действия при достижении максимального количества полуоткрытых TCP-соединений.		
Delete the oldest half open session when new connection request comes	Выберите эту опцию для удаления самого старого полуоткрытого соединения при получении запроса на новое соединение.	
Deny new connection request for (Не принимать новые запросы в течение)	Выберите эту опцию и укажите, как долго интернет-центр должен блокировать запросы на новое соединение при достижении порога **TCP Maximum Incomplete**. Введите длительность блокировки (Blocking Time) в минутах (от 1 до 256).	
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.	
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.	
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.	

Глава 12 Фильтрация на основе содержания (контентная фильтрация)

В этой части дается обзор настройки контент-фильтрования.

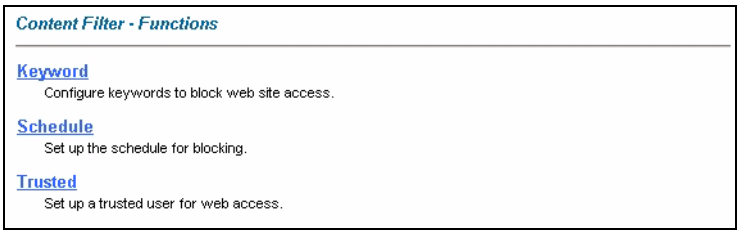
12.1 Фильтрация на основе содержания — общая информация

Фильтрация информации, поступающей из Интернета позволяет создавать и реализовывать правила доступа в Интернет, настроенные под конкретные потребности. Фильтрация на основе содержания дает возможность блокировать сайты по определенным ключевым словам в URL. Можно задать график выполнения интернет-центром фильтрации. Также можно установить правомочные (доверенные) IP-адреса в LAN, для которых интернет-центр не будет производить контентную фильтрацию.

12.2 Главное окно фильтрации на основе содержания

Нажмите кнопку **Content Filter**, при этом откроется главное окно контент-фильтрования.

Рис. 64 Фильтрация на основе содержания (контентная фильтрация)



В следующей таблице даны описания ссылок в этом окне.

Табл. 45 Фильтрация на основе содержания (контентная фильтрация)

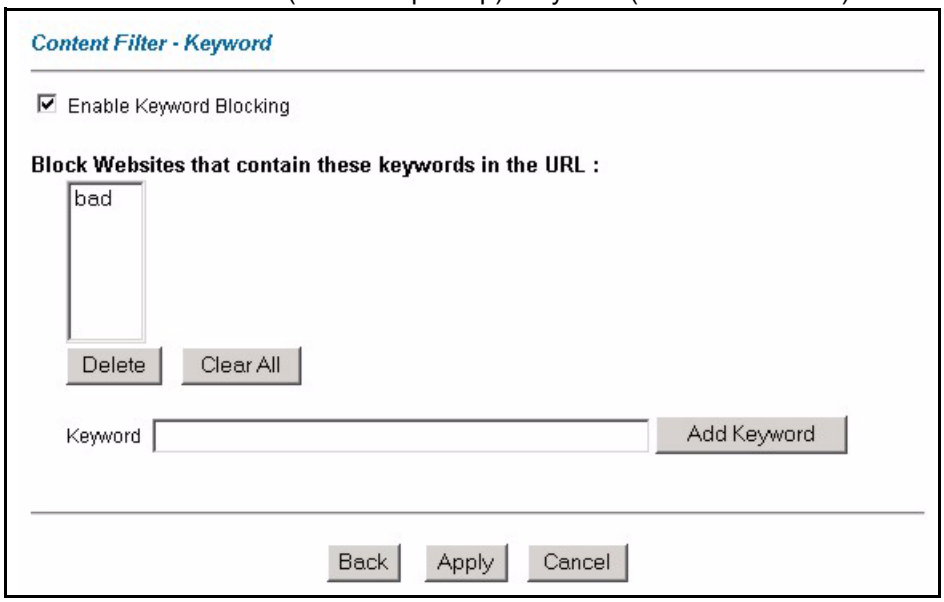
ССЫЛКА	ОПИСАНИЕ
Keyword (Ключевое слово)	Щелкните по этой ссылке, чтобы открыть окно настройки блокировки сайтов, в URL которых содержатся заданные ключевые слова,
Schedule (Расписание)	Щелкните по этой ссылке для вывода окна, где можно установить даты и время, когда интернет-центр будет производить контентную фильтрацию.
Trusted (Доверенный)	Щелкните по этой ссылке для вывода окна, где можно исключить ряд пользователей локальной сети из контент-фильтра интернет-центра.

12.3 Настройка блокировки по ключевым словам

Это окно используется для блокировки сайтов, содержащих определенные ключевые слова в URL. Например, если активировать ключевое слово "bad", то интернет-центр заблокирует доступ по всем сайтам, в которых оно содержится, в том числе URL http://www.website.com/bad.html, даже если он не включен в список фильтрации.

Для того, чтобы интернет-центр блокировал Web-сайты, содержащие ключевые слова в URL, нажмите **Content Filter** и **Keyword**.При этом откроется показанное ниже окно.

Рис. 65 Content Filter (Контент-фильтр): Keyword (Ключевое слово)



В следующей таблице даны описания полей этого окна.

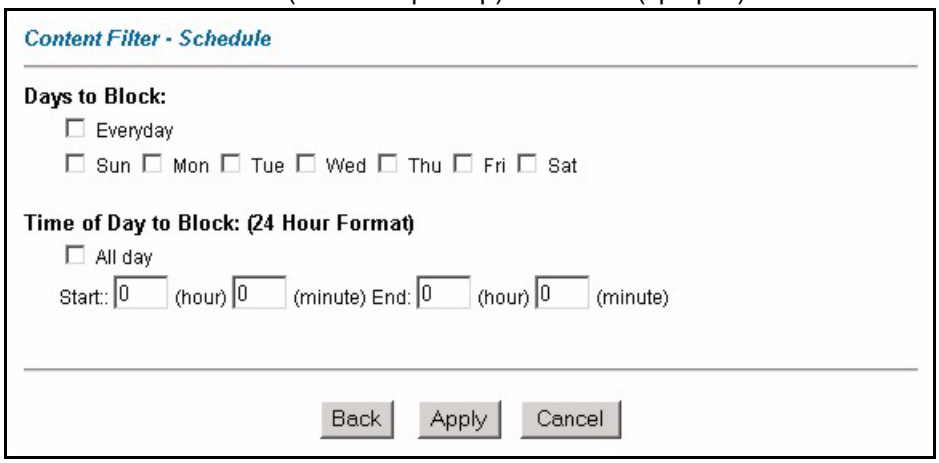
Табл. 46 Content Filter (Контент-фильтр): Keyword (Ключевое слово)

ПОЛЕ	ОПИСАНИЕ
Enable Keyword Blocking (Включение блокировки по ключевым словам)	Поставьте галочку в этом поле для включения функции.
Block Websites that contain these keywords in the URL: (Блокирование Web-сайтов, содержащих в URL ключевые слова:)	Это поле содержит список всех ключевых слов для блокировки.
Delete (Удалить)	Выделите ключевое слово в списке и нажмите **Delete**, чтобы удалить его.
Clear All (Очистить все)	Нажмите **Clear All**, чтобы удалить все ключевые слова из этого списка.
Keyword (Ключевое слово)	Введите в это поле ключевое слово. Допускается использование любых символов (до 127 символа). Использование знаков препинания не допускается.
Add Keyword (Добавить ключевое слово)	Нажмите **Add Keyword** после ввода ключевого слова. Повторите эту процедуру, если нужно добавить другие ключевые слова. Допускается до 64 ключевых слов. При попытке доступа к web-странице, содержащей ключевое слово, будет выведено сообщение о том, что контент-фильтр заблокировал запрос.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

12.4 Настройка графика фильтрации

Для установки даты и времени, когда интернет-центр будет производить контентную фильтрацию, нажмите **Content Filter** и **Schedule**. При этом откроется показанное ниже окно.

Рис. 66 Content Filter (Контент-фильтр): Schedule (График)



В следующей таблице даны описания полей этого окна.

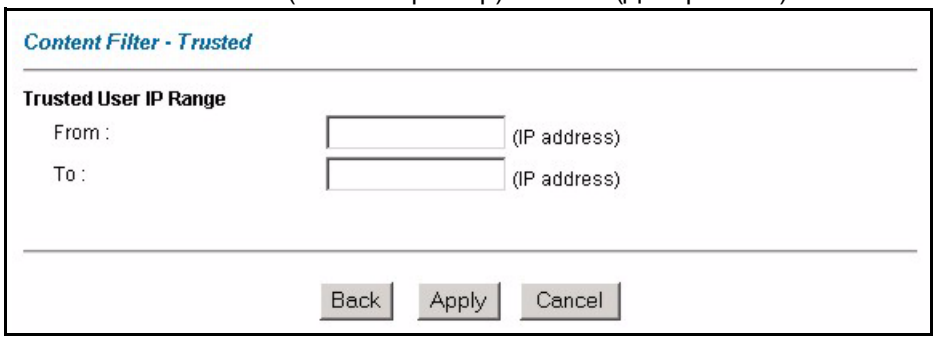
Табл. 47 Content Filter (Контент-фильтр): Schedule (График)

ПОЛЕ	ОПИСАНИЕ
Days to Block: (Дни блокирования)	Поставьте галочку в этом поле, чтобы задать, в какие дни недели (или каждый день) необходимо проводить контентную фильтрацию.
Time of Day to Block: (Время дня для блокирования)	Используя 24-часовой формат установите, в какое время дня (или поставьте галочку в поле **All day — В течение всего дня**) необходимо проводить контентную фильтрацию.
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)** для возврата к предыдущим сохраненным настройкам.

12.5 Настройка списка надежных (доверенных) компьютеров

Чтобы исключить диапазон пользователей ЛВС из контент-фильтрования, нажмите **Content Filter** и **Trusted**. При этом откроется показанное ниже окно.

Рис. 67 Content Filter (Контент-фильтр): Trusted (Доверенные)



В следующей таблице даны описания полей этого окна.

Табл. 48 Content Filter (Контент-фильтр): Trusted (Доверенные)

ПОЛЕ	ОПИСАНИЕ
Trusted User IP Range (Диапазон IP-адресов доверенных пользователей)	
From (От)	Введите IP-адрес компьютера локальной сети (или начальный IP-адрес конкретного диапазона компьютеров), который необходимо исключить из контент-фильтрования.
To (До)	Введите конечный IP-адрес конкретного диапазона пользователей локальной сети, которых необходимо исключить из контент-фильтрования. Оставьте это поле не заполненным, если необходимо исключить отдельный компьютер.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

Глава 13 Настройка удаленного управления

В этой главе предоставлена информация для настройки удаленного управления модемом.

13.1 Удаленное управление — общая информация

Функция удаленного управления позволяет определить, каким службам/протоколам разрешен доступ к интерфейсу управления интернет-центром (если таковые имеются), и с каких компьютеров.

При установке параметров конфигурации удаленного управления, предназначенного для реализации функций управления через глобальную вычислительную сеть (WAN), необходимо также настроить правило межсетевого экрана для получения доступа.

Возможны следующие варианты удаленного управления интернет-центром P–660HT/HTW EE:

- через глобальную сеть (Интернет)
- отовсюду (через локальную и глобальную сеть)
- только через локальную сеть
- отключение функции

Если Вы выберете **WAN only (только через глобальную сеть)** или **ALL (отовсюду)** (LAN & WAN (через локальную и глобальную сеть)), Вам все равно придется установить параметры правила межсетевого экрана для получения доступа.

Чтобы отключить удаленное управление конкретной службой, выберите **Disable (Отключить)** в соответствующем поле **Server Access (Доступ к серверу)**.

Одновременно допускается проведение только одного сеанса удаленного управления. Интернет-центр 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 Telnet

2 HTTP

13.1.1 Ограничения на удаленное управление

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

- Применен фильтр для блокировки службы Telnet, FTP или Web в меню SMT 3.1 (локальная сеть) или в меню 11.5 (глобальная сеть).
- 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 адресов интернет-центр немедленно разрывает сеанс управления.
- Уже выполняется другой сеанс удаленного управления, имеющий равный или более высокий приоритет. Одновременно допускается проведение только одного сеанса удаленного управления.
- Имеется правило межсетевого экрана, блокирующее удаленное управление.

13.1.2 Удаленное управление и NAT

При включении функции NAT:

- При настройке через глобальную сеть следует использовать IP-адрес интернет-центра в глобальной сети.
- При настройке через локальную сеть следует использовать IP-адрес интернет-центра в локальной сети.

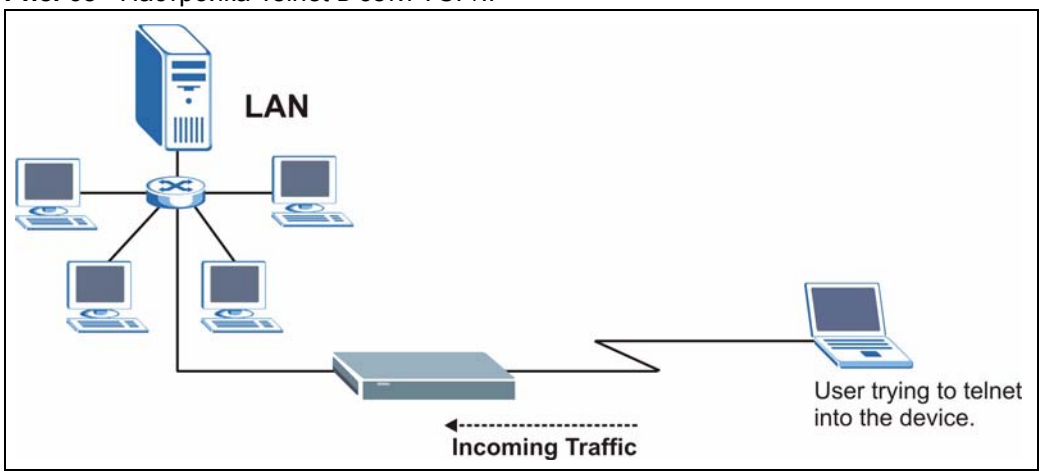
13.1.3 Время бездействия системы

Максимальное время бездействия системы во время сеанса управления по умолчанию установлено на 5 минут (300 секунд). Интернет-центр автоматически завершает сеанс управления при бездействии более этого периода. Сеанс управления не разрывается, если в окне статистики проводится опрос системы.

13.2 Управление с помощью Telnet

Можно настроить удаленный доступ к интернет-центру с использованием протокола Telnet, как показано ниже.

Рис. 68 Настройка Telnet в сети TCP/IP



13.3 FTP

Загрузка и выгрузка файлов микропрограммы и конфигурации интернет-центра производится с помощью протокола FTP. Для использования данной функции на компьютере должен быть установлен FTP-клиент.

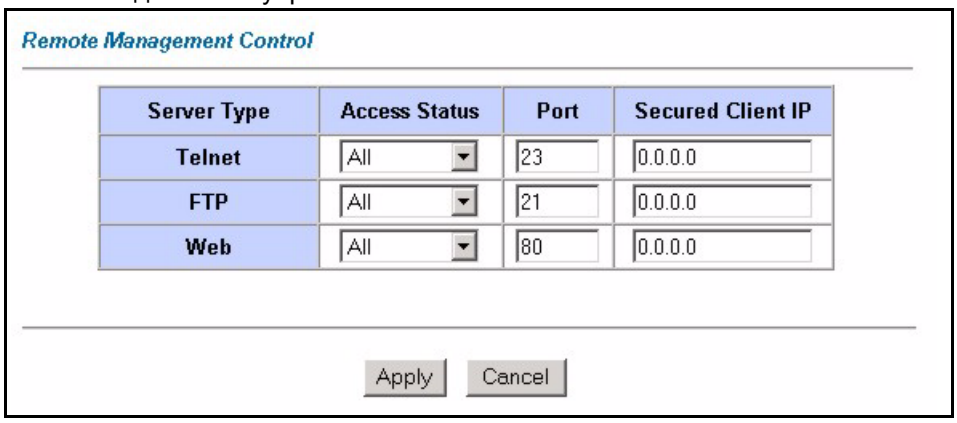
13.4 Web

Для настройки и управления файлами можно использовать встроенный Web-конфигуратор интернет-центра. Более подробную информацию см. во .

13.5 Настройка удаленного управления

Нажмите **Remote Management (Удаленное управление)** для отображения следующего окна. Более подробную информацию см. в Разд. 13.1 на с. 184.

Рис. 69 Удаленное управление



В следующей таблице даны описания полей этого окна.

Табл. 49 Удаленное управление

ПОЛЕ	ОПИСАНИЕ
Server Type (Тип сервера)	Каждое из этих полей определяет службу, которая может быть использована для удаленного управления интернет-центром.
Access Status (Состояние доступа)	Выберите состояние доступа. Вариантами являются **All (Через локальную и глобальную сеть)**, **LAN Only (Только через локальную сеть)**, **WAN Only (Только через глобальную сеть)** и **Disable (Отключить)**.
Port (Порт)	В данном поле отображается номер порта для службы удаленного управления. Вы можете изменить номер порта для службы в этом поле, но необходимо использовать этот же номер порта при использовании этой службы для удаленного управления.
Secured Client IP (IP-адрес доверенного клиента)	По умолчанию используется адрес 0.0.0.0, что позволяет любому клиенту использовать данную службу для удаленного управления интернет-центром. Введите IP-адрес, чтобы предоставить доступ к управлению только клиенту с совпадающим IP-адресом.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

Глава 14 Универсальная функция Plug and Play (UPnP)

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

14.1 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 подключаться к сети, получать IP-адрес, предоставлять свои ресурсы и собирать информацию о других устройствах сети. Кроме того, устройство может беспрепятственно и автоматически покидать сеть, если оно больше не используется.

Инструкции по настройке см. Разд. 14.2.1 на с. 189.

14.1.1 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. Выбор иконки устройства UPnP позволяет получить доступ к информации и свойствам данного устройства.

14.1.2 NAT Transversal

Функция NAT Transversal 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 Transversal 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.

14.1.3 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.

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

14.2 UPnP и ZyXEL

Корпорация ZyXEL получила сертификат UPnP от форума Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). Реализация UPnP ZyXEL поддерживает функцию IGD 1.0 (Internet Gateway Device — шлюзовое устройство подключения к Интернету). На момент написания документа реализация ZyXEL UPnP поддерживает Windows Messenger 4.6 и 4.7, а версии Windows Messenger 5.0 и Xbox находятся на стадии тестирования.

Широковещательные рассылки UPnP допускаются только внутри локальной сети.

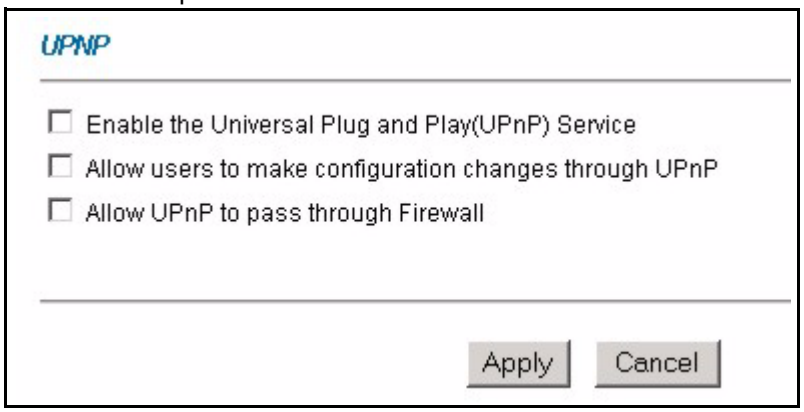
См. в следующих разделах примеры установки UPnP в Windows XP и Windows Me, а также примеры использования UPnP в Windows.

14.2.1 Настройка UPnP

В окне **Site Map (Карта сайта)** в главном меню нажмите **UPnP** в разделе **Advanced Setup (Дополнительная настройка)** для отображения представленного ниже окна.

Более подробную информацию см. в Разд. 14.1 на с. 188.

Рис. 70 Настройка UPnP



В следующей таблице даны описания полей этого окна.

Табл. 50 Настройка UPnP

ПОЛЕ	ОПИСАНИЕ
Enable the Universal Plug and Play (UPnP) Service (Включить службу UPnP)	Установите флажок в этом окошке для включения UPnP. Помните, что кто угодно может использовать приложение UPnP, чтобы открыть окно регистрации Web-конфигуратора, не вводя IP-адрес интернет-центра (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 флажок в этом окошке, чтобы разрешить приложениям UPnP автоматически настраивать интернет-центр с целью взаимодействия через него. Например, при использованием NAT Transversal, приложения UPnP автоматически резервируют порт переадресации NAT, чтобы иметь возможность взаимодействовать с другим устройством UPnP; это предотвращает необходимость ручной настройки переадресации портов для приложения UPnP.
Allow UPnP to pass through Firewall (Разрешить прохождение UPnP через межсетевой экран)	Поставьте галочку, если нужно разрешить прохождение трафика от приложений, использующих универсальные средства Plug&Play (UPnP) через межсетевой экран. Уберите галочку, если межсетевой экран должен блокировать все пакеты приложений на базе UPnP (например, пакеты MSN).
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

14.3 Пример установки UPnP в Windows

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

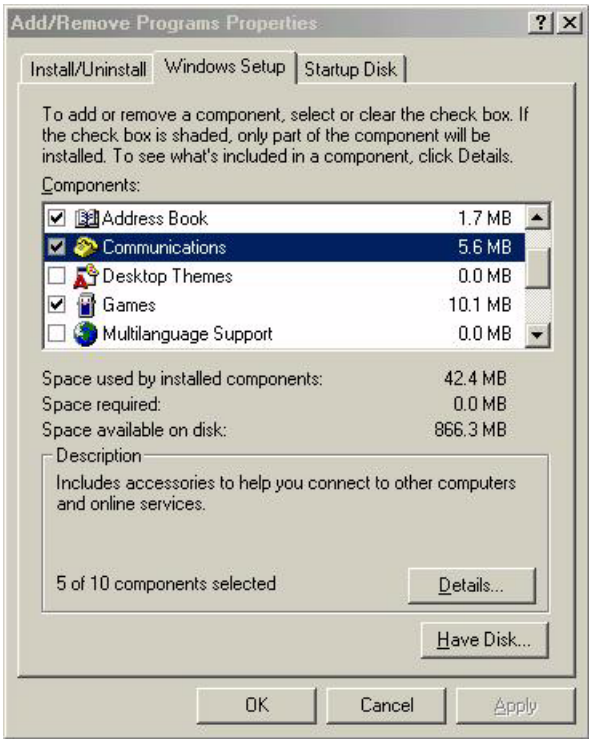
Установка UPnP в Windows Me

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)**.

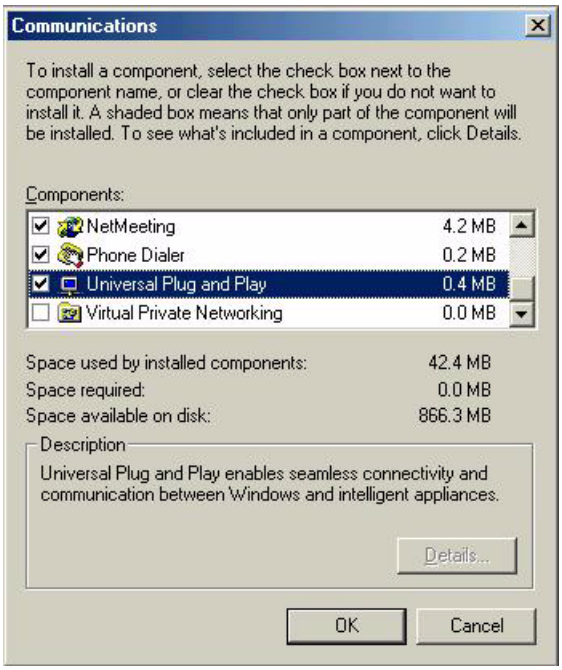
2 Выберите закладку **Windows Setup (Установка Windows)** и выберите **Communication (Связь)** в поле **Components (Компоненты)**. Нажмите **Details (Состав)**.

Рис. 71 Установка и удаление программ: Установка Windows: Связь



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

Рис. 72 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.

Установка UPnP в Windows XP

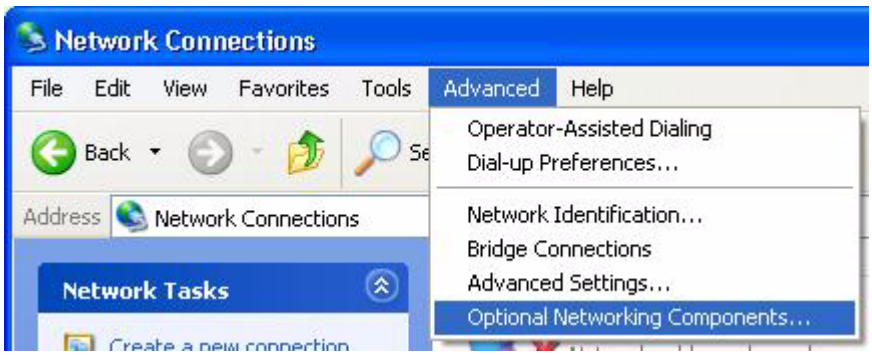
Выполните следующие действия для установки UPnP в Windows XP.

1 Нажмите **Start (Пуск)**, **Control Panel (Панель управления)**.

2 Дважды щелкните на **Network Connections (Сетевые подключения)**.

3 В окне **Network Connections (Сетевые подключения)** выберите **Advanced (Дополнительно)** в главном меню и выберите **Optional Networking Components … (Дополнительные сетевые компоненты...)**.

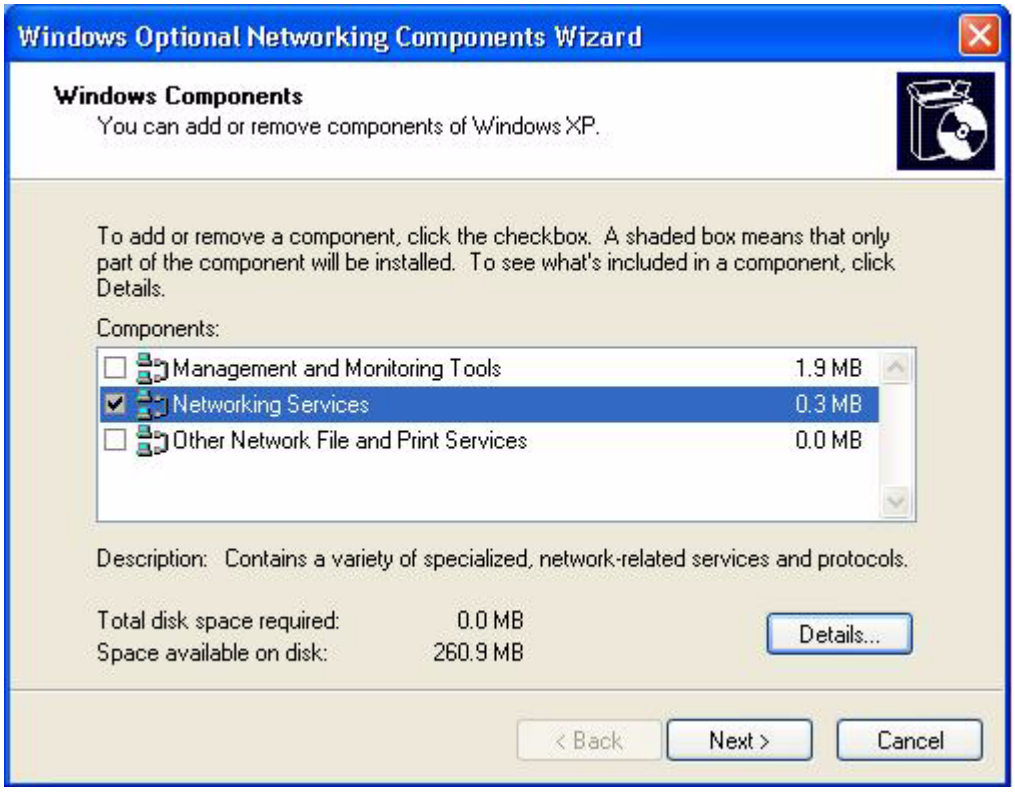
Рис. 73 Сетевые подключения



4 Появляется окно **Windows Optional Networking Components Wizard (Мастер установки дополнительных сетевых компонентов Windows)**. Выберите

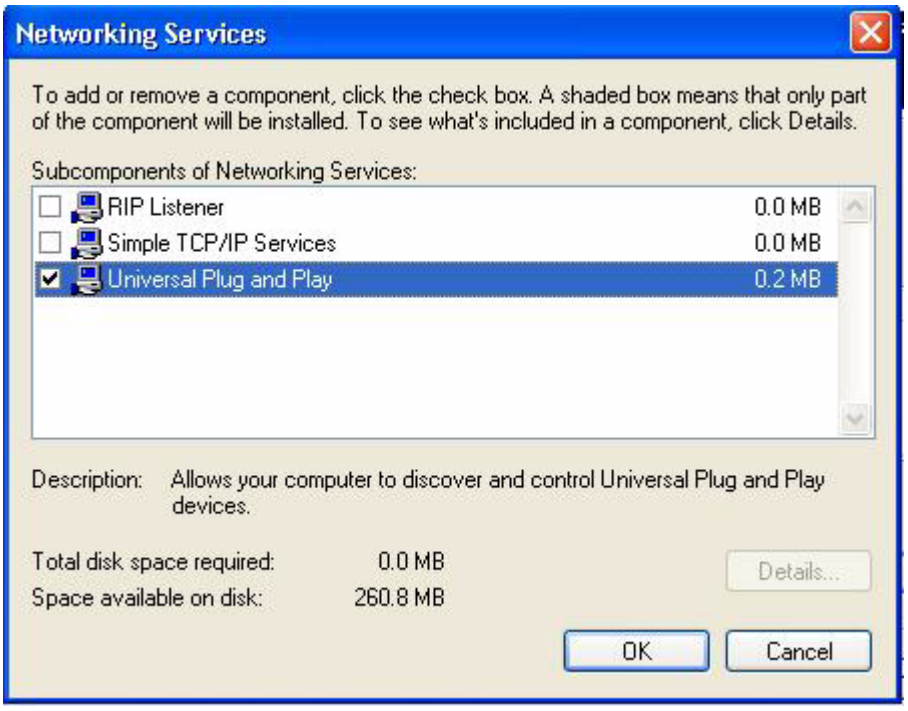
Networking Services (Сетевые службы) в поле **Components (Компоненты)** и нажмите **Details (Состав)**.

Рис. 74 Мастер установки дополнительных компонентов Windows



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

Рис. 75 Сетевые службы



6 Нажмите **OK** для возврата в окно **Windows Optional Networking Component Wizard (Мастер установки дополнительных сетевых компонентов Windows)** и нажмите **Next (Далее)**.

14.4 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 интернет-центре.

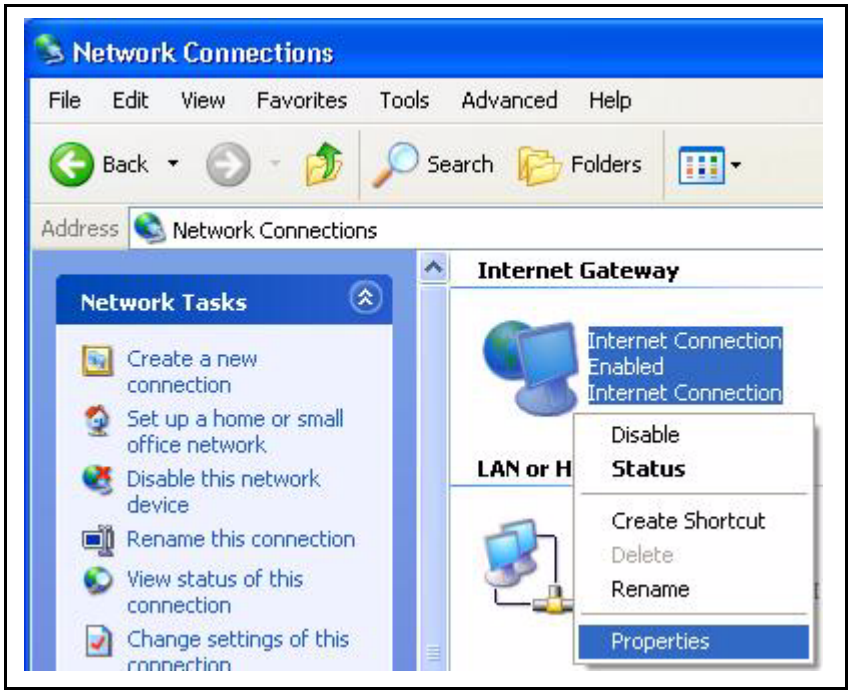
Убедитесь, что компьютер подключен к порту LAN интернет-центра. Включите компьютер и интернет-центр.

Автоматическое обнаружение сетевого устройства UPnP

1 Нажмите **Start (Пуск)**, **Control Panel (Панель управления)**. Дважды щелкните по иконке **Network Connections (Сетевые подключения)**. В разделе Internet Gateway (Шлюз в Интернет) отображается иконка.

2 Щелкните правой кнопкой мыши на этой иконке и выберите **Properties (Свойства)**.

Рис. 76 Сетевые подключения



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

Рис. 77 Internet Connection Properties (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. 78 Internet Connection Properties (Свойства подключения к Интернет): Advanced Settings (Дополнительные настройки)

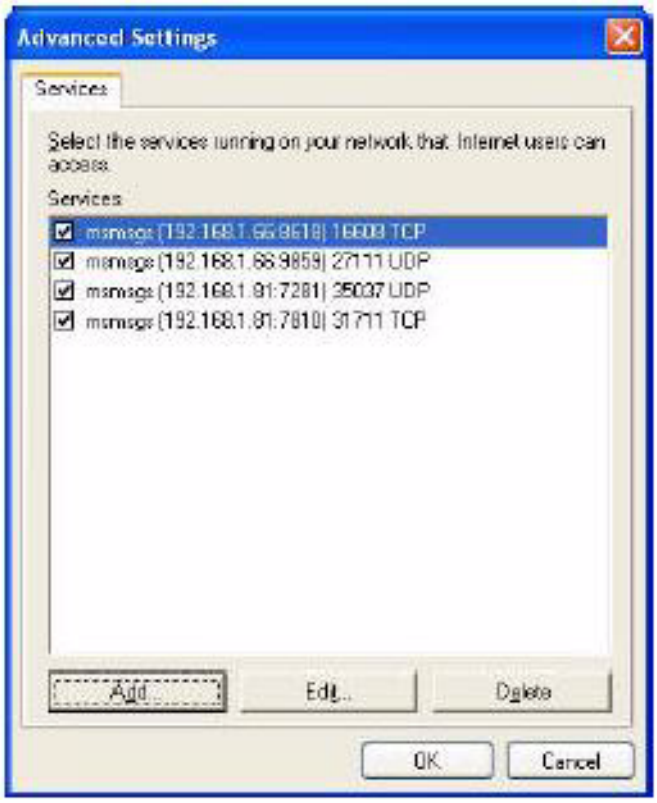
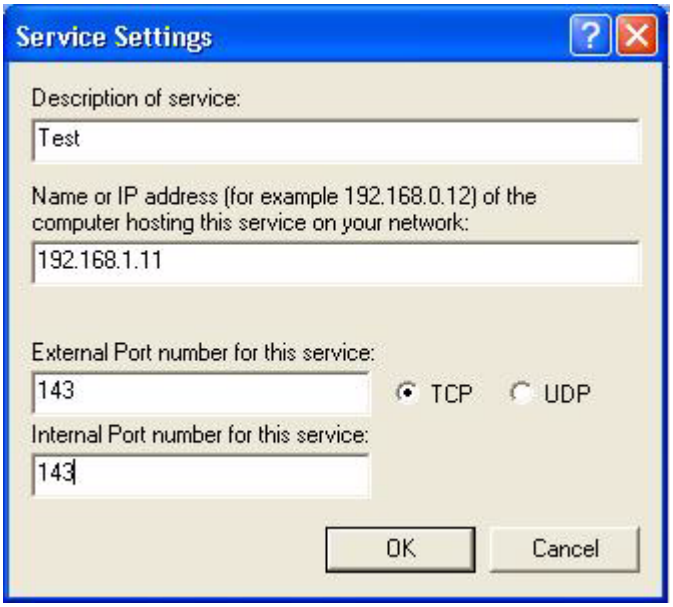


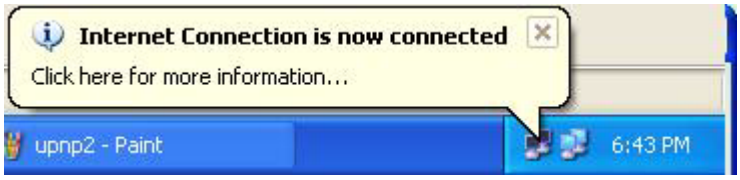
Рис. 79 Internet Connection Properties (Свойства подключения к Интернет): Advanced Settings (Дополнительные настройки): Add (Добавить)



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

6 Выберите **Show icon in notification area when connected (При подключении вывести значок в области уведомлений)** и нажмите **OK**. В области уведомлений (на панели задач) отображается значок.

Рис. 80 Значок в области уведомлений (на панели задач)



7 Дважды щелкните по иконке для отображения текущего состояния подключения к Интернету.

Рис. 81 Состояние подключения к Интернет

Простой доступ к Web-конфигуратору

С помощью UPnP вы можете получить доступ к конфигуратору интернет-центра через графический web-интерфейс без указания IP-адреса устройства. Это может оказаться полезным, если вы не знаете IP-адрес интернет-центра.

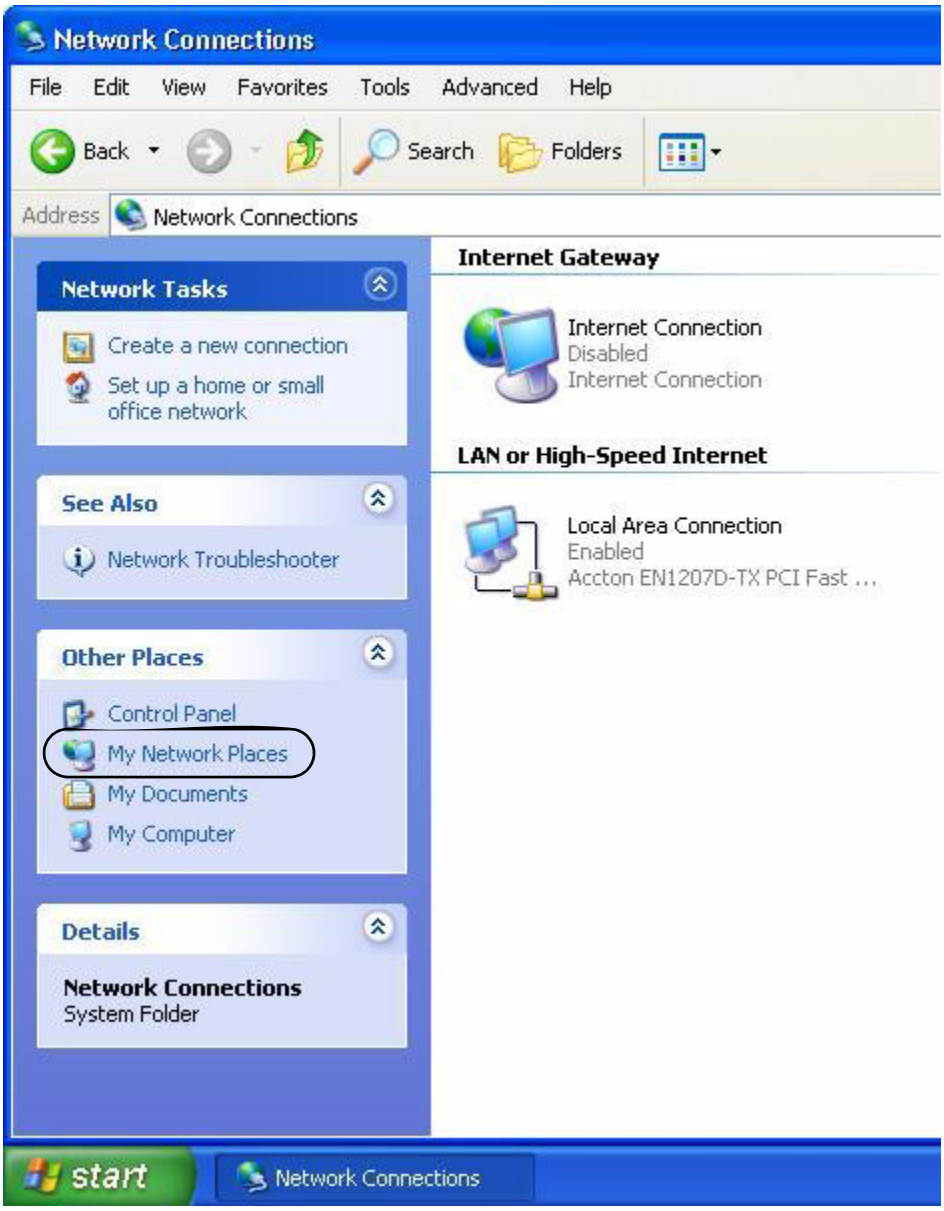
Выполните следующие действия для доступа к Web-конфигуратору.

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)**.

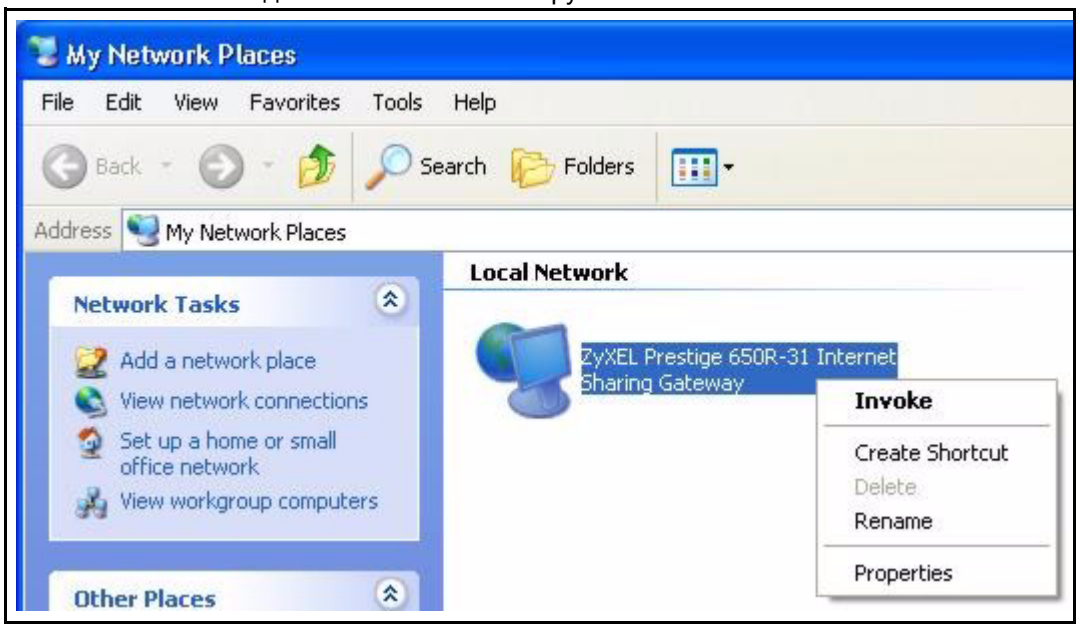
Рис. 82 Сетевые подключения



4 В разделе **Local Network (Локальная сеть)** для каждого UPnP-совместимого устройства отображается иконка с описанием.

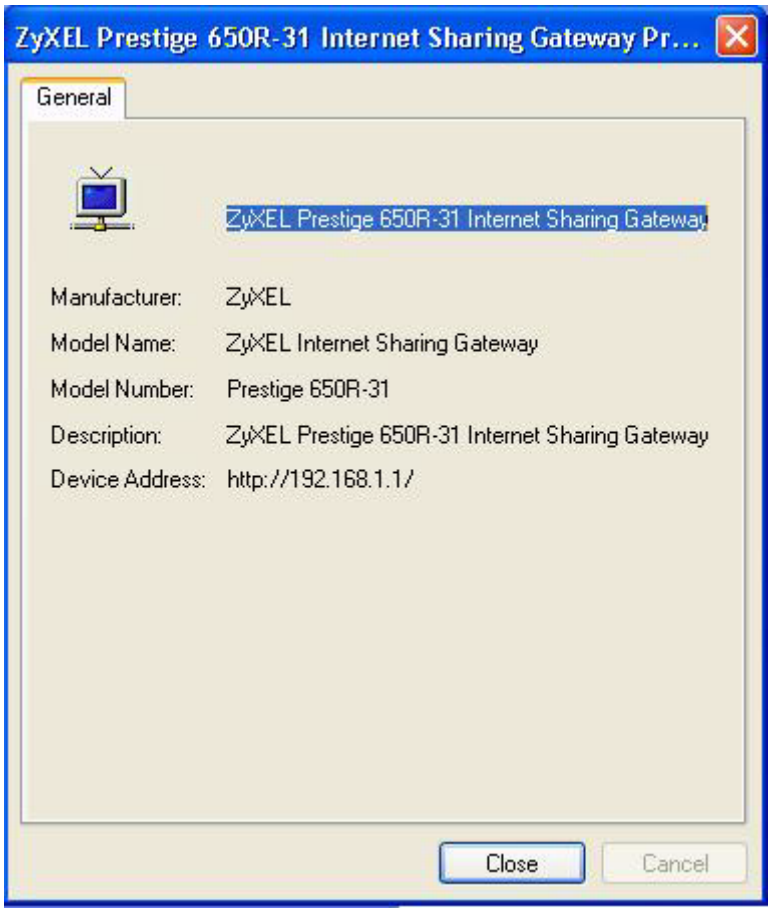
5 Щелкните правой кнопкой мыши на иконке интернет-центра и выберите **Invoke (Запуск)**. Появится окно регистрации Web-конфигуратора.

Рис. 83 Сетевые подключения: Сетевое окружение



6 Щелкните правой кнопкой мыши на иконке интернет-центра и выберите **Properties (Свойства)**. Появится окно свойств с основной информацией о интернет-центре.

Рис. 84 Сетевые подключения: Сетевое окружение: Свойства: Пример



Глава 15
Экраны регистрационных журналов

В этой главе описана настройка общих параметров регистрационных журналов и порядок просмотра журналов интернет-центра P–660HT/HTW EE. Примеры журнальных сообщений приведены в Приложении.

15.1 Регистрационные журналы — общие сведения

Web-конфигуратор позволяет выбрать категории событий и/или предупреждений, которые интернет-центр должен регистрировать, а затем отображать либо отправлять администратору (в виде сообщений электронной почты) или на сервер системных журналов.

15.1.1 Предупреждения и журнальные записи

Предупреждение — это тип журнальной записи, требующий серьезного внимания. К предупреждениям относятся сообщения о системных ошибках, атаках (управление доступом) и попытках доступа к заблокированным сайтам. Некоторые категории, такие как **System Errors (Системные ошибки)** состоят как из журнальных записей, так и предупреждений. Вы можете различить их по цвету в окне **View Log (Просмотр журнала)**. Предупреждения отображаются красным цветом, а обычные журнальные записи — черным.

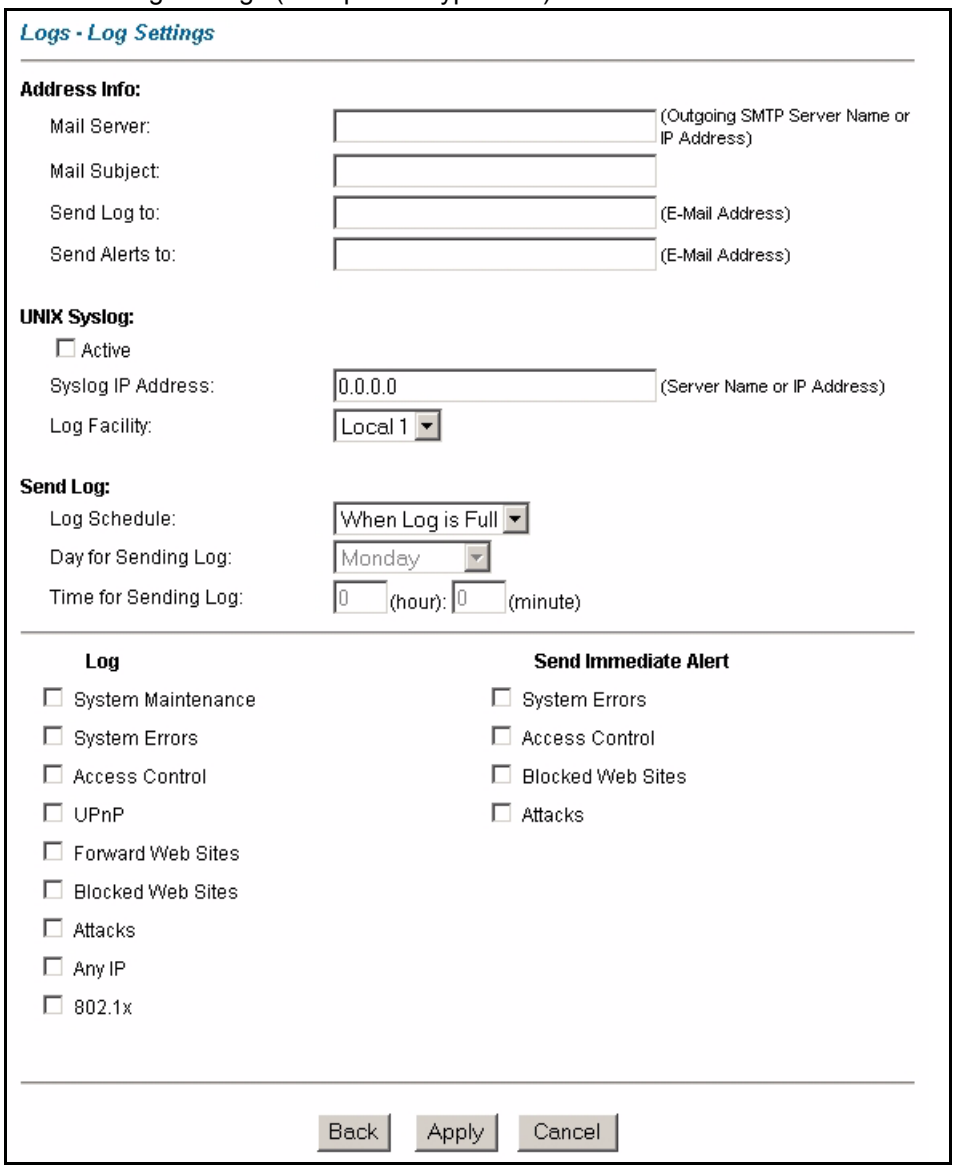
15.2 Настройка параметров журнала

В окне **Log Settings (Настройки журналов)** Вы можете указать, куда интернет-центр должен отправлять журнальные записи, график отправки записей, а также то, какие сообщения и/или немедленные предупреждения интернет-центр должен регистрировать. Более подробную информацию см. в Разд. 15.1 на с. 202.

Для изменения настроек интернет-центра, связанных с регистрацией, сообщений нажмите **Logs (Журналы)**, затем **Log Settings (Настройки журналов)**. При этом откроется показанное ниже окно.

Предупреждения отправляются адресату непосредственно в момент их появления. Журнальные записи отправляются по мере заполнения журнала. Выбор большого количества категорий предупреждений и/или журнальных записей (особенно это касается **Управления доступом**) может привести к тому, что будет рассылаться большое количество сообщений электронной почты.

Рис. 85 Log Settings (Настройки журналов)



В следующей таблице даны описания полей этого окна.

Табл. 51 Log Settings (Настройки журналов)

ПОЛЕ	ОПИСАНИЕ
Address Info (Информация об адресе)	
Mail Server (Почтовый сервер)	Введите имя сервера или IP-адрес почтового сервера для указанных ниже адресов электронной почты. Если не заполнять это поле, журнал и предупреждающие сообщения не будут высылаться по электронной почте.
Mail Subject (Тема сообщения)	Введите заголовок, который Вы хотите поместить в строку "Тема" (subject) отправляемого сообщения электронной почты.
Send log to (Адресаты журнальных записей)	Журнальные записи отправляются на адреса электронной почты, указанные в этом поле. Если не заполнять это поле, то журнальные записи не будут высылаться по электронной почте.

Табл. 51 Log Settings (Настройки журналов)

ПОЛЕ	ОПИСАНИЕ
Send alerts to (Адресаты предупреждений)	Предупреждения отправляются на адреса электронной почты, указанные в этом поле. Если не заполнять это поле, то предупреждения не будут высылаться по электронной почте.
UNIX Syslog (Системный журнал UNIX)	Записи системного журнала отправляются на внешний сервер системных журналов, предназначенный для хранения сообщений.
Active (Активировать)	Для активации системного журнала нажмите кнопку **Active (Активировать)**.
Syslog IP Address (IP-адрес сервера системных журналов)	Введите имя сервера или IP-адрес сервера системных журналов, который будет регистрировать выбранные категории сообщений.
Log Facility (Размещение журнала)	Из раскрывающегося списка выберите место, где будут храниться журнальные записи. Эта функция дает возможность регистрировать сообщения в различных файлах на сервере системных журналов. Более подробная информация приведена в документации к программе системных журналов.
Send Log (Отправка журнальных записей)	
Log Schedule (План журнальной регистрации)	В этом раскрывающемся меню выбирается частота рассылки журнальных записей по электронной почте: • Daily (Ежедневно) • Weekly (Еженедельно) • Hourly (Каждый час) • When Log is Full (По заполнении журнала) • None (Никогда). При выборе опции **Weekly (Еженедельно)** или **Daily (Ежедневно)** необходимо указать время дня для рассылки e-mail сообщений. При выборе опции **Weekly (Еженедельно)** также необходимо указать день недели для рассылки сообщений. При выборе опции **When Log is Full (По заполнении журнала)** сообщение посылается только при условии, что журнал заполнен. При выборе **None (Отключить)** сообщения не высылаются.
Day for Sending Log (День рассылки журнальных записей)	Из раскрывающегося списка выберите день недели, в который должны отправляться записи.
Time for Sending Log (Время рассылки журнальных записей)	Введите время отправки журнальных записей в 24-часовом формате (например, 23:00 для 11 часов вечера).
Log (Регистрационный журнал)	Выберите категории журнальных записей, которые необходимо регистрировать. К журнальным записям относятся и предупреждающие сообщения.
Send Immediate Alert (Отправить предупреждение немедленно)	Выберите категории предупреждений, которые интернет-центр должен немедленно отсылать на адрес электронной почты, указанный в поле **Send Alerts To (Адресаты предупреждений)**.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.

Табл. 51 Log Settings (Настройки журналов)

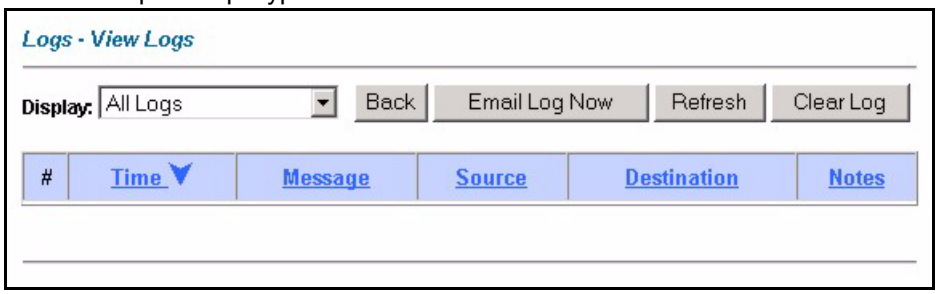
ПОЛЕ	ОПИСАНИЕ
Apply (Применить)	Нажмите кнопку **Apply**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

15.3 Отображение журнальных записей

Нажмите кнопку **Logs (Журналы)** и затем **View Log (Просмотр журнала)**, при этом откроется окно **View Logs (Просмотр журналов)**. В окне **View Logs** можно посмотреть журнальные записи по категориям, выбранным Вами в окне **Log Settings (Настройки журналов)** (см. Разд. 15.2 на с. 202).

Записи, выделенные красным цветом, означают предупреждения. Если журнал заполнен, самые старые журнальные записи стираются по мере добавления новых. Щелкните по заголовку столбца для сортировки записей. Треугольник показывает возрастающий или убывающий порядок сортировки.

Рис. 86 Просмотр журналов



В следующей таблице даны описания полей этого окна.

Табл. 52 Просмотр журналов

ПОЛЕ	ОПИСАНИЕ
Display (Отобразить)	Категории, выбранные Вами в окне **Log Settings (Настройки журналов)** отобразятся в раскрывающемся списке. Выберите категорию записей для просмотра. Чтобы посмотреть все категории записей, выбранные Вами в окне **Log Settings (Настройки журналов)**, выберите опцию **All Logs (Все записи)**.
Time (Время)	В этом поле отображается время, когда была зарегистрирована запись.
Message (Сообщение)	В этом поле приводится причина внесения записи в журнал.
Source (Источник)	В этом поле указываются IP-адрес источника и номер порта входящего пакета.
Destination: (Получатель:)	В этом поле указываются IP-адрес получателя и номер порта входящего пакета.

Табл. 52 Просмотр журналов

ПОЛЕ	ОПИСАНИЕ
Notes (Примечания)	В этом поле выводится дополнительная информация о регистрационной записи.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Email Log Now (Отправить журнал по e-mail)	Нажмите **Email Log Now (Отправить журнал по электронной почте)** для отправки журнала на адрес электронной почты, указанный в окне **Log Settings (Настройки журналов)** (в окне сначала нужно заполнить поле **Address Info (Информация об адресе)**).
Refresh (Обновить)	Нажмите **Refresh (Обновить)** для обновления экрана регистрационных записей.
Clear Log (Удалить записи)	Нажмите **Clear Log (Удалить записи)** для удаления всех регистрационных записей из журнала.

15.4 Сообщения об ошибках SMTP

При возникновении каких-либо трудностей при отправке электронной почты появляются следующие сообщения об ошибках.

Сообщение об ошибках E-mail появляются в меню SMT 24.3.1 в виде "SMTP action request failed. ret= ??". Значения “??" приводятся в следующей таблице.

Табл. 53 Сообщения об ошибках SMTP

-1 означает, что интернет-центр отключен от сети
-2 означает ошибку tcp SYN fail
-3 означает ошибку smtp server OK fail
-4 означает ошибку HELO fail
-5 означает ошибку MAIL FROM fail
-6 означает ошибку RCPT TO fail
-7 означает ошибку DATA fail
-8 означает ошибку mail data send fail

15.4.1 Пример журнала, высылаемого по электронной почте

Сообщение "End of Log" (Конец журнала) появляется каждый раз, когда отправляется полностью заполненный журнал. Ниже приводится пример журнала, посланного по электронной почте.

- Разрешено редактировать заглавие объекта.
- Ввод даты в формате День-Месяц-Год.
- Ввод даты в формате Месяц-День-Год. Ввод времени в формате Часы-Минуты-Секунды.

- Сообщение "`End of Log (Конец журнала)`" означает, что отправлен весь журнал.

Рис. 87 Пример журнала, высылаемого по E-mail

```
Subject:
        Firewall Alert From Prestige
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

Глава 16
Расширенная настройка управления пропускной способностью

В этой главе описано управление пропускной способностью с одним производным классом.

16.1 Управление пропускной способностью среды передачи — общая информация

Управление пропускной способностью позволяет разбить исходящий трафик порта на отдельные типы. Также можно настроить интернет-центр на переадресацию определенных типов трафика (особенно для приложений реального времени) с минимальными задержками. С распространением приложений реального времени, таких как передача голоса по IP-протоколу, (VoIP) увеличиваются и требования к распределению пропускной способности.

Управление пропускной способностью поднимает следующие вопросы:

- Кто получает доступ к тем или иным приложениям и в каком объеме?
- Какой уровень приоритетности следует присваивать каждому типу трафика?
- Какой трафик должен иметь гарантированную доставку?
- Какую пропускную способность следует задать, чтобы гарантировать доставку?

Управление пропускной способностью также позволяет задать разрешенный объем исходящего трафика для того или иного порта на основе пропускной способности сети. Это помогает снизить задержки и количество удаляемых пакетов на следующем маршрутизаторе. Например, можно установить скорость порта WAN равной 1000 кбит/с, если подключение по ADSL имеет скорость исходящего потока 1 Мбит/с. Во всех окнах настройки скорость передачи данных указана в кбит/с (килобит в секунду), однако для краткости в данном Руководстве пользователя используются и Мбит/с (мегабиты в секунду).

Активирование и настройка пропускной способности для различных портов — см. Разд. 16.9 на с. 218.

Настройка классов пропускной способности — см. Разд. 16.10 на с. 219.

Информация об использовании пропускной способности — см. Разд. 16.11 на с. 225.

16.2 Классы и фильтры пропускной способности

Используйте классы и подклассы пропускной способности для распределения пропускной способности (бюджетов пропускной способности). Настройте фильтр пропускной способности, чтобы определить класс или подкласс пропускной способности на основе того или иного приложения и/или подсети. В окне **Class Configuration (Параметры класса)** (см. Разд. 16.10 на с. 219) можно указать имя класса пропускной способности, квоту и фильтр для пропускной способности. Можно настроить один фильтр для каждого класса пропускной способности. Также можно настроить классы пропускной способности без фильтров. Однако для всех классов, настраиваемых без фильтров, рекомендуется настраивать подклассы с фильтрами. Для классов, не имеющих фильтров или подклассов с фильтрами интернет-центр оставляет бюджет пропускной способности зарезервированным и неиспользованным. Посмотреть настроенные классы и подклассы пропускной способности можно в окне **Class Setup** (см. Разд. 16.10 на с. 219).

Общая сумма бюджетов пропускной способности подклассов не может превышать бюджета пропускной способности исходного класса.

16.3 Пропорциональное распределение пропускной способности

Управление пропускной способностью позволяет определить, какую долю пропускной способности получит каждый класс; однако фактическая пропускная способность для каждого класса увеличивается либо уменьшается пропорционально существующей пропускной способности.

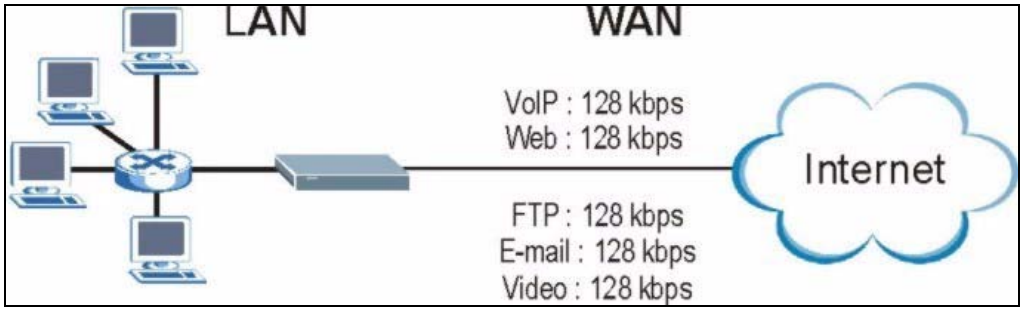
16.4 Примеры управления пропускной способностью

Дальнейшие примеры демонстрируют распределение пропускной способности для порта WAN, настроенного на 640 кбит/с.

16.4.1 Управление пропускной способностью на основе приложения

Классы пропускной способности в приведенном ниже примере связаны только с приложениями. На каждый класс пропускной способности (VoIP, Web, FTP, E-mail и Video) выделяется по 128 кбит/с.

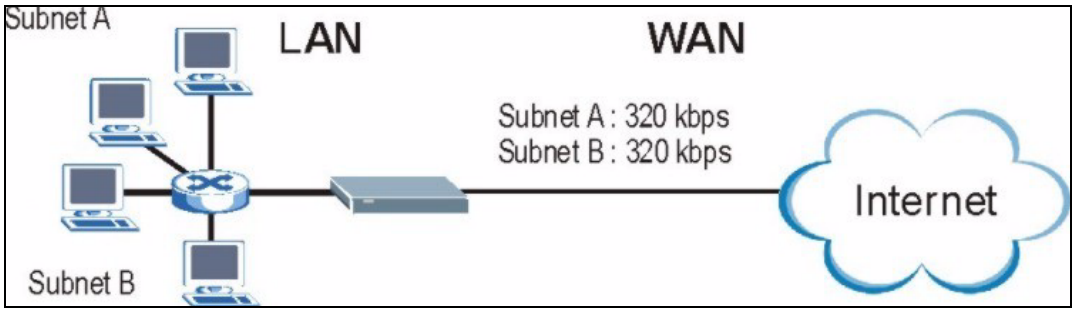
Рис. 88 Пример управления пропускной способностью на основе приложения



16.4.2 Управление пропускной способностью на основе подсети

Классы пропускной способности в приведенном ниже примере связаны только с подсетями локальной сети. На каждый класс пропускной способности (подсеть A и подсеть B) выделено по 320 кбит/с.

Рис. 89 Пример управления пропускной способностью на основе подсети



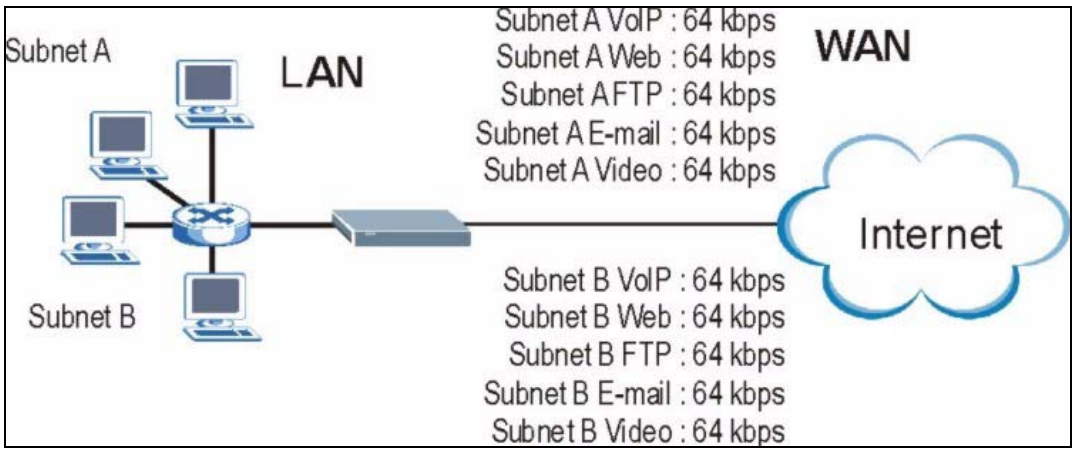
16.4.3 Управление пропускной способностью на основе приложения и подсети

В приведенном ниже примере используются классы пропускной способности на основе подсетей LAN и приложений (отдельным приложениям в каждой подсети выделяется определенная доля пропускной способности).

Табл. 54 Пример управления пропускной способностью на основе приложения и подсети

ТИП ТРАФИКА	ИЗ ПОДСЕТИ A	ИЗ ПОДСЕТИ B
VoIP	64 кбит/с	64 кбит/с
Web	64 кбит/с	64 кбит/с
FTP	64 кбит/с	64 кбит/с
E-mail	64 кбит/с	64 кбит/с
Video	64 кбит/с	64 кбит/с

Рис. 90 Пример управления пропускной способностью на основе приложения и подсети



16.5 Планировщик

Планировщик распределяет пропускную способность порта между классами пропускной способности. Модель P–660HT/HTW EE имеет два типа планировщиков: один — на основе равномерного распределения, другой — на основе приоритетов.

16.5.1 Планировщик на основе приоритетов

При использовании планировщика, работающего на основе приоритетов, интернет-центр пересылает трафик классов пропускной способности в соответствии с заданными приоритетами. Чем больше значение приоритета у того или иного класса, тем выше его приоритет. Для обеспечения более надежной работы, приложениям реального времени (где используется аудио или видео) следует присваивать большие приоритеты.

16.5.2 Планировщик на основе равномерного распределения

При использовании планировщика, работающего по принципу равенства приоритетов, интернет-центр распределяет пропускную способность между классами пропускной способности равномерно и, таким образом, предотвращает использование одним классом всей пропускной способности порта.

16.6 Увеличение использования пропускной способности

Функция увеличения использования пропускной способности (см. Разд. 16.7.1 на с. 216) позволяет интернет-центру распределять имеющуюся пропускную способность порта (в т.ч. незарезервированную и зарезервированную, но не используемую) между классами пропускной способности, требующими увеличения пропускной способности.

При включении этой опции интернет-центр сначала проверяет, получил ли каждый класс пропускной способности свою долю пропускной способности. Затем интернет-центр делит имеющуюся пропускную способность порта (небюджетированную либо неиспользованную классами) в зависимости от количества классов, требующих увеличения пропускной способности, и от уровней их приоритетов. Если дополнительная пропускная способность нужна только одному классу, то интернет-центр выделяет ее этому классу.

Когда дополнительная пропускная способность требуется нескольким классам, интернет-центр предоставляет имеющуюся пропускную способность сначала классамс более высоким приоритетом (столько, сколько им нужно, если достаточно имеющейся пропускной способности), а затем — классам с более низким приоритетом, если резерв пропускной способности еще имеется. Интернет-центр равномерно распределяет имеющуюся пропускную способность между классами с одинаковым уровнем приоритетов.

16.6.1 Резервирование пропускной способности для трафика, не относящегося к классам пропускной способности

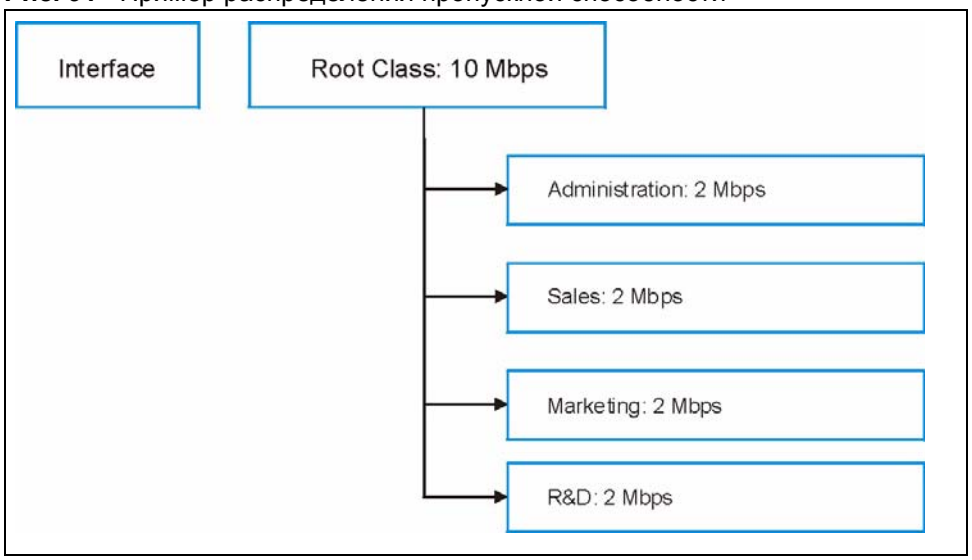
Чтобы интернет-центр выделял пропускную способность трафику, не указанному в фильтре, проделайте следующие три шага.

1. Оставьте часть пропускной способности порта нераспределенной.
2. Не включайте опцию **Maximize Bandwidth Usage (Увеличение использования пропускной способности)**.
3. Не активируйте заимствование пропускной способности для подклассов, исходным классом которых является корневой класс (см. Разд. 16.7 на с. 216).

16.6.2 Пример увеличения использования пропускной способности

Приведем пример того, как интернет-центр увеличивает использование пропускной способности, разрешенное для данного порта. На первом рисунке показаны бюджеты и приоритеты каждого класса пропускной способности. Классы построены на основе подсетей. Пропускная способность порта составляет 10 Мбит/с. Каждой подсети выделено по 2 Мбит/с. Небюджетированные 2 Мбит/с позволяют выпускать трафик, не определенный ни в одном фильтре, если не активировано увеличение пропускной способности.

Рис. 91 Пример распределения пропускной способности

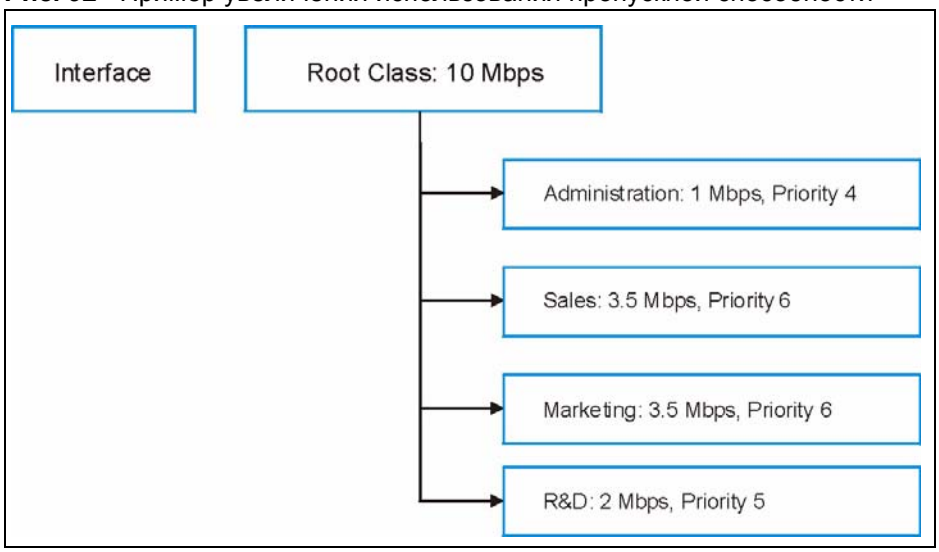


На представленном ниже рисунке показано распределение пропускной способности при активированном увеличении ее использования. Интернет-центр распределяет оставшиеся 2 Мбит/с между классами, требующими большей пропускной способности. Если административный отдел будет использовать лишь 1 Мбит/с из выделенных ему 2 Мбит/с, то интернет-центр также распределит оставшиеся 1 Мбит/с между классами, которым требуется дополнительная пропускная способность. Поэтому интернет-центр распределит между классами, испытывающими недостаток пропускной способности, в общей сложности 3 Мбит/с из небюджетированной и неиспользуемой пропускной способности.

Предположим, что в этом случае в дополнительной пропускной способности нуждаются все классы, за исключением класса "Администрация".

- Каждый класс получает свою запланированную долю пропускной способности (т.н. бюджет). Администрация использует лишь 1 Мбит/с из запланированных 2 Мбит/с.
- Отделы продаж и маркетинга получат дополнительную пропускную способность первыми, поскольку имеют наивысший приоритет (6). Если обоим отделам нужно дополнительно по 1,5 Мбит/с и более, то интернет-центр распределит 3 Мбит/с небюджетированной и неиспользованной пропускной способности равномерно между ними (плюс 1,5 Мбит/с каждому отделу, в общей сложности 3,5 Мбит/с), поскольку оба отдела имеют наивысший уровень приоритетов.
- Отделу R&D тоже требуется дополнительная пропускная способность, однако он получает лишь запланированные 2 Мбит/с, так как вся небюджетированная и неиспользованная пропускная способность выделяется отделам продаж и маркетинга, имеющим более высокий приоритет.
- Интернет-центр не отправляет трафик, не определенный в фильтрах пропускной способности, так так вся небюджетированная пропускная способность выделяется классам, испытывающим потребность в ней.

Рис. 92 Пример увеличения использования пропускной способности



16.7 Заимствование пропускной способности

Функция заимствования пропускной способности позволяет подклассам забирать неиспользуемую пропускную способность у своего исходного класса, в то время как увеличение использования пропускной способности позволяет классам пропускной способности забирать любую неиспользованную или небюджетированную пропускную способность порта.

Чтобы подклассы могли воспользоваться неиспользуемой пропускной способностью своего исходного класса, активируйте заимствование пропускной способности для подклассов. Неиспользуемая пропускная способность исходного класса сначала предоставляется подклассу с наивысшим приоритетом.

Общая сумма бюджетов пропускной способности подклассов не может превышать бюджета пропускной способности исходного класса. Для распределения неиспользуемой пропускной способности исходного класса между подклассами интернет-центр использует планировщик.

16.7.1 Увеличение использования пропускной способности с заимствованием пропускной способности

Если Вы активируете и увеличение использования пропускной способности (для порта), и заимствование пропускной способности (для отдельных подклассов), то интернет-центр будет работать следующим образом.

1. Интернет-центр отправляет трафик согласно бюджетам каждого класса пропускной способности.
2. Интернет-центр выделяет неиспользуемую пропускную способность исходного класса его подклассам, имеющим больше трафика, чем было запланировано, для

которых активировано заимствование пропускной способности. Интернет-центр отдает приоритет более приоритетным подклассам и одинаково относится к подклассам равной приоритетности.

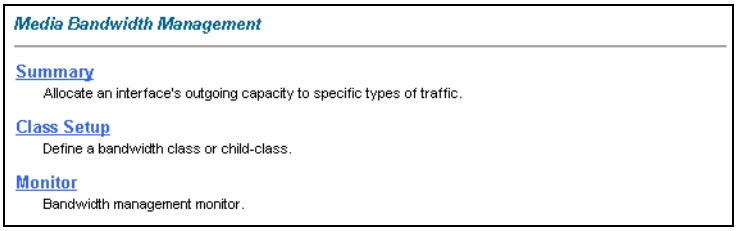
3 Интернет-центр выделяет оставшуюся неиспользуемую или небюджетированную пропускную способность порта любому классу, которому она требуется. Интернет-центр отдает приоритет более приоритетным классам и одинаково относится к классам равной приоритетности.

4 Интернет-центр выделяет оставшуюся небюджетированную пропускную способность трафику, не соответствующему ни одному из классов.

16.8 Главное окно управления пропускной способностью среды передачи

Нажмите кнопку **Media Bandwidth Mgnt. (Управление пропускной способностью среды передачи)**, при этом откроется показанное ниже окно **Media Bandwidth Management** .

Рис. 93 Media Bandwidth Mgnt (Управление пропускной способностью среды передачи)



В следующей таблице даны описания ссылок в этом окне.

Табл. 55 Media Bandwidth Mgnt (Управление пропускной способностью среды передачи)

ССЫЛКА	ОПИСАНИЕ
Summary (Общие настройки)	Щелкните по этой ссылке, чтобы открыть окно, где можно активировать управление пропускной способностью порта и установить максимальную пропускную способность для этого порта.
Class Setup (Настройка классов пропускной способности)	Щелкните по этой ссылке для перехода к окну настройки классов пропускной способности.
Monitor (Монитор)	Щелкните по этой ссылке для перехода к окну просмотра использования пропускной способности.

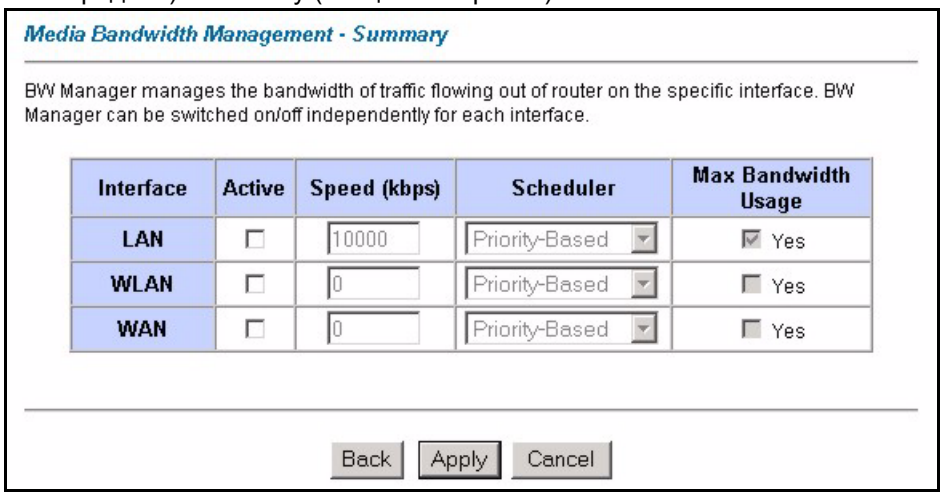
16.9 Настройка — окно "Общие настройки"

Нажмите кнопку **Media Bandwidth Management (Управление пропускной способностью среды передачи)**, **Summary (Общие настройки)**, при этом откроется показанное ниже окно.

Активируйте управление пропускной способностью порта и установите максимально допустимую пропускную способность для данного порта.

Более подробную информацию см. в Разд. 16.1 на с. 210.

Рис. 94 Media Bandwidth Management (Управление пропускной способностью среды передачи): Summary (Общие настройки)



В следующей таблице даны описания полей этого окна.

Табл. 56 Media Bandwidth Management (Управление пропускной способностью среды передачи): Summary (Общие настройки)

ПОЛЕ	ОПИСАНИЕ
LAN (ЛВС) WLAN (Беспроводная ЛВС) WAN (Глобальная сеть)	Эти поля "только для чтения" обозначают физические порты. Для включения управления пропускной способностью того или иного порта поставьте галочку напротив его названия. Управление пропускной способностью применяется ко всему трафику, выходящему через порт маршрутизатора, независимо от источника этого трафика. Переадресация трафика или использование IP-псевдонимов может привести к тому, что трафик между локальными сетями будет проходить через интернет-центр и управляться системой управления пропускной способностью.
Active (Активировать)	Для включения управления пропускной способностью того или иного порта поставьте галочку напротив его названия.
Speed (kbps) (Скорость, кбит/с)	Введите пропускную способность данного порта, которую необходимо назначить с помощью управления пропускной способностью. Отображается в виде бюджета пропускной способности корневого класса порта. Рекомендуется установить скорость, соответствующую возможностям порта. Например, установите скорость порта WAN равной 10 000 кбит/с, если подключение по ADSL имеет скорость исходящего потока 10 Мбит/с.

Табл. 56 Media Bandwidth Management (Управление пропускной способностью среды передачи): Summary (Общие настройки) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Scheduler (Планировщик)	Из раскрывающегося меню выберите **Priority-Based (Согласно приоритетам)** или **Fairness-Based (На основе равномерного распределения)**. Опцию **Priority-Based** следует выбрать, если нужно отдать предпочтение более приоритетным классам. Выберите опцию **Fairness-Based**, если все классы должны иметь равные приоритеты.
Maximize Bandwidth Usage (Увеличение использования пропускной способности)	Отметьте эту опцию, если интернет-центр должен распределять всю нераспределенную и/или неиспользуемую пропускную способность порта между классами, которым требуется дополнительная пропускная способность. Не отмечайте опцию, если нужно зарезервировать пропускную способность для трафика, не подпадающего ни под один класс, или если необходимо ограничить скорость порта (см. описание поля **Speed (Скорость)**).
Back (Назад)	Нажмите **Back** для возврата в главное окно **Media Bandwidth Management**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

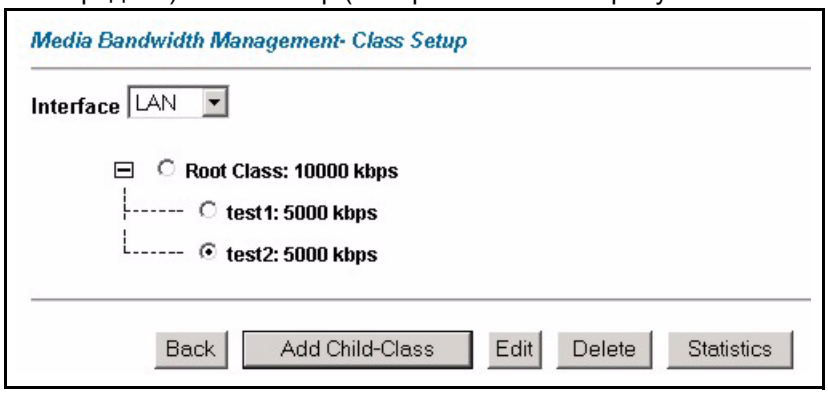
16.10 Настройка классов пропускной способности

В окне **Настройка классов пропускной способности** отображаются настроенные классы пропускной способности по отдельным портам. Выберите нужный порт и выполнените описанные ниже действия. Нажмите на “+”, чтобы раскрыть класс, или на “-“, чтобы спрятать дерево классов. У каждого порта имеется постоянный корневой класс. Бюджет пропускной способности корневого класса равен скорости, заданной для порта (настройка скорости порта — см. Разд. 16.9 на с. 218). Настройте уровни подклассов для корневого класса.

Более подробную информацию см. в Разд. 16.1 на с. 210.

Чтобы добавить или удалить подкласс того или иного порта, нажмите на **Media Bandwidth Management (Управление пропускной способностью среды передачи)**, затем на **Class Setup (Настройка классов пропускной способности)**. Откроется показанное ниже окно (с примерами классов).

Рис. 95 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Setup (Настройка классов пропускной способности)



В следующей таблице даны описания полей этого окна.

Табл. 57 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Setup (Настройка классов пропускной способности)

ПОЛЕ	ОПИСАНИЕ
Interface (Порт)	Из раскрывающегося списка выберите порт, для которого необходимо определить классы.
Back (Назад)	Нажмите **Back** для возврата в главное окно **Media Bandwidth Management**.
Add Child-Class (Добавить подкласс)	Нажмите кнопку **Add Child-class (Добавить подкласс)**, чтобы добавить подкласс.
Edit (Редактировать)	Чтобы настроить параметры выбранного класса, нажмите кнопку **Edit (Редактировать)**. Корневой класс редактировать нельзя.
Delete (Удалить)	Для удаления класса и всех его подклассов нажмите кнопку **Delete (Удалить)**. Корневой класс удалить нельзя.
Statistics (Статистика)	Для просмотра статуса выбранного класса нажмите кнопку **Statistics (Статистика)**.

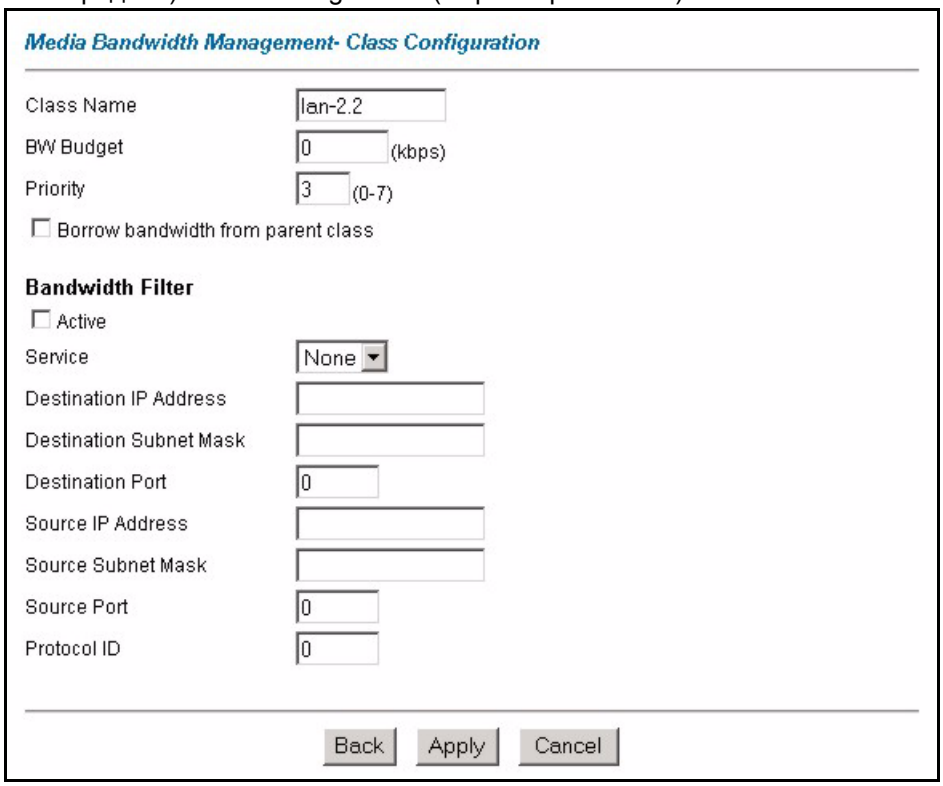
16.10.1 Управление пропускной способностью среды передачи — параметры класса

Настройка параметров класса пропускной способности производится в окне **Class Configuration (Параметры класса)**. Прежде чем настраивать классы для того или иного порта, необходимо активировать управление пропускной способностью этого порта в окне **Media Bandwidth Management — Summary (Управление пропускной способностью среды передачи — Общие настройки)**.

Более подробную информацию см. в Разд. 16.1 на с. 210.

Чтобы добавить подкласс, нажмите кнопку **Media Bandwidth Management (Управление пропускной способностью среды передачи)**, затем на **Class Setup (Настройка классов пропускной способности)**. Нажмите кнопку **Add Child-Class (Добавить подкласс)**, при этом откроется показанное ниже окно.

Рис. 96 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Configuration (Параметры класса)



В следующей таблице даны описания полей этого окна.

Табл. 58 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Configuration (Параметры класса)

ПОЛЕ	ОПИСАНИЕ
Class Name (Имя класса)	Используйте автоматически создаваемое имя или введите описательное имя длиной до 20 буквенно-цифровых символов, включая пробелы.
BW Budget (Бюджет пропускной способности) (кбит/с)	Укажите максимально допустимую для данного класса пропускную способность в кбит/с. Для отдельных классов рекомендуется установить скорость от 20 до 20 000 кбит/с.
Priority (Приоритет)	Введите число от 0 до 7, обозначив приоритетность класса. Чем больше число, тем выше приоритет. Установкой по умолчанию является 3.
Borrow bandwidth from parent class (Заимствование пропускной способности у исходного класса)	Выберите эту опцию, если нужно разрешить подклассам забирать пропускную способность у своего исходного класса, если она используется не полностью. Заимствование пропускной способности выполняется в зависимости от приоритета подклассов. Это значит, что подкласс с наивысшим приоритетом (7) сможет первым забрать часть пропускной способности у своего исходного класса. Не выбирайте эту опцию для классов, находящихся непосредственно под корневым классом, если нужно оставить свободную пропускную способность для других типов трафика или установить скорость порта равной скорости следующего устройства в сети (см. описание поля **Speed (Скорость)** в окне **Summary (Общие настройки)**).

Табл. 58 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Configuration (Параметры класса) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Bandwidth Filter (Фильтр пропускной способности) Интернет-центр использует фильтр пропускной способности для выявления трафика, относящегося к какому-либо классу пропускной способности.	
Active (Активировать)	Отметьте эту опцию, если интернет-центр должен использовать фильтр при управлении пропускной способностью.
Service (Служба)	Вместо ввода значений в поля **Destination Port (Порт получателя)**, **Source Port (Порт источника)** и **Protocol ID (ID (идентификатор) протокола)** можно выбрать уже заданные. SIP (Протокол инициирования сеанса) представляет собой протокол, используемый в Интернет-телефонии, рассылке сообщений и прочих приложениях VoIP (Передача голоса по IP). Выберите **SIP** из раскрывающегося списка для настройки фильтра пропускной способности на трафик, использующий SIP. Протокол передачи файлов (FTP) является службой передачи файлов по сети Интернет и по сетям на основе TCP/IP. Система, в которой запущен сервер FTP, принимает команды от системы, в которой запущен клиент FTP. Данная служба позволяет пользователям посылать команды на сервер для загрузки и выгрузки файлов. Выберите **FTP** из раскрывающегося списка для настройки этого фильтра пропускной способности для трафика FTP. **H.323** — стандартный протокол для телеконференций, обеспечивающий конференц-связь с обменом аудио, видео и обычными данными. Позволяет осуществлять связь в реальном времени между двумя и несколькими клиентскими компьютерами в сети с пакетным обменом, не гарантирующей качества обслуживания. Выберите **H.323** из раскрывающегося списка для настройки этого фильтра на трафик, использующий H.323 Если выбрать **None (Нет)**, то класс пропускной способности будет применяться ко всем службам, если не указать какую-то конкретную, задав параметры в полях **Destination Port (Порт получателя)**, **Source Port (Порт источника)** и **Protocol ID (ID (идентификатор) протокола)**.
Destination IP Address (IP-адрес получателя)	Введите IP-адрес получателя в десятичном виде с разделительными точками. Пустое поле IP-адреса означает любой IP-адрес.
Destination Subnet Mask (Маска подсети получателя)	Введите маску подсети получателя. Это поле будет деактивировано, если Вы не укажете **Destination IP Address (IP-адрес получателя)**. Для получения дополнительной информации о подсетях IP см. приложение D.
Destination Port (Порт получателя)	Введите номер порта получателя. Пустое поле означает любой порт получателя.
Source IP Address (IP-адрес источника)	Введите IP-адрес источника. Пустое поле означает любой IP-адрес источника.
Source Subnet Mask (Маска подсети отправителя)	Введите маску подсети отправителя. Это поле будет деактивировано, если Вы не укажете **Source IP Address (IP-адрес источника)**. Для получения дополнительной информации о подсетях IP см. приложение D.
Source Port (Порт источника)	Введите номер порта отправителя. В приведенной ниже таблице показаны некоторые общие службы и номера портов. Пустое поле означает любой порт источника.
Protocol ID (ID (идентификатор) протокола)	Введите ID (идентификатор) протокола, например: 1 для ICMP, 6 для TCP или 17 для UDP. Пустое поле означает любой ID (идентификатор) протокола.

Табл. 58 Media Bandwidth Management (Управление пропускной способностью среды передачи): Class Configuration (Параметры класса) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Back (Назад)	Нажмите **Back** для возврата в главное окно **Media Bandwidth Management**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки в интернет-центр.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

Табл. 59 Службы и номера портов

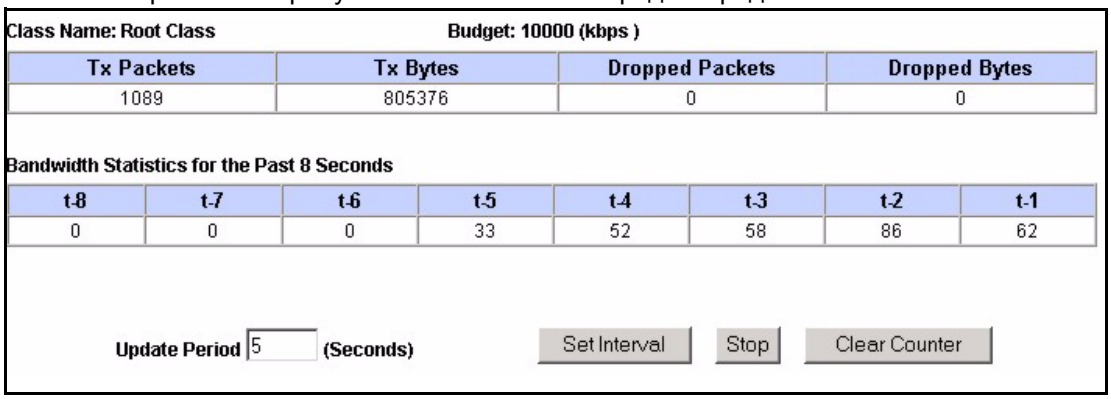
СЛУЖБЫ	НОМЕР ПОРТА
ECHO	7
FTP (File Transfer Protocol — Протокол передачи файлов)	21
SMTP (Simple Mail Transfer Protocol — Простой протокол электронной почты)	25
DNS (Domain Name System — Система доменных имен)	53
Finger (Указатель)	79
HTTP (Hyper Text Transfer Protocol — Протокол передачи гипертекста или WWW — "всемирная паутина")	80
POP3 (Post Office Protocol — Почтовый протокол)	110
NNTP (Network News Transfer Protocol — Сетевой протокол передачи новостей)	119
SNMP (Simple Network Management Protocol — Простой протокол управления сетью).	161
SNMP trap (Прерывание SNMP)	162
PPTP (Point-to-Point Tunneling Protocol — Протокол туннелирования "точка-точка")	1723

16.10.2 Управление пропускной способностью среды передачи: статистика

В окне **Media Bandwidth Management Statistics (Управление пропускной способностью среды передачи — Статистика)** можно посмотреть информацию о работе сети. В окне **Class Setup (Настройка классов пропускной способности)** нажмите кнопку **Statistics (Статистика)** — откроется одноименное окно

.

Рис. 97 Управление пропускной способностью среды передачи — Статистика



В следующей таблице даны описания полей этого окна.

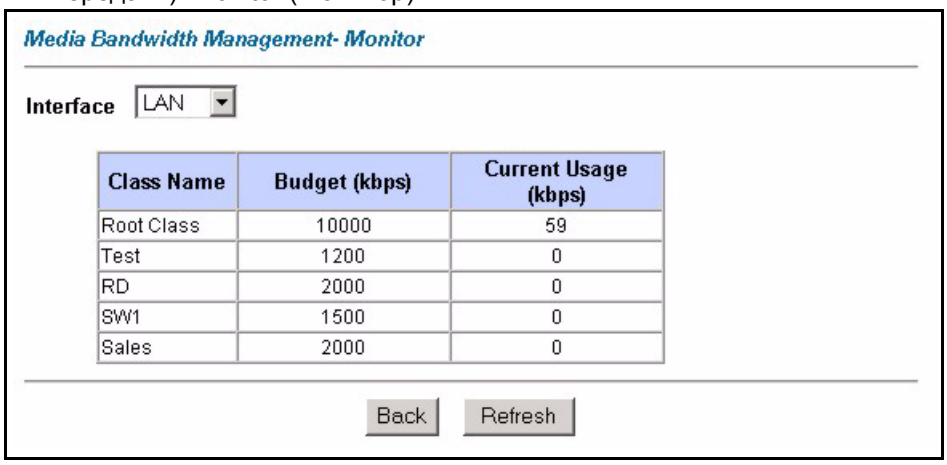
Табл. 60 Media Bandwidth Management Statistics (Управление пропускной способностью среды передачи: Статистика)

ПОЛЕ	ОПИСАНИЕ
Class Name (Имя класса)	В этом поле отображается имя класса, выводимое на странице статистики.
Budget (Бюджет, кбит/с)	В этом поле отображается пропускная способность, выделенная данному классу.
Tx Packets (Передано пакетов)	В этом поле отображается общее количество переданных пакетов.
Tx Bytes (Передано байт)	В этом поле отображается общее количество переданных байтов.
Dropped Packets (Сброшено пакетов)	В этом поле отображается общее количество сброшенных пакетов.
Dropped Bytes (Сброшено байт)	В этом поле отображается общее количество сброшенных байтов.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1) (Статистика пропускной способности за последние 8 секунд)	
В этом поле отображается статистика (в бит/с) по последним 8 секундам. Например, t-1 означает одну секунду назад.	
Update Period (seconds) (Периодичность обновления в секундах)	Введите интервал в секундах, через который должно выполняться обновление данных.
Set Interval (Установить интервал)	Нажмите кнопку **Set Interval (Установить интервал)**, чтобы задать новый интервал обновления, введенный в поле **Update Period (Периодичность обновления)**.
Stop Update (Прекратить обновление)	Нажмите кнопку **Stop Update**, чтобы браузер прекратил обновление статистики управления пропускной способностью.
Clear Counter (Сброс счетчика)	Для удаления всей статистики по пропускной способности нажмите кнопку **Clear Counter**.

16.11 Монитор пропускной способности

Для просмотра данных об использовании и распределении пропускной способности нажмите кнопку **Media Bandwidth Management (Управление пропускной способностью среды передачи)**, затем **Monitor (Монитор)**. При этом откроется показанное ниже окно.

Рис. 98 Media Bandwidth Management (Управление пропускной способностью среды передачи): Monitor (Монитор)



В следующей таблице даны описания полей этого окна.

Табл. 61 Media Bandwidth Management (Управление пропускной способностью среды передачи): Monitor (Монитор)

ПОЛЕ	ОПИСАНИЕ
Interface (Порт)	Из раскрывающегося списка выберите порт, для которого необходимо посмотреть использование пропускной способности по классам.
Class Name (Имя класса)	В этом поле отображается имя класса.
Budget (Бюджет, кбит/с)	В этом поле отображается пропускная способность, выделенная данному классу.
Current Usage (Текущее использование, кбит/с)	В этом поле отображается пропускная способность, используемая каждым из классов.
Back (Назад)	Нажмите **Back** для возврата в главное окно **Media Bandwidth Management**.
Refresh (Обновить)	Нажмите **Refresh (Обновить)**, чтобы обновить информацию.

Глава 17
Сопровождение

В этой главе описывается системные параметры, такие как микропрограмма ZyNOS, IP-адреса портов и статистика трафика, проходящего через порты.

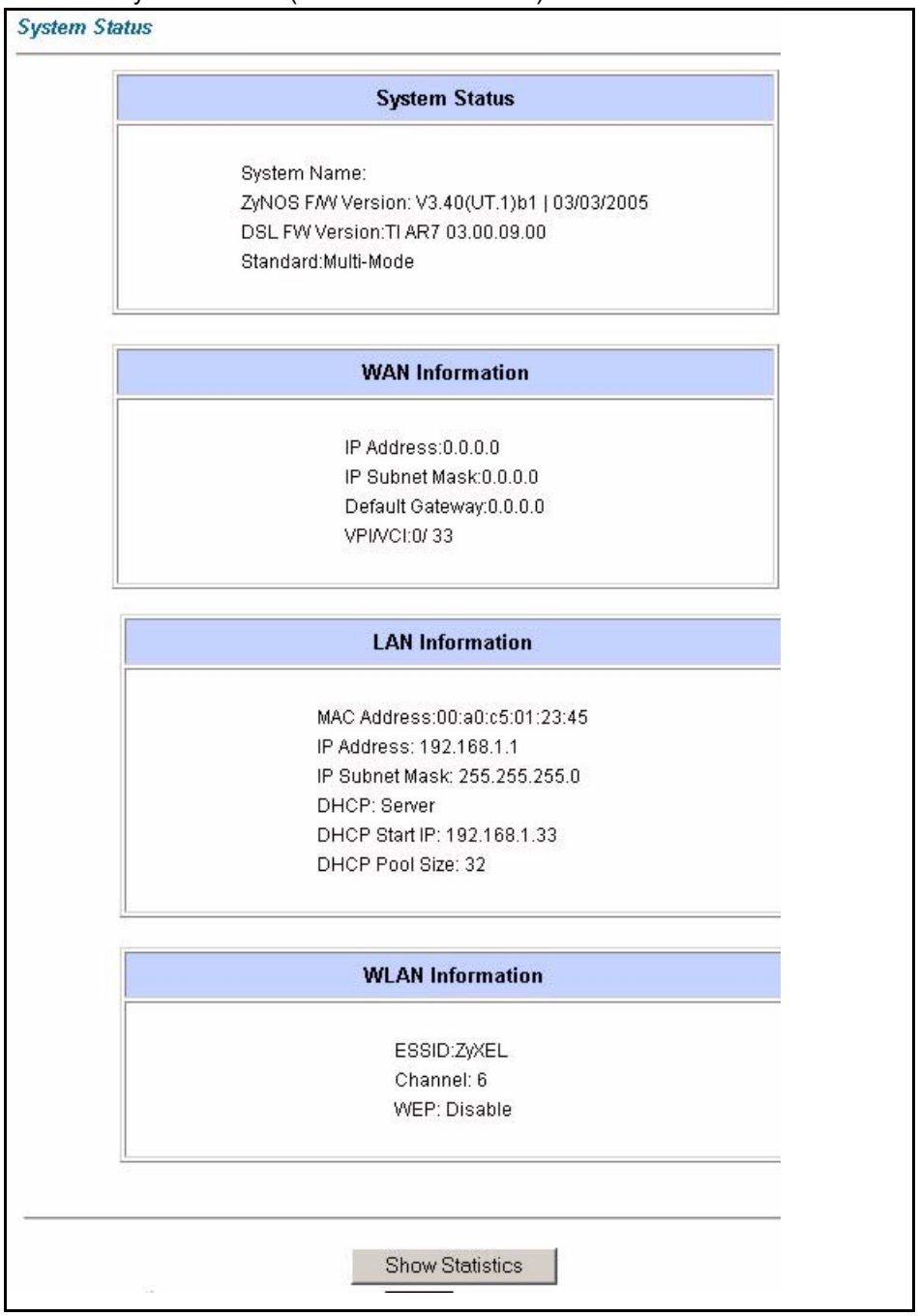
17.1 Сопровождение — общая информация

Окна обслуживания устройства служат для просмотра информации о системе, загрузки новой микропрограммы, управления конфигурацией и сброса настроек интернет-центра к заводским настройкам по умолчанию.

17.2 Окно "Состояние системы"

Нажмите **System Status (Состояние системы)** на вкладке **Maintenance (Сопровождение)**, при этом откроется следующее окно, предназначенное для наблюдения за работой интернет-центра. Следует отметить, что поля в этом окне отображаются в режиме ТОЛЬКО ДЛЯ ЧТЕНИЯ и используются только в целях диагностики.

Рис. 99 System Status (Состояние системы)



В следующей таблице даны описания полей этого окна.

Табл. 62 Состояние системы

ПОЛЕ	ОПИСАНИЕ
Состояние системы	
System Name (Системное имя)	В этом поле отображается имя интернет-центра. Это имя используется для идентификации.

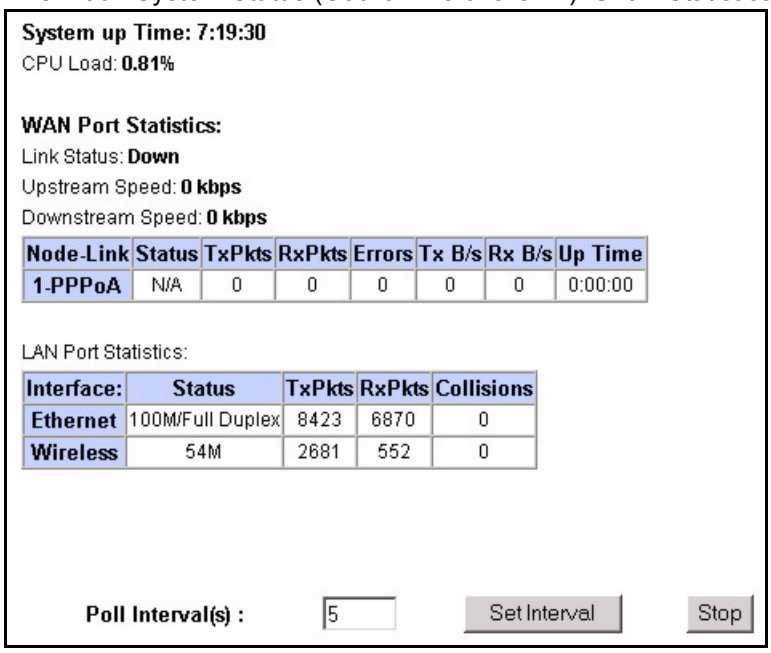
Табл. 62 Состояние системы (продолжение)

ПОЛЕ	ОПИСАНИЕ
ZyNOS Firmware Version (Версия микропрограммы ZyNOS)	Здесь отображается версия и дата создания микропрограммы ZyNOS. ZyNOS — это собственная разработка сетевой операционной системы ZyXEL.
DSL FW Version (Версия ПО DSL)	Здесь отображается версия микропрограммы DSL для интернет-центра.
Standard (Стандарт)	Здесь отображается используемый интернет-центром стандарт.
WAN Information (Параметры глобальной сети)	
IP Address (IP-адрес)	Здесь отображается IP-адрес порта WAN.
IP Subnet Mask (Маска IP подсети)	Здесь отображается маска IP подсети для порта WAN.
Default Gateway (Шлюз по умолчанию)	Здесь отображается IP-адрес шлюза по умолчанию, если он применяется.
VPI/VCI	Здесь отображаются номера Идентификатора виртуального пути (VPI) и Идентификатора виртуального канала (VCI), установленные в первом окне Мастера установки.
LAN Information (Параметры локальной сети)	
MAC Address (MAC-адрес)	В этом поле отображается уникальный MAC-адрес (Media Access Control — Управление доступом к среде) или Ethernet адрес интернет-центра.
IP-Address (IP-адрес)	Здесь отображается IP-адрес порта LAN.
IP Subnet Mask (Маска IP подсети)	Здесь отображается маска IP подсети для порта LAN.
DHCP	Здесь отображается режим DHCP порта WAN: **Server (Сервер)**, **Relay (Ретранслятор)** (не во всех моделях) или **None (Отключить)**.
DHCP Start IP (Начальный IP-адрес дипазона DHCP)	Здесь устанавливается первый адрес из непрерывного дипазона IP-адресов.
DHCP Pool Size (Размер дипазона DHCP)	Здесь устанавливается количество IP-адресов дипазона DHCP.
WLAN Information (Информация о беспроводной ЛВС)	
ESSID	Это описательное имя, используемое для идентификации интернет-центра в беспроводной локальной сети.
Channel (Канал)	Номер канала, используемого интернет-центром.
WEP	Отображает статус шифрования данных WEP.
Show Statistics (Показать статистику)	Нажмите кнопку **Show Statistics (Показать статистику)** для просмотра статистики производительности, например, количества пакетов, переданных и принятых через каждый порт.

17.2.1 Статистика системы

В окне **System Status (Состояние системы)** нажмите кнопку **Show Statistics (Показать статистику)** для отображения представленного ниже окна. Здесь отображается информация о состоянии портов и точная статистика пакетов в режиме только для чтения. Также здесь отображается "system up time" (время работы системы) и "poll interval(s)" (интервал опроса системы). Поле **Poll Interval(s) (Интервал опроса)** можно настраивать.

Рис. 100 System Status (Состояние системы): Show Statistics (Показать статистику)



В следующей таблице даны описания полей этого окна.

Табл. 63 Состояние системы: Показать статистику

ПОЛЕ	ОПИСАНИЕ
System up Time (Время работы системы)	Здесь отображается время, истекшее с момента запуска системы.
CPU Load (Загрузка ЦП)	В этом поле отображается процент загрузки процессора модема.
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 состояние подключения к глобальной сети.
Upstream Speed (Скорость исходящего трафика)	В этом поле отображается скорость исходящего от интернет-центра трафика

Табл. 63 Состояние системы: Показать статистику (продолжение)

ПОЛЕ	ОПИСАНИЕ
Downstream Speed (Скорость входящего трафика)	В этом поле отображается скорость входящего в интернет-центр трафика
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)	Для порта WAN здесь отображается скорость порта и режим передачи, если используется инкапсуляция Ethernet, а также **Down (Не работает)** — канал не работает, **Idle (Ожидание)** — простой канала (ppp), **Dial (Установление соединения)** — выполняется вызов и **Drop (Завершение соединения)** — разрыв соединения, если используется инкапсуляция PPPoE. Для порта LAN здесь отображается скорость порта и режим передачи.
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 (Скорость передачи, байт/с)	В этом поле отображается количество байтов, переданных в последнюю секунду.
Rx B/s (Скорость приема, байт/с)	В этом поле отображается количество байтов, принятых в последнюю секунду.
Up Time (Время соединения)	В этом поле отображается время, прошедшее с момента установления соединения через этот порт.
Collisions (Конфликты)	Здесь отображается количество конфликтов при передаче через данный порт.
Poll Interval(s) (Интервал(ы) опроса)	Введите интервал времени, через который браузер будет обновлять информацию о системе.
Set Interval (Установить интервал)	Нажмите на эту кнопку, чтобы применить новый интервал опроса, заданный в поле **Poll Interval (Интервал опроса)**.
STOP (Остановить)	Нажмите на эту кнопку, чтобы прекратить обновление информации о системе.

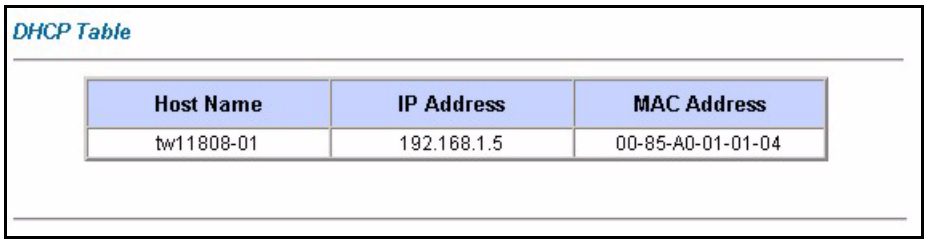
17.3 Окно "Таблица DHCP"

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 интернет-центр как сервер DHCP или отключить эту функцию. При включенной

функции сервера DHCP, интернет-центр предоставляет клиентам настройки TCP/IP. При установке значения **None (Отключить)**, служба DHCP будет отключена, следовательно, необходимо иметь другой сервер DHCP в локальной сети, или изменять параметры компьютера вручную.

Нажмите **Maintenance (Сопровождение)** и затем выберите закладку **DHCP Table (Таблица DHCP)**. Появится окно с информацией о состоянии DHCP в режиме только для чтения. В таблице DHCP отображается текущая информация о клиентах DHCP (включая **IP-адрес**, **имя узла** и **MAC-адрес**) для всех клиентов в сети, использующих сервер DHCP.

Рис. 101 Таблица DHCP



В следующей таблице даны описания полей этого окна.

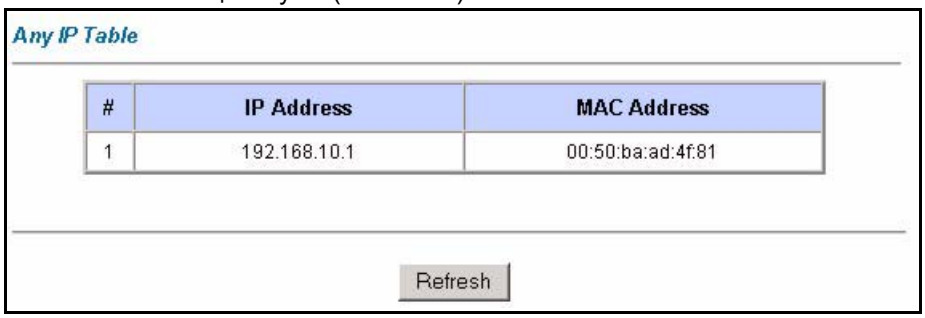
Табл. 64 Таблица DHCP

ПОЛЕ	ОПИСАНИЕ
Host Name (Имя узла)	Здесь отображается имя узла.
IP-Address (IP-адрес)	В этом поле отображается IP-адрес узла с именем, указанным в поле **Host Name (Имя узла)**.
MAC Address (MAC-адрес)	В этом поле отображается MAC-адрес (Media Access Control — Управление доступом к среде) компьютера с данным именем. Каждое устройство Ethernet имеет уникальный MAC-адрес. MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатиричных символов, например, 00:A0:C5:00:00:02.

17.4 Окно "Таблица Any IP"

Нажмите **Maintenance (Сопровождение)**, выберите **Any IP (Любой IP)**. В таблице Any IP отображается текущая информация в режиме только для чтения (включая IP-адрес и MAC-адрес) для всех сетевых устройств, которые используют функцию Any IP для подключения к интернет-центру.

Рис. 102 Таблица Any IP (Любой IP)



В следующей таблице даны описания полей этого окна.

Табл. 65 Таблица Any IP (Любой IP)

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер.
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 назначается изготовителем и состоит из 6 пар шестнадцатиричных символов, например, 00:A0:C5:00:00:02.
Refresh (Обновить)	Нажмите кнопку **Refresh (Обновить)** для обновления информации в этом окне.

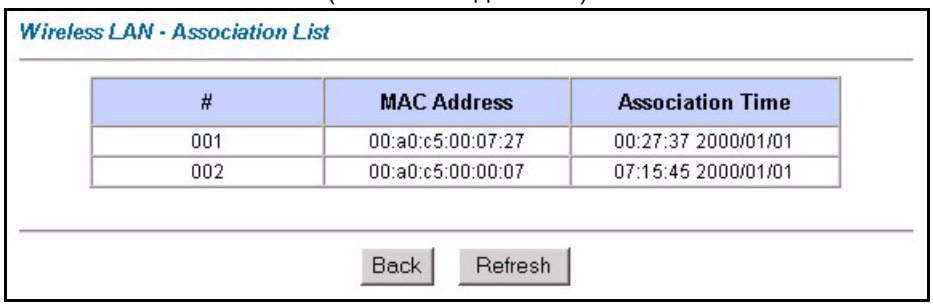
17.5 Окно "Беспроводная сеть" (Wireless)

В этом окне только для чтения отображаются сведения о беспроводной локальной сети интернет-центра.

17.5.1 Association List (Список соединений)

Этот экран отображает MAC-адрес(а) беспроводных устройств, зарегистрированных в сети в данный момент. Нажмите **Wireless LAN (Беспроводная ЛВС)** и затем **Association List (Список соединений)**, чтобы открыть окно, представленное ниже.

Рис. 103 Association List (Список соединений)



В следующей таблице даны описания полей этого окна.

Табл. 66 Association List (Список соединений)

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер подключенного беспроводного устройства.
MAC Address (MAC-адрес)	В этом поле отображается MAC-адрес (Media Access Control — Управление доступом к среде) соответствующего беспроводного устройства. Каждое устройство Ethernet имеет уникальный MAC-адрес. MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатиричных символов, например, 00:A0:C5:00:00:02.
Association Time (Время подключения)	В этом поле отображается время, в течение которого беспроводное устройство подключено к интернет-центру.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Refresh (Обновить)	Нажмите кнопку **Refresh** для обновления информации в таблице.

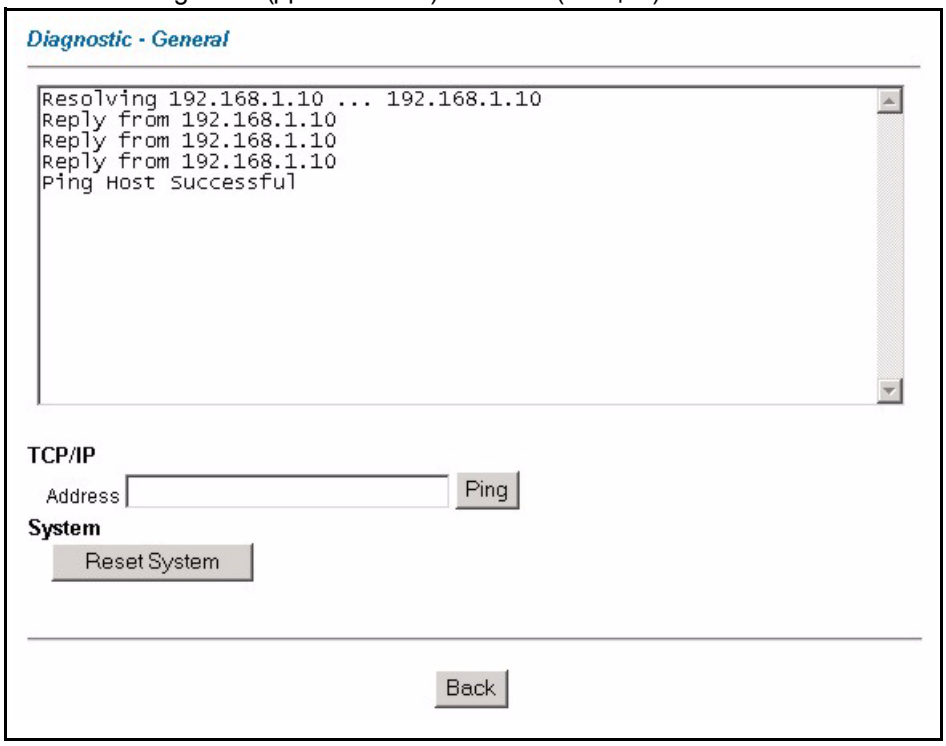
17.6 Окна диагностики

Информация в этих окнах представлена в режиме только для чтения и предназначена для определения неисправностей интернет-центра.

17.6.1 Общая диагностика

Нажмите **Diagnostic (Диагностика)** и затем **General (Общая диагностика)** для отображения окна, представленного ниже.

Рис. 104 Diagnostic (Диагностика): General (Общая)



В следующей таблице даны описания полей этого окна.

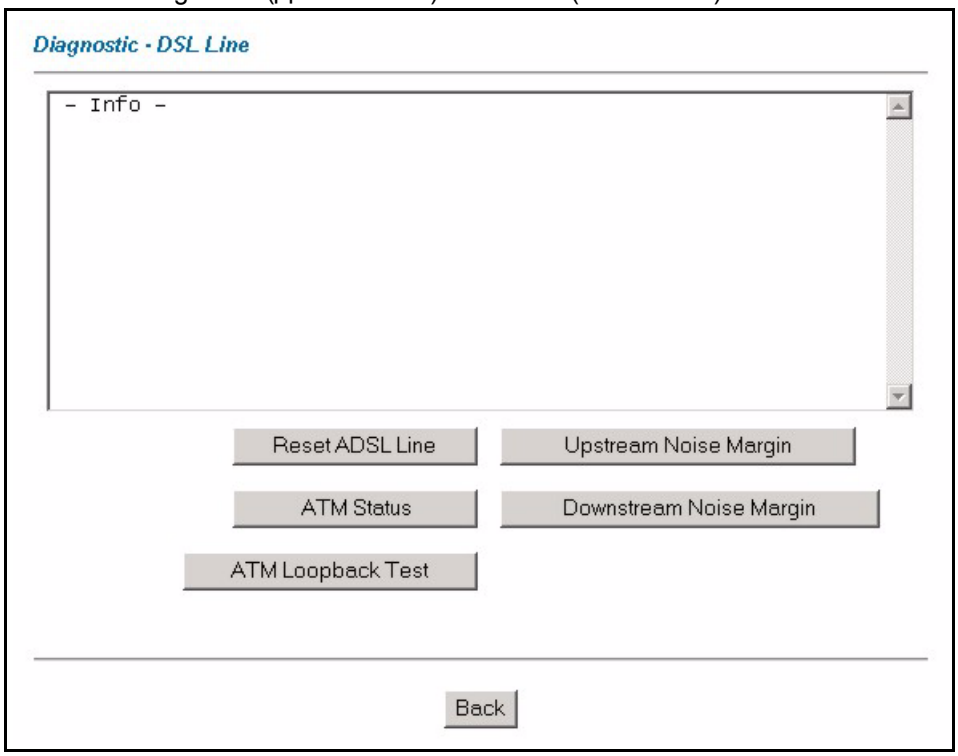
Табл. 67 Diagnostic (Диагностика): General (Общая)

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)	Нажмите эту кнопку для тестирования устройства с введенным IP-адресом с помощью команды "ping".
Reset System (Сброс настроек)	Нажмите эту кнопку для сброса настроек интернет-центра к заводским настройкам по умолчанию. Появится диалоговое окно с предупреждением: "уверены ли вы, что хотите выполнить сброс настроек интернет-центра к заводским настройкам по умолчанию?". Нажмите **OK** для продолжения.
Back (Назад)	Нажмите на эту кнопку для перехода обратно к главному окну **Diagnostic (Диагностика)**.

17.6.2 Диагностика линии DSL

Нажмите **Diagnostic (Диагностика)** и затем **DSL Line (DSL линия)** для отображения окна, представленного ниже.

Рис. 105 Diagnostic (Диагностика): DSL Line (DSL линия)



В следующей таблице даны описания полей этого окна.

Табл. 68 Diagnostic (Диагностика): DSL Line (DSL линия)

ПОЛЕ	ОПИСАНИЕ
Reset ADSL Line (Сброс ADSL линии)	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!"
ATM Status (Состояние ATM)	Нажмите на эту кнопку для отображения состояния ATM.
ATM Loopback Test (Тест петля ATM)	Нажмите на эту кнопку для запуска кольцевого тестирования ATM. Прежде чем начать выполнение теста, убедитесь, что вы настроили хотя бы один PVC с соответствующими VPI/VCI. Интернет-центр посылает пакет OAM F5 на ATM/DSL-коммутатор, после чего он возвращается обратно в интернет-центр. Кольцевое тестирование ATM используется для поиска и устранения неисправностей в сети ATM.
Upstream Noise Margin (Запас помехоустойчивости при передаче)	Нажмите на эту кнопку для отображения запаса помехоустойчивости при передаче.

Табл. 68 Diagnostic (Диагностика): DSL Line (DSL линия) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Downstream Noise Margin (Запас помехоустойчивости при приеме)	Нажмите на эту кнопку для отображения запаса помехоустойчивости при приеме.
Back (Назад)	Нажмите на эту кнопку для перехода обратно к главному окну **Diagnostic (Диагностика)**.

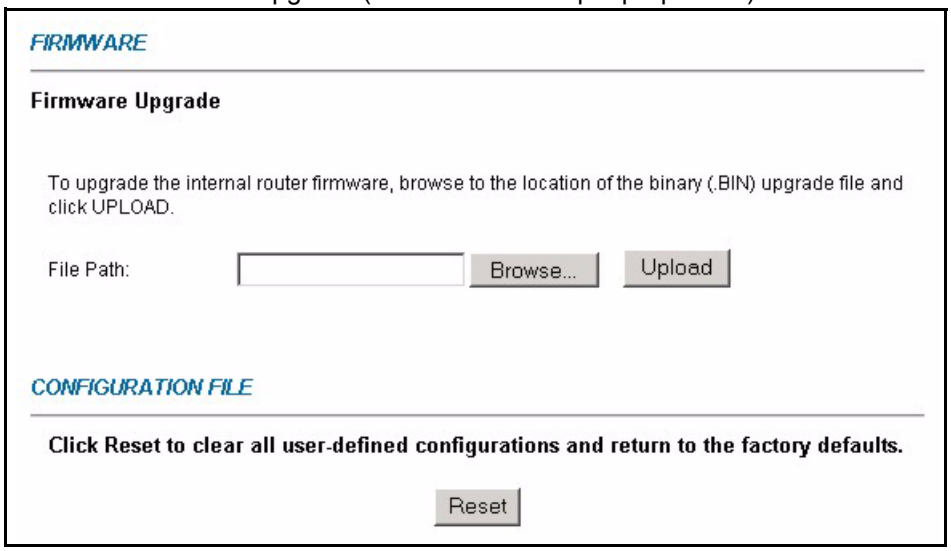
17.7 Обновление микропрограммы

Найдите на сайте www.zyxel.ru файл микропрограммы с именем, состоящим (как правило) из наименования модели системы с расширением .bin, например, "P-660RU.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.Обновление микропрограммы с помощью команд FTP/TFTP — см. Гл. 33, на с. 352.

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

Нажмите **Firmware (Микропрограмма)** для отображения следующего окна. Следуйте указаниям в этом окне для загрузки микропрограммы в интернет-центр.

Рис. 106 Firmware Upgrade (Обновление микропрограммы)



В следующей таблице даны описания полей этого окна.

Табл. 69 Firmware Upgrade (Обновление микропрограммы)

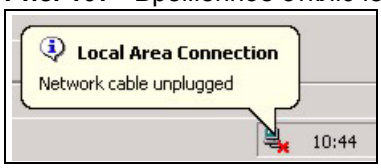
ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите путь к файлу, который вы хотите загрузить, или нажмите кнопку **Browse (Просмотр)**, чтобы указать местонахождение файла.
Browse (Просмотр)...	Нажмите кнопку **Browse (Просмотр)**,чтобы указать местонахождение файла с расширением .bin, который вы хотите загрузить. Необходимо помнить, что архивированные файлы (.zip) необходимо распаковать, прежде чем выполнять загрузку в модем.
Upload (Загрузка)	Нажмите кнопку **Upload (Загрузка)** для запуска процесса загрузки. Процесс загрузки может занять до 2 минут.
Reset (Сброс)	Нажмите на эту кнопку для полного удаления пользовательской конфигурации и возвращения параметров интернет-центра к заводским настройкам по умолчанию.

ПРИМЕЧАНИЕ: Нельзя выключать питание интернет-центра во время загрузки микропрограммы!

После того как вы увидите окно **Firmware Upload in Process (Выполняется загрузка микропрограммы)**, подождите 2 минуты, прежде чем повторно подключиться к интернет-центру по сети и войти в систему.

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

Рис. 107 Временное отключение сети



По истечении 2 минут, снова подключитесь к модему по сети, войдите в web-конфигуратор и проверьте версию новой микропрограммы в окне **System Status (Состояние системы)**.

Если загрузку не удалось завершить успешно, появится следующее окно. Нажмите кнопку **Back (Назад)** для возврата к окну **Firmware (Микропрограмма)**.

Рис. 108 Error Message (Сообщение об ошибке)

Глава 18
Знакомство с SMT

В этой главе описывается, как получить доступ и работать с интерфейсом SMT (System Management Terminal — Системная консоль), а также представлен обзор меню SMT.

18.1 Описание SMT (System Management Terminal)

Системная консоль интернет-центра (System Management Terminal) — это интерфейс управления на основе меню, к которому можно получить доступ с помощью программы эмулятора терминала через соединение telnet. В этой главе описывается, как получить доступ к меню SMT (Системная консоль) с помощью Telnet, как работать с интерфейсом SMT, а также настраивать параметры модема с помощью меню SMT.

18.1.1 Процедура настройки при помощи SMT через соединение Telnet

Далее представлен порядок подключения к интернет-центру с помощью Telnet.

1. В Windows, нажмите кнопку **Start (Пуск)** (обычно в левом нижнем углу), **Run (Выполнить)**, затем напечатайте "`telnet 192.168.1.1`" (IP-адрес по умолчанию), нажмите **OK**.
2. Введите “`1234`” в поле **`Password (Пароль)`**.
3. После ввода пароля появится главное меню.

Если в течение пяти минут (время ожидания по умолчанию) после регистрации не производится никаких действий, интернет-центр автоматически завершает сеанс. Вам придется заново подключаться к интернет-центру с помощью Telnet.

18.1.2 Ввод пароля

После нажатия клавиши [ENTER] появляется окно с запросом на ввод пароля, как показано ниже.

При первой регистрации введите пароль по умолчанию "`1234`". При вводе пароля каждый набираемый символ на экране отображается как символ звездочка "`*`".

Если в течение пяти минут после регистрации не производится никаких действий, интернет-центр автоматически завершает сеанс.

Рис. 109 Экран регистрации

```
Enter Password: ****
```

18.1.3 Обзор меню SMT интернет-центра

В приведенной ниже таблице дан обзор различных меню SMT интернет-центра.

Табл. 70 Обзор меню SMT модема

МЕНЮ	ПОДМЕНЮ		
1 General Setup — Настройка общих параметров	1.1 Configure Dynamic DNS — Настройка динамической DNS		
2 WAN Backup Setup — Настройка резервирования глобальной сети			
3 LAN Setup — Настройка локальной сети	3.1 LAN Port Filter Setup — Настройка фильтра для порта локальной сети		
	3.2 TCP/IP and DHCP Setup — Настройка TCP/IP и DHCP	3.2.1 IP Alias Setup — Настройка псевдонимов IP	
	3.5 Wireless LAN Setup — Настройка беспроводной локальной сети	3.5.1 WLAN MAC Address Filter — Фильтр MAC-адресов WLAN	
4 Internet Access Setup — Настройка доступа в Интернет			
11 Remote Node Setup — Настройка удаленного узла	11.1 Remote Node Profile — Профиль удаленного узла		
	11.3 Remote Node Network Layer Options — Параметры сетевого уровня удаленного узла		
	11.5 Remote Node Filter — Фильтр для удаленного узла		
	11.6 Remote Node ATM Layer Options — Параметры уровня ATM удаленного узла		
	11.8 Advance Setup Options (PPPoE passthrough) — Параметры расширенной настройки (транзит PPPoE-соединений)		
12 Static Routing Setup — Настройка статической маршрутизации	12.1 Edit Static Route Setup — Редактирование настроек статического маршрута	12.1.1 Edit IP Static Route — Редактирование статического маршрута IP	
	12.3 Bridge Static Route Setup — Настройка статического маршрута для моста	12.3.1 Edit Bridge Static Route — Редактирование статического маршрута моста	

Табл. 70 Обзор меню SMT модема (продолжение)

МЕНЮ	ПОДМЕНЮ		
14 Dial-in User Setup — Настройка подключения удаленного пользователя	14.1 Dial-in User Setup — Настройка подключения удаленного пользователя через коммутируемое соединение		
15 NAT Setup — Настройка NAT	15.1 Address Mapping Sets — Наборы отображения адресов	15.1.x Address Mapping Rules — Правила отображения адресов	15.1.x.x Address Mapping Rule — Правило отображения адресов
	15.2 NAT Server Sets — Наборы серверов NAT	15.2.x NAT Server Setup — Настройка сервера NAT	
21 Filter and Firewall Rule Setup — Настройка правил фильтров и межсетевого экрана	21.1 Filter Setup — Настройка фильтров	21.1 Filter Rules Summary — Список правил фильтров	21.1.x.1 Generic Filter Rule — Правило фильтра общего типа
			21.1.x.1 TCP/IP Filter Rule — Правило фильтра TCP/IP
	21.2 Firewall Setup — Настройка межсетевого экрана		
22 SNMP Configuration — Настройка SNMP			
23 System Security — Системные функции безопасности	23.1 Change Password — Смена пароля		
	23.2 RADIUS Server — Сервер RADIUS		
	23.4 IEEE 802.1X		

Табл. 70 Обзор меню SMT модема (продолжение)

МЕНЮ	ПОДМЕНЮ		
24 System Maintenance (Сопровождение системы)	24.1 Status — Статус		
	24.2 System Information and Console Port Speed — Системная информация и скорость консольных портов	24.2.1 Information — Информация	
		24.2.2 Change Console Port Speed — Изменение скорости консольного порта	
	24.3 Log and Trace — Журнал регистрации и трассировка	24.3.1 View Error Log — Просмотр журнала ошибок	
		24.3.2 UNIX Syslog — Системный журнал UNIX	
	24.4 Diagnostic — Диагностика		
	24.5 Backup Configuration — Резервное сохранение конфигурации		
	24.6 Restore Configuration — Восстановление конфигурации		
	24.7 Upload Firmware — Загрузка микропрограммного обеспечения	24.7.1 Upload System Firmware — Загрузка микропрограммного обеспечения	
		24.7.2 Upload System Configuration File — Загрузка файла системной конфигурации	
	24.8 Command Interpreter Mode — Режим интерпретатора команд		
	24.9 Call Control — Контроль вызовов	24.9.1 Budget Management — Управление бюджетом	
	24.10 Time and Date Setting — Установка времени и даты		
	24.11 Remote Management Control — Контроль удаленного управления		
25 IP Routing Policy Setup — Настройка политики маршрутизации IP	25.1 IP Routing Policy Setup — Настройка политики маршрутизации IP	25.1.1 IP Routing Policy — Политика маршрутизации IP	
26 Schedule Setup — Настройка расписания	26.1 Schedule Set Setup — Создание набора расписаний		

18.2 Работа с интерфейсом SMT

SMT (System Management Terminal — Системная консоль) является интерфейсом, предназначенным для настройки параметров интернет-центра.

Прежде, чем выполнять изменения в конфигурации, необходимо ознакомиться с некоторыми операциями, приведенными в представленной ниже таблице.

Табл. 71 Работа с интерфейсом SMT

ОПЕРАЦИЯ	НАЖАТИЕ КЛАВИШИ	ОПИСАНИЕ
Переход к меню нижнего уровня	[Enter]	Для перехода в подменю введите его номер и нажмите клавишу [ENTER].
Переход к меню верхнего уровня	[Esc]	Для возврата к предыдущему меню нажмите клавишу [ESC].
Переход к "скрытому" меню	Нажмите клавишу [ПРОБЕЛ] для изменения **No** на **Yes**, а затем нажмите клавишу [ENTER].	Поля, начинающиеся с "Edit", ведут к "скрытым" меню и имеют значение по умолчанию **No**. Чтобы перейти к "скрытому" меню нажмите клавишу [ПРОБЕЛ] для изменения **No** на **Yes**, затем нажмите клавишу [ENTER] .
Перемещение курсора	Клавиша [ENTER] или клавиши со стрелками "вверх/вниз".	Находясь в меню, для перемещения к следующему полю нажмите клавишу [ENTER]. Для перемещения к предыдущему/следующему полю можно также использовать клавиши со стрелками "вверх/вниз".
Ввод данных	Введите данные или нажмите клавишу [ПРОБЕЛ], затем нажмите клавишу [ENTER].	Меню содержат два типа полей. В поле первого типа следует напечатать требуемые данные. Поля второго типа предназначены для ввода параметров, просмотр вариантов которых производится с помощью клавиши [ПРОБЕЛ].
Обязательные поля	<? > или **ChangeMe (Измени меня)**	Все поля с символом <?> подлежат обязательному заполнению, чтобы иметь возможность сохранения новой конфигурации. Чтобы иметь возможность сохранения новой конфигурации, поля **ChangeMe (Измени меня)** нельзя оставлять пустыми.
Недоступные поля	<N/A>	В некоторых полях SMT отображается <N/A> (недоступно). Это означает, что данное поле недоступно.
Сохранение конфигурации	[Enter]	Для сохранения конфигурации нажмите клавишу [ENTER] при появлении сообщения "Press ENTER to confirm or ESC to cancel" (Нажмите [ENTER] для подтверждения или [ESC] для отмены). После сохранения данных, как правило, происходит возврат к предыдущему меню.
Выход из SMT		Введите 99 и затем нажмите клавишу [ENTER]. Ввод символов 99 в строке приглашения Главного меню и нажатие [ENTER] используются для выхода из интерфейса SMT.

После ввода пароля на экране отображается Главное меню SMT, как показано ниже.

Табл. 72 Главное меню SMT

```
                Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

                          Prestige 660HW-T1  Main Menu

  Getting Started                       Advanced Management
    1. General Setup                      21. Filter and Firewall Setup
    2. WAN Backup Setup                   22. SNMP Configuration
    3. LAN Setup                          23. System Security
    4. Internet Access Setup              24. System Maintenance
                                          25. IP Routing Policy Setup
  Advanced Applications                   26. Schedule Setup
    11. Remote Node Setup
    12. Static Routing Setup
    14. Dial-in User Setup                99. Exit
    15. NAT Setup




                        Enter Menu Selection Number:
```

18.2.1 Обзор интерфейса SMT

Табл. 73 Обзор Главного меню

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
1	General Setup (Настройка общих параметров)	Данное меню используется для ввода общих параметров.
2	WAN Backup Setup (Настройка резервирования глобальной сети)	Данное меню используется для настройки перенаправления трафика и резервного соедининения через модем.
3	LAN Setup (Настройка локальной сети)	Данное меню используется для настройки беспроводной локальной сети и подключения к локальной сети.
4	Internet Access Setup (Настройка доступа в Интернет)	Простой и быстрый способ настройки подключения к Интернету.
11	Remote Node Setup (Настройка удаленного узла)	Данное меню используется для настройки удаленного узла для соединения между локальными сетями, включая подключение к Интернет.
12	Static Routing Setup (Настройка статической маршрутизации)	Данное меню используется для настройки статических маршрутов.

Табл. 73 Обзор Главного меню

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
14	Dial-in User Setup (Настройка подключения удаленного пользователя)	Данное меню используется для настройки учетных записей локального пользователя в интернет-центре.
15	NAT Setup (Настройка NAT)	Данное меню используется для определения внутренних серверов, когда включена служба NAT.
21	Filter and Firewall Setup (Настройка фильтров и межсетевого экрана)	Данное меню используется для настройки фильтров, включения/отключения межсетевого экрана и просмотра журнала сообщений межсетевого экрана.
22	SNMP Configuration (Настройка SNMP)	Данное меню используется для настройки параметров SNMP.
23	System Security (Системные функции безопасности)	Данное меню используется для настройки защиты беспроводных соединений и для изменения пароля.
24	System Maintenance (Сопровождение системы)	Данное меню обеспечивает просмотр информации о состоянии системы, диагностику, загрузку микропрограммы и т. д.
25	IP Routing Policy Setup (Настройка политики маршрутизации IP)	Данное меню используется для настройки политики маршрутизации IP.
26	Schedule Setup (Составление плана)	Данное меню используется для составления расписания исходящих вызовов.
99	Exit (Выход)	Данное меню используется для выхода из SMT и перехода к пустому экрану.

18.3 Изменение системного пароля

Для изменения пароля интернет-центра, заданного по умолчанию, выполните следующие действия.

1. Введите "23" в главном меню для перехода в **Меню 23 — System Security (Системные функции безопасности)**.
2. Введите 1 для перехода в **Меню 23.1 — System Security (Системные функции безопасности): Change Password (Изменение пароля)**, как показано ниже.
3. Введите текущий системный пароль в поле **Old Password (Старый пароль)**, например, “1234" и нажмите клавишу [ENTER].

Рис. 110 Меню 23.1 — Изменение пароля

```
            Menu 23.1 - System Security - Change Password

                Old Password= ?
                New Password= ?
                Retype to confirm=?

            Enter here to CONFIRM or ESC to CANCEL:
```

4 Введите новый системный пароль в поле **New Password (Новый пароль)** (до 30 символов) и нажмите клавишу [ENTER].

5 Для подтверждения повторите ввод нового системного пароля в поле **Retype to Confirm (Повторный ввод для подтверждения)** и нажмите клавишу [ENTER].

ПРИМЕЧАНИЕ: При вводе пароля каждый символ на экране отображается символом звездочка “*”.

Глава 19
Меню 1 — Настройка общих параметров

Меню 1 — Настройка общих параметров содержит административную и общесистемную информацию.

19.1 Настройка общих параметров

Меню 1 — Настройка общих параметров содержит административную и общесистемную информацию (см. ниже). Поле **System Name (Имя системы)** служит только для идентификации. Однако, поскольку некоторые Интернет-провайдеры проверяют это имя, следует вводить имя вашего компьютера.

- В Windows 95/98 нажмите **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)**, **Network (Сеть и удаленный доступ к сети)**. Выберите закладку **Identification (Идентификация)**, запишите имя, указанное в поле **Computer Name (Имя компьютера)** и введите его как **Системное имя** интернет-центра.
- В Windows 2000 нажмите **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)** и дважды щелкните по иконке **System (Система)**. Выберите закладку **Network Identification (Сетевая идентификация)**, а затем на кнопке **Properties (Свойства)**. Запишите имя, указанное в поле **Computer Name (Имя компьютера)** и введите его как **Системное имя** интернет-центра.
- В Windows XP нажмите **Start (Пуск)**, **My Computer (Мой компьютер) -View system information (Информация о системе)**, а затем выберите закладку **Computer Name (Имя компьютера)**. Запишите имя, указанное в поле **Full Computer Name (Полное имя компьютера)**, и введите его как **Системное имя** интернет-центра.

Запись **Domain Name (Имя домена)** передается клиентам DHCP в локальной сети. Если вы оставите это поле незаполненным, будет использоваться имя домена, полученное протоколом DHCP от Интернет-провайдера. В отличие от имени узла (системное имя), которое необходимо вводить на каждом конкретном компьютере, имя домена может быть назначено интернет-центром с помощью DHCP.

19.2 Процедура настройки в Меню 1

В главном меню введите 1 для перехода в **Меню 1 — Настройка общих параметров**, как показано ниже.

Рис. 111 Меню 1 — Настройка общих параметров

```
                Menu 1 General Setup

                      System Name= ?
                      Location=
                      Contact Person's Name=
                      Domain Name=
                      Edit Dynamic DNS= No

                      Route IP= Yes
                      Bridge= No

           Press ENTER to Confirm or ESC to Cancel:
```

Заполните обязательные поля. Подробная информация по этим полям представлена в таблице ниже.

Табл. 74 Меню 1 — Настройка общих параметров

ПОЛЕ	ОПИСАНИЕ
System Name (Системное имя)	Введите описательное имя в целях идентификации. Имя может включать до 30 буквенно-цифровых символов. Использование пробелов не допускается, но допускается использование тире "-" и символа подчеркивания "_".
Location (Местонахождение) (необязательное поле)	Введите географическое местонахождение интернет-центра (до 31 символа).
Contact Person`s Name (Имя ответственного лица (необязательное поле))	Введите имя ответственного за интернет-центр лица (до 30 символов).
Domain Name (Имя домена)	Введите имя домена (если известно). Если это поле оставлено пустым, Интернет-провайдер может назначить имя домена с помощью DHCP. Чтобы увидеть текущее имя домена, используемое вашим шлюзом, нужно перейти в меню 24.8 и ввести команду "sys domainname". Чтобы очистить это поле, просто нажмите клавишу [ПРОБЕЛ]. Имя домена, введенное вручную, имеет более высокий приоритет, чем имя домена, назначенное Интернет-провайдером.
Edit Dynamic DNS (Редактировать динамическую DNS)	Нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)** или **No (Нет)** (по умолчанию). Выберите **Yes (Да)** для настройки **Меню 1.1 — Настройка динамической DNS** (описано далее).
Route IP (Маршрутизация IP)	Установите значение этого поля **Yes (Да)** для включения или **No (Нет)** для отключения маршрутизации IP. Для доступа в Интернет, необходимо включить маршрутизацию IP.

Табл. 74 Меню 1 — Настройка общих параметров

ПОЛЕ	ОПИСАНИЕ
Bridge (Мост)	Включение/выключение моста для передачи неподдерживаемых протоколов (например, SNA) или протоколов,которые не включены в предыдущем поле **Route IP (Маршрутизация IP)**. Выберите **Yes (Да)**, чтобы включить мост; выберите **No (Нет)**, чтобы отключить его.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "`Press ENTER to Confirm or ESC to Cancel:`" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

19.2.1 Процедура настройки динамической DNS (DYNDNS)

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

Для настройки динамической DNS перейдите в **Меню 1 — Настройка общих параметров** и выберите **Yes (Да)** в поле **Edit Dynamic DNS (Редактировать динамическую DNS)**. Нажмите клавишу [ENTER] для отображения **Меню 1.1— Настройка динамической DNS**, как показано ниже.

Рис. 112 Меню 1.1 — Настройка динамической DNS

```
                Menu 1.1 - Configure Dynamic DNS
            Service Provider= WWW.DynDNS.ORG
            Active= No
            Host=
            EMAIL=
            USER=
            Password= ********
            Enable Wildcard= No

                Press ENTER to Confirm or ESC to Cancel:
```

Для настройки параметров динамической DNS выполните действия, приведенные в следующей таблице.

Табл. 75 Меню 1.1 — Настройка динамической DNS

ПОЛЕ	ОПИСАНИЕ
Service Provider (Провайдер услуг)	Это имя провайдера услуг динамической DNS (DYNDNS).
Active (Активировать)	Чтобы включить динамическую DNS, нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)** и затем нажмите клавишу [ENTER].
Host (Имя узла)	Введите имя домена, назначенное интернет-центру провайдером услуг динамической DNS.

Табл. 75 Меню 1.1 — Настройка динамической DNS

ПОЛЕ	ОПИСАНИЕ
EMAIL (Адрес электронной почты)	Введите адрес электронной почты.
User (Пользователь)	Введите имя пользователя.
Password- (Пароль)	Введите назначенный пароль.
Enable Wildcard (Включить шаблоны)	Интернет-центр поддерживает шаблоны DYNDNS. Нажмите клавишу [ПРОБЕЛ] и затем [ENTER], чтобы выбрать **Yes (Да)** или **No (Нет)**. Данное поле имеет значение **N/A (Не доступно)**, если вы выберете клиент DDNS в качестве провайдера услуг .
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Глава 20 Меню 2 — Настройка резервирования глобальной сети

В этой главе описывается настройка функции перенаправления трафика и резервного соединения с глобальной сетью через модем с помощью Меню 2 и 2.1.

20.1 Описание настройки резервирования глобальной сети

В этой главе описывается настройка интернет-центра для перенаправления трафика и создания резервных соединений.

20.2 Настройка резервного соединения через модем в Меню 2

Введите 2 в главном меню для перехода в меню 2.

Рис. 113 Меню 2 — Настройка резервирования глобальной сети

```
                        Menu 2 - Wan Backup Setup

                    Check Mechanism = DSL Link
                    Check WAN IP Address1 = 0.0.0.0
                    Check WAN IP Address2 = 0.0.0.0
                    Check WAN IP Address3 = 0.0.0.0
                      KeepAlive Fail Tolerance = 0
                      Recovery Interval(sec) = 0
                      ICMP Timeout(sec) = 0
                    Traffic Redirect = No

            Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 76 Меню 2 — Настройка резервирования глобальной сети

ПОЛЕ	ОПИСАНИЕ
Check Mechanism (Проверка алгоритма)	Нажмите [ПРОБЕЛ], затем нажмите [ENTER] для выбора способа, который используется интернет-центром для проверки соединения DSL. Выберите **DSL Link (Канал DSL)**, чтобы интернет-центр проверял соединение DSL на физическом уровне. Выберите **ICMP** (Internet Control Message Protocol — Протокол управляющих сообщений в сети Интернет), чтобы интернет-центр периодически выполнял эхо-тестирование IP-адресов, введенных в полях **Check WAN IP Address (Проверять IP-адрес глобальной сети)**.
Check WAN IP Address1-3 (Проверять IP-адреса глобальной сети 1-3)	Заполните эти поля, чтобы интернет-центр проверял доступность глобальной сети. Введите IP-адрес ближайшего надежного компьютера (например, адрес сервера DNS Интернет-провайдера). При использовании резервного соединения с глобальной сетью интернет-центр периодически проводит эхо-тестирование заданных здесь адресов и, если не получает ответа, использует другое резервное соединение (если таковое настроено).
KeepAlive Fail Tolerance (Допуск на отказы)	Введите число (рекомендуется 2), которое показывает, сколько раз интернет-центр будет выполнять эхо-тестирование IP-адресов, введенных в поле **Check WAN IP Address (Проверять IP-адреса глобальной сети)** при отсутствии ответа, прежде чем переключиться на какое-либо из резервных соединений.
Recovery Interval (sec) (Интервал восстановления, с)	Когда интернет-центр использует соединение с более низким приоритетом (обычно резервное соединение с глобальной сетью), устройство периодически проверяет, можно или нет перейти на соединение с более высоким приоритетом. Введите интервал между проверками в секундах (рекомендуется 30). Увеличьте время, если в устройстве с IP-адресом получателя обрабатывается большой объем трафика.
ICMP Timeout (Время ожидания ICMP)	Введите время в секундах, необходимое для ожидания ответа ICMP для сеанса ICMP .

Табл. 76 Меню 2 — Настройка резервирования глобальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
Traffic Redirect (Перенаправление трафика)	Нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)** или **No (Нет)**. Выберите **Yes (Да)** и нажмите [ENTER] для настройки **Меню 2.1 Traffic Redirect Setup (Настройка перенаправления трафика)**. Выберите **No (Нет)** (по умолчанию), если не требуется настраивать эту функцию.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "`Press ENTER to Confirm or ESC to Cancel:`" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

20.2.1 Настройка перенаправления трафика

Меню 2.1 — Traffic Redirect Setup (Настройка перенаправления трафика) используется для настройки параметров, которые определяют, в каком случае интернет-центр направляет трафик глобальной сети на резервный шлюз.

Рис. 114 Меню 2.1 — Настройка перенаправления трафика

```
                    Menu 2.1 - Traffic Redirect Setup
                Active= No
                Configuration:
                  Backup Gateway IP Address= 0.0.0.0
                  Metric= 15

                Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 77 Меню 2.1 — Настройка перенаправления трафика

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Нажмите [ПРОБЕЛ] и выберите **Yes** (для включения) или **No** (для отключения) функции перенаправления трафика. По умолчанию установлено **No**.
Configuration (Настройка)	
Backup Gateway IP Address (IP-адрес резервного шлюза)	Введите IP-адрес резервного шлюза в десятичном формате с разделительными точками. Интернет-центр автоматически пересылает трафик на этот IP-адрес при разрыве подключения к Интернету.

Табл. 77 Меню 2.1 — Настройка перенаправления трафика

ПОЛЕ	ОПИСАНИЕ
Metric (Метрика)	В этом поле устанавливается приоритет маршрутов, которые использует интернет-центр. Метрика представляет собой "стоимость передачи данных". Маршрутизатор определяет наилучший маршрут для передачи, выбирая путь с самой низкой "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве единицы "стоимости", минимальное значение которой равно 1 и соответствует прямому соединению между сетями. Число, определяющее стоимость, должно лежать в интервале от "1" до "15"; значение больше "15" означает, что канал не работает. Чем меньше число, тем ниже "стоимость".
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Глава 21
Меню 3 — Настройка локальной сети

В этой главе описывается настройка параметров проводной локальной сети.

21.1 Настройка локальной сети

В данном разделе описывается настройка сети Ethernet с помощью **Меню 3 — Настройка локальной сети**. В главном меню введите 3 для перехода в меню 3.

Рис. 115 Меню 3 — Настройка локальной сети

```
Menu 3 - LAN Setup

1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup

5. Wireless LAN Setup

Enter Menu Selection Number:
```

21.1.1 Настройка сети Ethernet — общие настройки

Данное меню позволяет установить набор(-ы) фильтров, которые необходимо применять к трафику Ethernet. Необходимость в фильтрации трафика Ethernet возникает редко; тем не менее, наборы фильтров могут быть полезными для блокировки определенных пакетов, снижения объема трафика и предотвращения несанкционированного доступа.

Рис. 116 Меню 3.1 — Настройка фильтра порта LAN

```
            Menu 3.1 - LAN Port Filter Setup

              Input Filter Sets:
                protocol filters=
                device filters=
              Output Filter Sets:
                protocol filters=
                device filters=

            Press ENTER to Confirm or ESC to Cancel:
```

Если требуется информация по созданию фильтров, то сначала следует ознакомиться с Гл. 29 на с. 310, а затем вернуться к данному меню для настройки наборов фильтров.

21.2 Настройка Ethernet в зависимости от используемого протокола

В зависимости от протоколов, используемых для ваших задач, необходимо выполнить соответствующую настройку Ethernet, как описывается далее.

- Настройка TCP/IP порта Ethernet
- Настройка моста Ethernet

21.3 Настройка TCP/IP и DHCP для Ethernet

Меню 3.2 используется для настройки TCP/IP в интернет-центре.

Для редактирования меню 3.2, в главном меню введите 3 для перехода в **Меню 3 — Настройка локальной сети**. В меню 3 нажмите клавишу" 2" и затем нажмите [ENTER] для отображения **Меню 3.2 — TCP/IP and DHCP Ethernet Setup (Настройка TCP/IP и DHCP для Ethernet)**, как показано ниже:

Рис. 117 Меню 3.2 — Настройка TCP/IP и DHCP для Ethernet

```
                    Menu 3.2 - TCP/IP and DHCP Setup

                DHCP Setup
                  DHCP= Server
                  Client IP Pool Starting Address= 192.168.1.33
                  Size of Client IP Pool= 32
                  Primary DNS Server= 0.0.0.0
                  Secondary DNS Server= 0.0.0.0
                  Remote DHCP Server= N/A
                TCP/IP Setup:
                  IP Address= 192.168.1.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= None
                    Version= N/A
                  Multicast= None
                  IP Policies=
                  Edit IP Alias= No

                Press ENTER to Confirm or ESC to Cancel:
```

Для настройки полей DHCP выполните действия, представленные в следующей таблице.

Табл. 78 Настройка DHCP для Ethernet

ПОЛЕ	ОПИСАНИЕ
DHCP Setup (Настройка DHCP)	
DHCP	Если в этом поле установлено значение **Server (Сервер)**, интернет-центр может назначать IP-адреса, шлюз IP 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)**, интернет-центр работает в качестве фиктивного сервера DHCP и ретранслирует запросы и ответы DHCP между удаленным сервером и клиентами. В данном случае необходимо ввести IP-адрес фактического удаленного сервера DHCP в поле Remote DHCP Server (Удаленный сервер DHCP). Если используется сервер DHCP, необходимо установить следующие параметры:
Client IP Pool Starting Address (Начальный IP-адрес клиентского диапазона)	В этом поле вводится первый адрес из непрерывного диапазона IP-адресов.
Size of Client IP Pool (Размер диапазона IP-адресов клиентов)	В этом поле устанавливается размер непрерывного диапазона IP-адресов.

Табл. 78 Настройка DHCP для Ethernet (продолжение)

ПОЛЕ	ОПИСАНИЕ
Primary DNS Server (Основной сервер DNS) Secondary DNS Server (Дополнительный сервер DNS)	Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Remote DHCP Server (Удаленный сервер DHCP)	Если в поле **DHCP** выбрано значение **Relay (Ретранслятор)**, следует ввести IP-адрес фактического удаленного сервера DHCP.

Для настройки параметров TCP/IP порта Ethernet выполните действия, представленные в следующей таблице.

Табл. 79 Настройка TCP/IP порта Ethernet

ПОЛЕ	ОПИСАНИЕ
TCP/IP Setup (Настройка TCP/IP)	
IP Address (IP-адрес)	Введите IP-адрес (в локальной сети) интернет-центра в десятичном формате с разделительными точками.
IP Subnet Mask (Маска IP подсети)	Интернет-центр вычисляет маску подсети автоматически на основе назначенного IP-адреса. Если организация подсетей не требуется, следует использовать маску подсети, вычисленную интернет-центром (более подробно описано в приложениях).
RIP Direction (Направление RIP)	Нажмите клавишу [ПРОБЕЛ] для выбора направления RIP. Вариантами являются: **None (Нет)**, **Both (Оба)**, **In Only (Только входящие)** или **Out Only (Только исходящие)**.
Version (Версия)	Нажмите клавишу [ПРОБЕЛ] для выбора версии RIP. Вариантами являются: **RIP-1**, **RIP-2B** или **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. Интернет-центр поддерживает как версию 1 (**IGMP-v1**), так и версию 2 (**IGMP-v2**). Нажмите клавишу [ПРОБЕЛ] для включения многоадресной рассылки IP или выберите **None (Нет)** для отключения этой функции.
Политики IP	С помощью меню SMT 25 создайте политики IP и примените их к порту LAN интернет-центра путем ввода их номеров в это поле. Можно применить до четырех наборов политик IP (из двенадцати), вводя их номера через запятую.
Edit IP Alias (Редактирование псевдонима IP)	Интернет-центр поддерживает три логических порта локальной сети на одном физическом порте Ethernet, при этом сам интернет-центр является шлюзом для каждой логической сети. Нажмите клавишу [ПРОБЕЛ] для изменения **No** на **Yes** и затем нажмите [ENTER] для перехода в меню 3.2.1.

Глава 22
Настройка беспроводной локальной сети

В этой главе описывается настройка беспроводной локальной сети в Меню 3.5 для P–660HTW EE.

22.1 Описание беспроводной локальной сети

Вводную информацию об экранах настройки беспроводной локальной сети см. в главе "Беспроводная локальная сеть (WLAN)".

22.2 Настройка беспроводной локальной сети

Для настройки интернет-центра в качестве беспроводной точки доступа используйте Меню 3.5. Для редактирования меню 3.5 в главном меню введите 3 для перехода в **Меню 3 — Настройка локальной сети**. В Меню 3 нажмите 5 и затем клавишу [ENTER] для перехода в **Меню 3.5 — Wireless LAN Setup (Настройка беспроводной локальной сети)**, как показано ниже.

Рис. 118 Меню 3.5 — Настройка беспроводной локальной сети

```
            Menu 3.5- Wireless LAN Setup
                        ESSID= Wireless
                        Hide ESSID= No
                        Channel ID= CH06 2437MHz
                        RTS Threshold= 2432
                        Frag. Threshold= 2432
                        WEP= Disable
                          Default Key= N/A
                          Key1= N/A
                          Key2= N/A
                          Key3= N/A
                          Key4= N/A
                        Edit MAC Address Filter= No

            Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 80 Меню 3.5 — Настройка беспроводной локальной сети

ПОЛЕ	ОПИСАНИЕ
ESSID	The ESSID (Extended Service Set IDentifier — Идентификатор расширенного набора служб) определяет точку доступа, с которой связаны беспроводные устройства. Беспроводные устройства, подключенные к точке доступа должны иметь одинаковый ESSID. Введите описательное имя (не более 32 печатных 7-битных знаков ASCII).
Hide ESSID (Скрыть ESSID)	Нажмите клавишу [ПРОБЕЛ] и выберите **Yes (Да)**,чтобы скрыть ESSID в исходящем сигнальном кадре (кадре-маяке) для того, чтобы устройство не могло обнаружить ESSID при помощи пассивного сканирования.
Channel ID (Идентификатор канала)	Нажмите клавишу [ПРОБЕЛ] для выбора канала. Это позволяет установить рабочую частоту/канал в зависимости от Вашего региона.
RTS Threshold (Порог RTS)	Порог RTS (Request To Send — Запрос на передачу) (количество байт) предназначен для включения механизма квитирования RTS/CTS. Данные, размер кадра которых превышает это значение, проходят квитирование RTS/CTS. Установка этого значения больше максимального размера MSDU (Сервисного блока данных MAC) выключает квитирование RTS/CTS. Установка значения, равного нулю приведет к включению квитирования RTS/CTS. Введите значение от 0 до 2432.
Frag. Threshold (Порог фрагментации)	Порог (количество байт) фрагментации для направленных сообщений. Это максимальный размер фрагмента данных, который можно послать. Введите значение от 256 до 2432.
WEP (Протокол шифрования WEP)	WEP (Wired Equivalent Privacy — Конфиденциальность эквивалентная проводным сетям) обеспечивает шифрование данных, препятствующее доступу беспроводных устройств к передаваемым через беспроводную сеть данным. Выберите **Disable (Отключить)** для того, чтобы беспроводные устройства поддерживали связь с точками доступа без шифрования данных. Выберите **64-bit WEP** или **128-bit WEP** для ввода шифрования данных. WEP вызывает снижение скорости соединения.
Default Key (Ключ по умолчанию)	Введите номер ключа в качестве активного ключа.

Табл. 80 Меню 3.5 — Настройка беспроводной локальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
Key 1 - Key 4 (Ключ 1 — Ключ 4)	При выборе **64-bit WEP** в поле **WEP Encryption (WEP-шифрование)** введите 5 символов или 10 шестнадцатиричных символов ("0-9", "A-F"),начинающихся с символа 0x. При выборе **128-bit WEP** в поле **WEP Encryption (WEP-шифрование)** введите 13 символов или 26 шестнадцатиричных символов ("0-9", "A-F"),начинающихся с символа 0x.. Существует четыре ключа шифрования данных для защиты данных от несанкционированного получения неправомочными беспроводными пользователями. Как для точек доступа, так и для беспроводных устройств должны быть установлены одинаковые значения ключей.
Edit MAC Address Filter (Редактирование фильтра MAC-адресов)	Для редактирования таблицы фильтрации MAC-адресов, нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, а затем нажмите клавишу [ENTER] для вывода Меню 3.5.1.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

22.2.1 Фильтр MAC-адресов для беспроводной локальной сети

Следующий уровень безопасности — фильтр MAC-адресов. Для того чтобы разрешить соединение беспроводного устройства с интернет-центром, введите MAC-адрес сетевого беспроводного адаптера в таблицу MAC-адресов.

Рис. 119 Меню 3.5.1 Фильтр MAC-адресов беспроводной сети

```
                  Menu 3.5.1 - WLAN MAC Address Filter
                Active= No
                Filter Action= Allowed Association
------------------------------------------------------------------------
  1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
  2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
  3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
  4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
  5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
  6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
  7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
  8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
  9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
 10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
 11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
 12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
------------------------------------------------------------------------
                  Enter here to CONFIRM or ESC to CANCEL:
```

В следующей таблице описываются поля данного меню.

Табл. 81 Меню 3.5.1 Фильтр MAC-адресов беспроводной сети

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Для включения фильтрации MAC-адресов, нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, а затем нажмите [ENTER].
Filter Action (Действие фильтра)	Определите способ фильтрации для списка MAC-адресов в таблице фильтрации MAC-адресов. Для запрета доступа к интернет-центру, нажмите клавишу [ПРОБЕЛ] для выбора **Deny Association (Запретить подключение)**и нажмите клавишу [ENTER]. MAC-адресам, не указанным в списке, будет разрешен доступ к маршрутизатору. Действие по умолчанию, **Allowed Association (Разрешить подключение)**, разрешает соединение с интернет-центром. MAC-адресам, не указанным в списке, будет отказано в доступе к маршрутизатору.
MAC Address Filter (Фильтрация MAC-адресов)	
Address 1. (Адрес 1)	В полях адресов введите MAC-адреса (в формате XX:XX:XX:XX:XX:XX) беспроводных устройств, которым разрешено или отказано в доступе к интернет-центру.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Глава 23
Доступ в Интернет

В данной главе описывается настройка в интернет-центре параметров локальной и глобальной сети для доступа в Интернет.

23.1 Описание доступа в Интернет

Для более подробной информации по настройке полей в меню SMT, которые описываются в этой главе, см. главы с описанием Мастера установки Web-конфигуратора, а также окон настройки локальной и глобальной сети.

23.2 Политики IP (IP Policies)

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. Маршрутизация на основе политики, применяемая к входящим пакетам каждого порта, имеет приоритет перед стандартной маршрутизацией. В Меню 25 SMT можно создать политики маршрутизации и применить их к портам интернет-центра LAN и/или WAN с помощью меню 3.2 (LAN) и 11.3 (WAN).

23.3 Псевдоним IP (IP Alias)

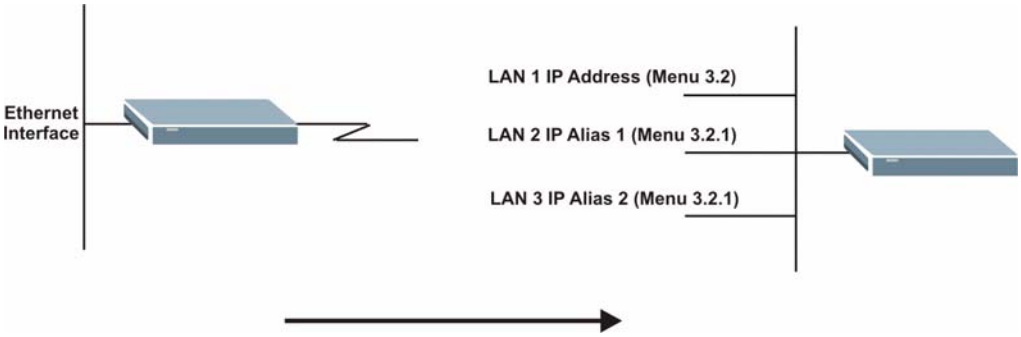
Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей на основе одного порта Ethernet. Интернет-центр поддерживает три логических порта локальной сети на одном физическом порте Ethernet, при этом сам интернет-центр является шлюзом для каждой логической сети.

Если используется псевдоним IP, можно также настроить правила межсетевого экрана для контроля доступа к логическим сетям (подсетям) локальной сети.

ПРИМЕЧАНИЕ: Необходимо следить, чтобы логические сети не перекрывались.

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

Рис. 120 Пример сети с использованием псевдонимов IP



Для настройки псевдонимов IP в интернет-центре используется Меню 3.2.1.

23.4 Создание псевдонимов IP

Настройте первую сеть с помощью Меню 3.2. Переместите курсор в поле **Edit IP Alias (Редактировать псевдоним IP)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**, затем нажмите [ENTER] для настройки второй и третьей сети.

Рис. 121 Меню 3.2 — Настройка TCP/IP и DHCP

```
                Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
    Version= N/A
  Multicast= None
  IP Policies=
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:
```

При нажатии клавиши [ENTER] открывается **Меню 3.2.1 — Настройка псевдонима IP**, как показано ниже.

Рис. 122 Меню 3.2.1 — Настройка псевдонима IP

```
            Menu 3.2.1 - IP Alias Setup
              IP Alias 1= No
                IP Address= N/A
                IP Subnet Mask= N/A
                RIP Direction= N/A
                Version= N/A
                Incoming protocol filters= N/A
                Outgoing protocol filters= N/A
              IP Alias 2= No
                IP Address= N/A
                IP Subnet Mask= N/A
                RIP Direction= N/A
                Version= N/A
                Incoming protocol filters= N/A
                Outgoing protocol filters= N/A

                 Enter here to CONFIRM or ESC to CANCEL:
```

Для настройки параметров псевдонима IP выполните действия, приведенные в следующей таблице.

Табл. 82 Меню 3.2.1 — Настройка псевдонима IP

ПОЛЕ	ОПИСАНИЕ
IP Alias (Псевдоним IP)	Выберите **Yes (Да)** для настройки локальной сети в интернет-центре.
IP Address (IP-адрес)	Введите IP-адрес интернет-центра в десятичном формате с разделительными точками.
IP Subnet Mask (Маска IP подсети)	Интернет-центр вычисляет маску подсети автоматически на основе назначенного IP-адреса. Если организация подсетей не требуется, следует использовать маску подсети, вычисленную интернет-центром
RIP Direction (Направление RIP)	Нажмите клавишу [ПРОБЕЛ] для выбора направления RIP. Вариантами являются: **None (Нет)**, **Both (Оба)**, **In Only (Только входящие)** или **Out Only (Только исходящие)**.
Version (Версия)	Нажмите клавишу [ПРОБЕЛ] для выбора версии RIP. Вариантами являются: **RIP-1**, **RIP-2B** или **RIP-2M**.
Incoming Protocol Filters (Фильтры входных протоколов)	Введите набор(-ы) фильтров, которые должны применяться к входящему трафику между данным узлом и интернет-центром.
Outgoing Protocol Filters (Фильтры выходных протоколов)	Введите набор(-ы) фильтров, которые должны применяться к исходящему трафику между данным узлом и интернет-центром.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

23.5 Настройка маршрута IP

Сначала необходимо включить функцию маршрутизации IP в **Меню 1 — Настройка общих параметров**.

Для редактирования Меню 1, в главном меню введите 1 и нажмите клавишу [ENTER]. Установите **Yes (Да)** в поле **Route IP (Маршрут IP)** с помощью нажатия клавиши [ПРОБЕЛ].

Рис. 123 Меню 1 — Настройка общих параметров

```
Menu 1 - General Setup
           System Name= ?
           Location= location
           Contact Person's Name=
           Domain Name=
           Edit Dynamic DNS= No
           Route IP= Yes
           Bridge= No

Press ENTER to Confirm or ESC to Cancel:
```

23.6 Настройка доступа в Интернет

Меню 4 позволяет ввести все параметры доступа в Интернет в одном окне. Фактически, Меню 4 представляет собой упрощенную настройку для одного из удаленных узлов, к которым можно получить доступ через Меню 11. Прежде, чем выполнять настройку интернет-центра для доступа в Интернет, необходимо получить учетные данные для подключения к Интернету.

Используйте таблицу *Параметры учетной записи Интернет* в *Кратком руководстве* для внесения учетной информации Интернет. Если используется инкапсуляция PPPoA или PPPoE, то потребуется ввести только регистрационное имя и пароль, предоставляемые Интернет-провайдером. Если используется инкапсуляция ENET ENCAP, то потребуется ввести только IP-адрес шлюза инкапсуляции Ethernet.

В Главном меню, введите 4 для входа в **Меню 4 — Настройка доступа в Интернет**, как показано ниже.

Рис. 124 Меню 4 — Настройка доступа в Интернет

```
Menu 4 - Internet Access Setup
  ISP's Name= MyISP
  Encapsulation= RFC 1483
  Multiplexing= LLC-based
  VPI #= 8
  VCI #= 35
  ATM QoS Type= CBR
    Peak Cell Rate (PCR)= 0
    Sustain Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
  My Login= N/A
  My Password= N/A
  ENET ENCAP Gateway= N/A
  IP Address Assignment= Static
    IP Address= 0.0.0.0
  Network Address Translation= SUA Only
    Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице содержатся указания по настройке интернет-центра для доступа в Интернет.

.

Табл. 83 Меню 4 — Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ
ISP’s Name (Имя Интернет-провайдера)	Введите имя вашего Интернет-провайдера. (Эта информация используется только в целях идентификации).
Encapsulation (Инкапсуляция)	Нажмите клавишу [ПРОБЕЛ] для выбора метода инкапсуляции, который используется вашим Интернет-провайдером. Вариантами являются: **PPPoE**, **PPPoA**, **RFC 1483** или **ENET ENCAP**.
Multiplexing (Мультиплексирование)	Нажмите клавишу [ПРОБЕЛ] для выбора метода мультиплексирования, который используется вашим Интернет-провайдером. Вариантами являются: **VC-based (на базе VC)** или **LLC-based (на базе LLC)**.
VPI # (Номер VPI)	Введите назначенный номер VPI (Virtual Path Identifier — Идентификатор виртуального пути).
VCI # (Номер VCI)	Введите назначенный номер VCI (Virtual Channel Identifier — Идентификатор виртуального канала).
ATM QoS Type (Тип качества обслуживания ATM)	Нажмите клавишу [ПРОБЕЛ] и выберите **CBR** (Continuous Bit Rate — постоянная скорость передачи), чтобы установить постоянную (всегда доступную) пропускную способность. Выберите **UBR** (Unspecified Bit Rate — Неопределенная скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите **VBR** (Variable Bit Rate — Переменная скорость передачи) для пульсирующего трафика и разделения пропускной способности с другими приложениями.
Peak Cell Rate (PCR) (Пиковая скорость ячеек)	Это максимальная скорость, с которой отправитель может передавать ячейки. Введите пиковую скорость ячеек.

Табл. 83 Меню 4 — Настройка доступа в Интернет (продолжение)

ПОЛЕ	ОПИСАНИЕ
Sustain Cell Rate (SCR) (Поддерживаемая скорость ячеек)= 0	SCR (Sustained Cell Rate — поддерживаемая скорость ячеек) это средняя скорость ячеек источника пульсирующего трафика типа "есть-нет", который может передаваться с пиковой скоростью и является параметром пульсирующего трафика. Введите поддерживаемую скорость ячеек. SCR должно быть меньше, чем PCR.
Maximum Burst Size (MBS) (Максимальный размер пакета)= 0	MBS — это максимальное количество ячеек, которое может быть передано с пиковой скоростью. Введите максимальный размер пакета. Значение должно быть меньше 65535.
My Login (Имя пользователя)	Поля **My Login (Имя пользователя)** и **My Password (Пароль)** заполняются только при использовании инкапсуляции PPPoA и PPPoE. Введите регистрационное имя, предоставленное Интернет-провайдером. Если используется инкапсуляция PPPoE**,** это поле имеет формат user@domain, где domain определяет имя услуги PPPoE.
My Password (Пароль)	Введите пароль для данного регистрационного имени.
ENET ENCAP Gateway (Шлюз ENET ENCAP)	Если используется инкапсуляция **ENET ENCAP**, введите IP-адрес шлюза, предоставленный Интернет-провайдером.
Idle Timeout (Время простоя)	Значение в этом поле определяет интервал простоя в секундах, по истечении которого интернет-центр автоматически завершает сеанс связи PPPoE.
IP Address Assignment (Назначение IP-адреса)	Нажмите клавишу [ПРОБЕЛ], чтобы выбрать **Static (Статический)** или **Dynamic (Динамический)** IP адрес.
IP Address (IP-адрес)	Введите IP-адрес, предоставленный Интернет-провайдером (если требуется).
Network Address Translation (Трансляция сетевых адресов)	Нажмите клавишу [ПРОБЕЛ], чтобы выбрать режим NAT: **None (Нет)**, **SUA Only (Только SUA)** или **Full Feature (Полный набор функциональных возможностей)**. Для получения более подробной информации по функции SUA (Single User Account — Учетная запись одиночного пользователя), см. главу "Трансляция сетевых адресов (NAT)".
Address Mapping Set (Набор отображения адресов)	Введите номера наборов отображения (от 1 до 8) для использования с NAT.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Если все настройки верны, интернет-центр должен автоматически подключиться к сети Интернет. Если при подключении происходит сбой, на экран выводится сообщение об ошибке, с помощью которого необходимо предпринять соответствующие меры для устранения неисправности.

Глава 24
Настройка удаленного узла

В данной главе описывается настройка удаленного узла.

24.1 Описание настройки удаленного узла

В данном разделе описываются протокольно-независимые параметры удаленного узла. Удаленный узел используется для отправки вызовов на удаленный шлюз. Удаленный узел функционирует как удаленный шлюз и как вход в сеть, которая за ним находится. При настройке доступа в Интернет в Меню 4 фактически настраиваются параметры одного из удаленных узлов.

Сначала выберите удаленный узел в **Меню 11- Настройка удаленного узла**. После этого можно редактировать профиль этого узла в Меню 11.1, а также настраивать конкретные параметры с помощью трех подменю: редактировать параметры IP и моста в Меню 11.3; редактировать параметры ATM в Меню 11.6; и редактировать наборы фильтров в Меню 11.5.

24.2 Настройка удаленного узла

В данном разделе описываются протокольно-независимые параметры удаленного узла.

24.2.1 Профиль удаленного узла

Для настройки удаленного узла выполните следующие действия:

1. В главном меню введите 11 для отображения **Меню 11 — Настройка удаленного узла.**
2. В Меню 11 введите номер удаленного узла, параметры которого необходимо настроить, как показано на следующем рисунке.

Рис. 125 Меню 11 — Настройка удаленного узла

```
                Menu 11 - Remote Node Setup
            1. MyISP (ISP, SUA)
            2. _________
            3. _________
            4. _________
            5. _________
            6. _________
            7. _________
            8. _________

                     Enter Node # to Edit:
```

24.2.2 Сценарии инкапсуляции и мультиплексирования

Для доступа в Интернет необходимо использовать методы инкапсуляции и мультиплексирования, используемые вашим 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 зависит также от количества имеющихся виртуальных каналов и от количества необходимых сетевых протоколов. При инкапсуляции ENET ENCAP требуется передача дополнительной служебной информации, что делает этот метод нерациональным для соединения локальных сетей. Далее приводится несколько примеров комбинирования методов, наиболее подходящих для такого применения.

24.2.2.1 Сценарий 1: один виртуальный канал, несколько 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.

24.2.2.2 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 будущем имеется потенциальная потребность поддержки нескольких протоколов, то правильнее выбрать инкапсуляцию **PPPoA**, вместо **RFC-1483**, так как в этом случае не придется заново настраивать все компьютеры.

24.2.2.3 Сценарий 3: несколько виртуальных каналов

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

Рис. 126 Меню 11.1 — Профиль удаленного узла

```
                Menu 11.1 - Remote Node Profile

    Rem Node Name= MyISP                  Route= IP
    Active= Yes                           Bridge= No
    Encapsulation= RFC 1483               Edit IP/Bridge= No
    Multiplexing= LLC-based               Edit ATM Options= No
    Service Name= N/A                     Edit Advance Options= N/A
    Incoming:                             Telco Option:
      Rem Login= N/A                        Allocated Budget(min)= N/A
      Rem Password= N/A                     Period(hr)= N/A
    Outgoing:                               Schedule Sets= N/A
      My Login= N/A                         Nailed-Up Connection= N/A
      My Password= N/A                    Session Options:
      Authen= N/A                           Edit Filter Sets= No
                                              Idle Timeout(sec)= N/A
    Press ENTER to Confirm or ESC to Cancel:
```

Заполните поля в **Меню 11.1 — Профиль удаленного узла**, как описывается в следующей таблице.

Табл. 84 Меню 11.1 — Профиль удаленного узла

ПОЛЕ	ОПИСАНИЕ
Rem Node Name (Имя удаленного узла)	Введите уникальное описательное имя для данного узла длиной до восьми символов.
Active (Активировать)	Нажмите клавишу [ПРОБЕЛ], затем клавишу [ENTER] для выбора **Yes (Да)**, чтобы включить, или **No (Нет)**, чтобы отключить данный узел. Неактивные узлы отображаются в Меню 11 SMT со знаком минус ("–").
Encapsulation (Инкапсуляция)	**PPPoA** относится к RFC-2364 (Инкапсуляция PPP по уровню 5 адаптации ATM). Если выбрана инкапсуляция RFC-1483 (многопротокольная инкапсуляция по уровню 5 адаптации ATM) **ENET ENCAP**, то поля **Rem Login (Имя пользователя удаленного узла)**, **Rem Password (Пароль удаленного узла)**, **My Login (Имя пользователя)**, **My Password (Пароль)** и **Authen (Аутентификация)** являются недоступными (**N/A**).
Multiplexing (Мульти-плексирование)	Нажмите клавишу [ПРОБЕЛ], затем клавишу [ENTER] для выбора метода мультиплексирования, используемого Интернет-провайдером: **на базе VC** или **на базе LLC**.
Service Name (Имя услуги)	В случае использования инкапсуляции **PPPoE**, введите название услуги PPPoE.
Incoming (Входящие вызовы):	
Rem Login (Регистрационное имя удаленного узла)	Введите регистрационное имя, которое данный удаленный узел будет использовать при вызове интернет-центра. Регистрационное имя и пароль удаленного узла (**Rem Password**) используются для аутентификации данного узла.
Rem Password (Пароль удаленного узла)	Введите пароль, который данный удаленный узел будет использовать при вызове интернет-центра.

Табл. 84 Меню 11.1 — Профиль удаленного узла (продолжение)

ПОЛЕ	ОПИСАНИЕ
Outgoing (Исходящие вызовы):	
My Login (Имя пользователя)	Введите регистрационное имя, назначенное Интернет-провайдером, которое интернет-центр будет использовать при вызове данного удаленного узла.
My Password (Пароль)	Введите пароль, назначенный Интернет-провайдером, который интернет-центр будет использовать при вызове данного удаленного узла.
Authen (Аутентификация)	В данном поле устанавливается протокол аутентификации, используемый для исходящих вызовов. Возможны следующие варианты:
	CHAP/PAP — интернет-центр будет осуществлять вызовы по протоколу **CHAP** или **PAP** при запросе от данного удаленного узла.
	CHAP — только вызовы **CHAP** (Challenge Handshake Authentication Protocol — Протокол аутентификации по методу "вызов-рукопожатие").
	PAP — только вызовы PAP (Password Authentication Protocol — Протокол аутентификации по паролю).
Route (Маршрут)	Данное поле определяет протокол, используемый при маршрутизации. Возможны варианты: **IP** и **None (Нет).**
Bridge (Мост)	Если функция моста включена, интернет-центр будет пересылать все пакеты, которые он не маршрутизирует, на данный удаленный узел. В другом случае, пакеты будут отбрасываться. Выберите **Yes (Да)** для включения или **No (Нет)** для отключения моста.
Edit IP/Bridge (Редактировать IP/мост)	Нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, затем нажмите клавишу [ENTER] для вывода **Меню 11.3 — Параметры сетевого уровня удаленного узла**.
Edit ATM Options (Редактирование параметров ATM)	Нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, затем нажмите клавишу [ENTER] для вывода **Меню 11.6 — Параметры уровня ATM удаленного узла**.
Edit Advance Options (Редактировать дополнительные параметры)	Это поле доступно, только если в поле **Encapsulation (Инкапсуляция)** установлено значение **PPPoE**. Нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, затем нажмите клавишу [ENTER] для вывода **Меню 11.8 — Настройка дополнительных параметров**.
Telco Option (Параметры телефонной компании)	
Allocated Budget (min) (Выделенный бюджет, мин.)	В этом поле устанавливается предельное значение времени для исходящих вызовов данного удаленного узла. По умолчанию установлено 0, т.е. контроль бюджета не ведется.
Period (hr) (Интервал, ч)	В этом поле устанавливается интервал времени, через который сбрасывается выделенный бюджет. Например, чтобы разрешить вызов данного удаленного узла не более 10 минут каждый час, установите значение 10 (минут) в поле **Allocated Budget (Выделенный бюджет)** и значение 1 (час) в поле **Period (Интервал)**.
Schedule Sets (Наборы расписаний)	Это поле доступно только при инкапсуляции **PPPoE** и **PPPoA**. Можно применять до четырех расписаний. Более подробную информацию см. в Гл. 37 на с. 384
Nailed up Connection (Постоянное соединение)	Это поле доступно только при инкапсуляции **PPPoE** и **PPPoA**. Данное поле определяет, является ли соединение с данным удаленным узлом постоянным соединением. Более подробная информация приведена ранее в этом разделе.

Табл. 84 Меню 11.1 — Профиль удаленного узла (продолжение)

ПОЛЕ	ОПИСАНИЕ
Session Options (Параметры сеанса связи)	
Edit Filter Sets (Редактирование наборов фильтров)	Нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, а затем нажмите клавишу [ENTER] и перейдите в Меню 11.5 для редактирования наборов фильтров. Более подробную информацию см. в Гл. 29 на с. 310.
Idle Timeout (sec) (Время простоя, с)	Введите интервал времени в секундах (0-9999), разрешенный для простоя (трафик к удаленному узлу отсутствует), по истечении которого интернет-центр автоматически завершает соединение с удаленным узлом. Значение 0 означает, что сеанс связи не ограничен по времени.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "`Press ENTER to Confirm or ESC to Cancel:`" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

24.2.3 Протокол аутентификации исходящих вызовов

По очевидным причинам рекомендуется использовать максимально надежный протокол аутентификации. Однако, в некоторых исполнениях оборудования профиль пользователя включает специальный протокол аутентификации. Если для такого устройства используемый протокол аутентификации отличается от протокола в профиле пользователя, соединение будет разорвано, даже если используемый протокол является более надежным, чем специальный. Если соединение разрывается сразу после успешной аутентификации, убедитесь, что используется соответствующий протокол аутентификации при подключении к такому устройству.

24.3 Параметры сетевого уровня удаленного узла

Для настройки параметров TCP/IP необходимо в **Меню 11.3 — Параметры сетевого уровня удаленного узла** выполнить следующие действия.

1. В Меню 11.1 убедитесь, что **IP** входит в число протоколов в поле **Route (Маршрут)**.
2. Переместите курсор в поле **Edit IP/IPX/Bridge (Редактировать IP/IPX/мост)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, а затем нажмите клавишу [Enter] для отображения **Меню 11.3 — Параметры сетевого уровня удаленного узла**.

Рис. 127 Меню 11.3 — Параметры сетевого уровня удаленного узла

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment = Static       Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= None
    Version= RIP-1
  Multicast= None
  IP Policies=

            Enter here to CONFIRM or ESC to CANCEL:
```

В следующей таблице описываются поля **Меню 11.3 — Параметры сетевого уровня удаленного узла**.

Табл. 85 Меню 11.3 — Параметры сетевого уровня удаленного узла

ПОЛЕ	ОПИСАНИЕ
IP Address Assignment (Назначение IP-адреса)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER], чтобы выбрать **Dynamic (Динамический)**, если удаленный узел использует динамически назначаемый IP-адрес, или **Static (Статический)**, если используется статический (постоянный) IP-адрес. Вы сможете настраивать этот параметр только в узле Интернет-провайдера (также можно использовать Меню 4), все остальные узлы установлены на использование **Static (Статический)**.
Rem IP Addr (IP-адрес удаленного узла)	IP-адрес, установленный в предыдущем меню.
Rem Subnet Mask (Маска подсети для удаленного узла)	Введите маску подсети, назначенную для удаленного узла.
My WAN Addr (Мой адрес в глобальной сети)	В некоторых реализациях, в частности на базе UNIX, необходимо обеспечить отдельные номера сетей IP для соединений WAN и LAN, и каждое окончание должно иметь уникальный адрес внутри номера сети. В таком случае, введите IP-адрес, назначенный порту WAN интернет-центра. ПРИМЕЧАНИЕ: Это относится к локальному адресу интернет-центра, но не к адресу удаленного маршрутизатора.
NAT	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER], чтобы выбрать **Full Feature (Полный набор функциональных возможностей)**, если интернет-центр имеет несколько общедоступных IP-адресов в глобальной сети.
	Выберите **SUA Only (Только SUA)**, если интернет-центр имеет только один общедоступный IP-адрес в глобальной сети. В SMT используется набор отображения адресов 255 (см. Рис. 145 на с. 293). Выберите **None (Нет)** для отключения функции NAT.

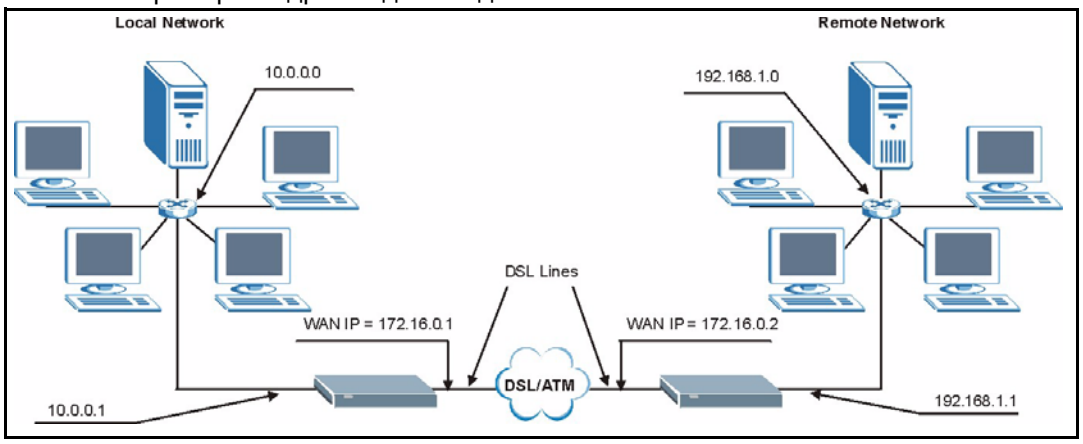
Табл. 85 Меню 11.3 — Параметры сетевого уровня удаленного узла (продолжение)

ПОЛЕ	ОПИСАНИЕ
Address Mapping Set (Набор отображения адресов)	Если в поле **NAT** установлено значение **Full Feature (Полный набор функциональных возможностей)**, настройте наборы отображения адресов в Меню 15.1. Выберите один из наборов серверов NAT (от 2 до 10) в Меню 15.2 (более подробную информацию см. в Гл. 27 на с. 290) и введите его номер в это поле. Если в поле **NAT** установлено значение **SUA Only (Только SUA)**, в SMT используется набор серверов NAT 1 в Меню 15.2 (более подробную информацию см. в Гл. 27 на с. 290).
Metric (Метрика)	Метрика определяет "стоимость" передачи и используется для целей маршрутизации. При маршрутизации IP в качестве единицы "стоимости" используется счетчик переходов по сети, при этом минимальное значение "стоимости" равно 1 и соответствует прямому соединению между сетями. Введите число, которое будет приблизительно выражать "стоимость" трафика для данного канала. Число не обязательно должно быть точным, но должно находиться в диапазоне от 1 до 15. В большинстве случаев хорошо подходит значение 2 или 3.
Private (Частный адрес)	Этот параметр определяет, будет ли интернет-центр включать маршрут к этому удаленному узлу в свою широковещательную рассылку RIP. Если установлено **Yes (Да)**, данный маршрут считается частным и не включается в широковещательную рассылку RIP. Если установлено **No (Нет)**, маршрут к этому удаленному узлу является доступным для других узлов через широковещательную рассылку RIP.
RIP Direction (Направление RIP)	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER] для выбора направления RIP. Вариантами являются: **Both (Оба направления)**, **In Only (Только входящие)**, **Out Only (Только исходящие)** или **None (Нет)**.
Version (Версия)	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER] для выбора версии RIP. Вариантами являются: **RIP-1**, **RIP-2B** или **RIP-2M**.
Multicast (Многоадресная рассылка)	Значение **IGMP-v1** устанавливает версию 1 IGMP, **IGMP-v2** устанавливает версию 2 IGMP, а **None (Нет)** отключает IGMP.
IP Policies (Политики IP)	Можно применять до четырех наборов политик IP (из 12), номера которых вводятся через запятую. Сначала создайте наборы фильтров в Меню 25 (см. Гл. 36 на с. 374), а затем примените их в этом поле.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

24.3.1 IP-адреса в поле My WAN Addr (Мой адрес в глобальной сети)

На следующем рисунке показан пример использования IP-адресов, который разъясняет заполнение поля **My WAN Addr (Мой адрес в глобальной сети)** в Меню 11.3. Поле **My WAN Addr (Мой адрес в глобальной сети)** показывает IP-адрес локального интернет-центра в глобальной сети (172.16.0.1 на следующем рисунке), а поле **Rem IP Addr (IP-адрес удаленного узла)** показывает IP-адрес в глобальной сети такого же удаленного устройства (172.16.0.2 на следующем рисунке).

Рис. 128 Пример IP-адресов для соединения локальных сетей на базе TCP/IP



24.4 Фильтр удаленного узла

В Меню 11.1 переместите курсор в поле **Edit Filter Sets (Редактировать наборы фильтров)**, а затем нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**. Затем нажмите клавишу [ENTER] для вывода **Меню 11.5 — Фильтр удаленного узла**.

В **Меню 11.5 — Фильтр удаленного узла** установите набор(-ы) фильтров для применения к входящему и исходящему трафику между данным удаленным узлом и интернет-центром, а также для предотвращения инициирования вызовов конкретными пакетами. Можно применять до 4 наборов фильтров для каждого типа фильтра, номера которых вводятся через запятую, например, 1, 5, 9, 12.

При заполнении данного поля допускается использование пробелов. Интернет-центр имеет готовый набор фильтров NetBIOS_WAN, который блокирует пакеты NetBIOS. Его можно включить в набор фильтров вызовов, если вы не хотите, чтобы пакеты NetBIOS инициировали вызовы удаленного узла.

Рис. 129 Меню 11.5 — Фильтр удаленного узла (инкапсуляция RFC 1483 или ENET)

```
            Menu 11.5 - Remote Node Filter
                     Input Filter Sets:
                       protocol filters=
                         device filters=
                     Output Filter Sets:
                       protocol filters=
                         device filters=

            Enter here to CONFIRM or ESC to CANCEL:
```

Рис. 130 Меню 11.5 — Фильтр удаленного узла (инкапсуляция RFC или ENET)

```
                Menu 11.5 - Remote Node Filter
            Input Filter Sets:
              protocol filters=
                device filters=
            Output Filter Sets:
              protocol filters=
                device filters=
            Call Filter Sets:
              protocol filters=
                device filters=

             Enter here to CONFIRM or ESC to CANCEL:
```

24.5 Редактирование параметров уровня ATM

Для редактирования **Меню 11.6 — Параметры уровня ATM удаленного узла** выполните следующие действия.

В Меню 11.1 переместите курсор в поле **Edit ATM Options (Редактирование параметров ATM)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**. Нажмите клавишу [ENTER] для отображения **Меню 11.6 — Параметры уровня ATM удаленного узла**.

Вид Меню 11.6 имеет два варианта в зависимости от выбранного в Меню 11.1 метода мультиплексирования: **на базе VC** или **на базе LLC** и инкапсуляции **PPP**.

24.5.1 Мультиплексирование на базе VC (не-PPP инкапсуляция)

При мультиплексировании **на базе VC** по предварительному соглашению каждому протоколу назначается отдельный виртуальный канал, например, по VC1 передается IP. Для каждого протокола должны быть заданы отдельные номера VPI и VCI.

Рис. 131 Меню 11.6 — Мультиплексирование на базе VC

```
          Menu 11.6 – Remote Node ATM Layer Options
          VPI/VCI (VC-Multiplexing)

VC Options for IP:             VC Options for Bridge:
  VPI #= 8                       VPI #= 1
  VCI #= 35                      VCI #= 36
  ATM QoS Type= UBR              ATM QoS Type= N/A
  Peak Cell Rate (PCR)= 0        Peak Cell Rate (PCR)= N/A
  Sustain Cell Rate (SCR)= 0     Sustain Cell Rate (SCR)= N/A
  Maximum Burst Size (MBS)= 0    Maximum Burst Size (MBR)= N/A

              Enter here to CONFIRM or ESC to CANCEL:
```

24.5.2 Мультиплексирование на базе LLC или инкапсуляция PPP

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.

Рис. 132 Меню 11.6 — Мультиплексирование на базе LLC или инкапсуляция PPP

```
          Menu 11.6 - Remote Node ATM Layer Options
          VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)
                              VPI #= 0
                              VCI #= 38
                              ATM QoS Type= UBR
                              Peak Cell Rate (PCR)= 0
                              Sustain Cell Rate (SCR)= 0
                              Maximum Burst Size (MBS)= 0

          ENTER here to CONFIRM or ESC to CANCEL:
```

В этом случае для всех протоколов нужно указать только один набор номеров VPI и VCI. Допустимый диапазон для номеров VPI — от 0 до 255, а для VCI — от 32 до 65535 (номера от 1 до 31 зарезервированы для локального управления трафиком ATM).

24.5.3 Параметры дополнительной настройки

В Меню 11.1 в поле **Encapsulation (Инкапсуляция)** выберите **PPPoE**.

Рис. 133 Меню 11.1 — Профиль удаленного узла

```
                  Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP                  Route= IP
Active= Yes                           Bridge= No
Encapsulation= PPPoE                Edit IP/Bridge= No
Multiplexing= LLC-based               Edit ATM Options= No
Service Name=                         Edit Advance Options= Yes
Incoming:                             Telco Option:
  Rem Login=                            Allocated Budget(min)= 0
  Rem Password= ********                Period(hr)= 0
Outgoing:                               Schedule Sets=
  My Login= ?                           Nailed-Up Connection= No
  My Password= ?                      Session Options:
  Authen= CHAP/PAP                      Edit Filter Sets= No
                                        Idle Timeout(sec)= 0

                Press ENTER to Confirm or ESC to Cancel:
```

Переместите курсор в поле **Edit Advance Options (Редактировать дополнительные параметры)** и нажмите [ПРОБЕЛ] для выбора **Yes**, затем нажмите [ENTER] для отображения **Меню 11.8 — Параметры дополнительной настройки**.

Рис. 134 Меню 11.8 — Параметры дополнительной настройки

```
                        Menu 11.8 - Advance Setup Options

                    PPPoE pass-through= No

                    Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 86 Меню 11.8 — Параметры дополнительной настройки

ПОЛЕ	ОПИСАНИЕ
PPPoE pass-through (Транзит PPPoE-соединений)	Нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, затем нажмите [ENTER] для включения функции транзита PPPoE-соединений. В дополнение к встроенному в интернет-центр PPPoE клиенту, вы можете включить функцию транзита PPPoE-соединений, чтобы разрешить до 10 узлам локальной сети использовать у себя программное обеспечение PPPoE клиента для подключения к Интернет-провайдеру через интернет-центр. 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. Нажмите [ПРОБЕЛ] для выбора **No (Нет)** и затем нажмите [ENTER] для отключения функции транзита PPPoE-соединений, если вы не хотите разрешать узлам в локальной сети использовать программное обеспечение клиента PPPoE для подключения к Интернет-провайдеру.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Глава 25
Настройка статических маршрутов

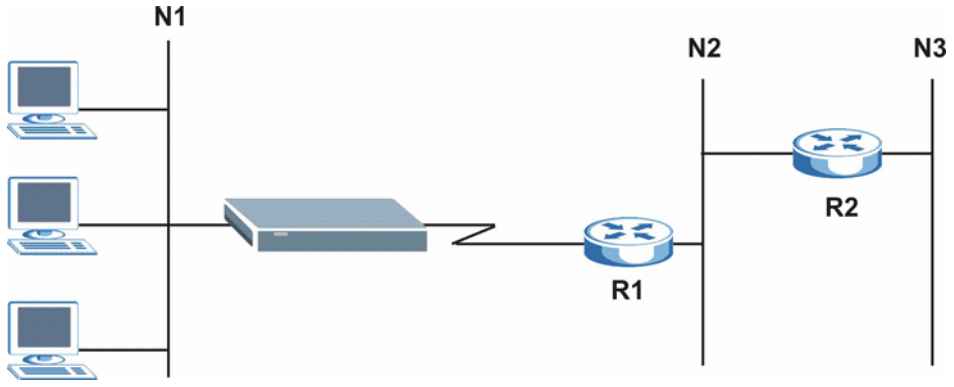
В этой главе описывается создание статических маршрутов IP.

25.1 Статические маршруты IP — общая информация

Статические маршруты дают интернет-центру информацию о маршрутизации, которую устройство не может получить автоматически другими средствами. Такая ситуация может возникать, если в локальной сети отключен RIP, или если удаленная сеть находится за другой сетью, напрямую подключенной к удаленному узлу.

Каждый удаленный узел определяет только ту сеть, к которой непосредственно подключен шлюз, при этом интернет-центр не имеет информации о других сетях. Например, интернет-центр имеет информацию о сети N2 (на следующем рисунке) через маршрутизатор удаленного узла 1. Однако интернет-центр не может послать пакет в сеть N3, так как он "не знает", что существует маршрут через маршрутизатор удаленного узла 1 (и далее через маршрутизатор 2). Статические маршруты дают интернет-центру информацию о сетях, находящихся за удаленными узлами.

Рис. 135 Пример топологии статической маршрутизации



25.2 Настройка

Для создания статического маршрута IP используется **Меню 12 — Настройка статического маршрута** (показано ниже).

Рис. 136 Меню 12 - Настройка статического маршрута

```
                    Menu 12 - Static Route Setup

               1. IP Static Route

               3. Bridge Static Route

                       Please enter selection:
```

В Меню 12, выберите 1 для перехода в **Меню 12.1 — Настройка статического маршрута IP** (показано ниже).

Рис. 137 Меню 12.1 — Настройка статического маршрута IP

```
                     Menu 12.1 - IP Static Route Setup
                  1. ________
                  2. ________
                  3. ________
                  4. ________
                  5. ________
                  6. ________
                  7. ________
                  8. ________
                  9. ________
                  10. ________
                  11. ________
                  12. ________
                  13. ________
                  14. ________
                  15. ________
                  16. ________

               Enter selection number:
```

Введите номер статического маршрута, который требуется создать.

Рис. 138 Меню 12.1.1 — Редактирование статического маршрута IP

```
          Menu 12.1.1 - Edit IP Static Route
                      Route #: 1
                      Route Name= ?
                      Active= No
                      Destination IP Address= ?
                      IP Subnet Mask= ?
                      Gateway IP Address= ?
                      Metric= 2
                      Private= No

           Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля **Меню 12.1.1 — Редактирование статического маршрута IP**.

Табл. 87 Меню 12.1.1 — Редактирование статического маршрута IP

ПОЛЕ	ОПИСАНИЕ
Route # (Номер маршрута)	Это порядковый номер статического маршрута, выбранный в Меню 12.1.
Route Name (Имя маршрута)	Введите описательное имя данного маршрута. Эта информация используется только в целях идентификации.
Active (Активировать)	Это поле служит для включения/отключения данного статического маршрута.
Destination IP Address (IP-адрес получателя)	Данный параметр определяет адрес IP-сети конечного получателя. Маршрутизация всегда выполняется на основе номера сети. Если нужно определить маршрут к одиночному узлу, в поле маски подсети используйте маску подсети 255.255.255.255, чтобы номер сети и адрес узла были одинаковыми.
IP Subnet Mask (Маска IP подсети)	Введите маску подсети для получателя.
Gateway IP Address (IP-адрес шлюза)	Введите IP-адрес шлюза. Шлюз — это маршрутизатор или коммутатор, находящийся в том же сегменте сети, что и порт LAN или WAN устройства. Шлюз помогает пересылать пакеты их адресатам.
Metric (Метрика)	Метрика определяет "стоимость" передачи и используется для целей маршрутизации. При маршрутизации IP в качестве единицы "стоимости" используется счетчик переходов по сети, при этом минимальное значение "стоимости" равно 1 и соответствует прямому соединению между сетями. Введите число, которое будет приблизительно выражать "стоимость" трафика для данного канала. Число не обязательно должно быть точным, но должно находиться в диапазоне от 1 до 15. В большинстве случаев хорошо подходит значение 2 или 3.
Private (Частный адрес)	Этот параметр определяет, будет ли интернет-центр включать маршрут к этому удаленному узлу в широковещательную рассылку RIP. Если установлено **Yes (Да)**, данный маршрут считается частным и не включается в широковещательную рассылку RIP. Если установлено **No (Нет)**, маршрут к этому удаленному узлу является доступным для других узлов через широковещательную рассылку RIP.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Глава 26
Настройка моста

В данной главе рассматривается настройка параметров моста.

26.1 Общие сведения о мосте

При использовании моста решение о передаче пакетов принимается на основе MAC-адреса (Media Access Control — Управление доступом к среде) или аппаратного адреса, в то время как при маршрутизации — на основе адреса сетевого уровня (IP). Организация моста позволяет интернет-центру передавать пакеты протоколов сетевого уровня, которые интернет-центр не маршрутизирует, например, SNA, из одной сети в другую. Недостатком моста является то, что по сравнению с маршрутизацией, передача по мосту генерирует значительно больший объем трафика для того же самого сетевого протокола и потребляет больше памяти и циклов процессора устройства.

В целях повышения производительности *не* следует включать мост, пока не возникает необходимость в поддержке в вашей сети протоколов, отличных от IP. Для протокола IP включите маршрутизацию, если необходимо; не используйте мост в тех случаях, когда интернет-центр может выполнять маршрутизацию.

26.2 Настройка Ethernet для организации моста

В основном, все нелокальные пакеты передаются по мосту в глобальную сеть. Интернет-центр не поддерживает протокол IPX (Internetwork Packet eXchange — Межсетевой обмен пакетами).

26.2.1 Настройка моста для удаленного узла

Для настройки протокольно-независимых параметров в **Меню 11.1 — Профиль удаленного узла** необходимо выполнить процедуру, описанную в соответствующем разделе. Параметры моста настраиваются в **Меню 11.3 — Параметры сетевого уровня удаленного узла**.

1. Для настройки **Меню 11.3 — Параметры сетевого уровня удаленного узла**, показанного на следующем рисунке, необходимо выполнить следующие действия:
2. В Меню 11.1 убедитесь, что в поле **Bridge (Мост)** установлено **Yes (Да)**.

Рис. 139 Меню 11.1 — Профиль удаленного узла

```
                Menu 11.1 - Remote Node Profile
  Rem Node Name= ?                      Route= IP
  Active= Yes                           Bridge= Yes
  Encapsulation= ENET ENCAP             Edit IP/Bridge= No
  Multiplexing= VC-based                Edit ATM Options= No
  Service Name= N/A                     Edit Advance Options= N/A
  Incoming:                             Telco Option:
    Rem Login= N/A                        Allocated Budget(min)= N/A
    Rem Password= N/A                     Period(hr)= N/A
  Outgoing:                               Schedule Sets= N/A
    My Login= N/A                         Nailed-Up Connection= N/A
    My Password= N/A                    Session Options:
    Authen= N/A                           Edit Filter Sets= No
                                          Idle Timeout(sec)= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

3 Переместите курсор в поле **Edit IP/Bridge (Редактировать IP/мост)** и нажмите клавишу [ПРОБЕЛ], чтобы установить значение **Yes (Да)**, а затем клавишу [ENTER] для перехода в **Меню 11.3 — Параметры сетевого уровня удаленного узла**.

Рис. 140 Меню 11.3 — Параметры сетевого уровня удаленного узла

```
            Menu 11.3 - Remote Node Network Layer Options
 IP Options:                          Bridge Options:
   IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
   Rem IP Addr: 0.0.0.0
   Rem Subnet Mask= 0.0.0.0
   My WAN Addr= 0.0.0.0
   NAT= Full Feature
     Address Mapping Set=2
   Metric= 2
   Private= No
   RIP Direction= Both
     Version= RIP-2B
   Multicast= IGMP-v2
   IP Policies=

            Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 88 Параметры сетевого уровня удаленного узла: Поля для настройки моста

ПОЛЕ	ОПИСАНИЕ
Bridge (Мост) (Меню 11.1)	Убедитесь, что в данном поле установлено значение **Yes (Да)**.

Табл. 88 Параметры сетевого уровня удаленного узла: Поля для настройки моста

ПОЛЕ	ОПИСАНИЕ
Edit IP/Bridge (Редактировать IP/мост) (Меню 11.1)	Нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, а затем нажмите клавишу [ENTER] для отображения меню 11.3.
Ethernet Addr Timeout (Время хранения адреса Ethernet) (мин.) (Меню 11.3)	Введите интервал времени (в минутах), в течение которого интернет-центр сохраняет информацию об адресе Ethernet в своих внутренних таблицах, пока соединение не работает. Если данная информация сохраняется, то интернет-центру не нужно заново компилировать таблицы при восстановлении соединения.

26.2.2 Настройка статического маршрута для моста

Аналогично статическим маршрутам сетевого уровня, статический маршрут для моста дает интернет-центру информацию о маршруте до узла, прежде чем устанавливается соединение. Статические маршруты для моста настраиваются в Меню 12.3.1, которое показано ниже (перейдите в Меню 12, выберите пункт 3, затем выберите статический маршрут для редактирования).

Рис. 141 Меню 12.3.1 — Редактировать статический маршрут для моста

```
Menu 12.3.1 - Edit Bridge Static Route
Route #: 1
Route Name=
Active= No
Ether Address= ?
IP Address=
Gateway Node= 1

Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описывается Меню **Редактировать статический маршрут для моста**.

Табл. 89 Меню 12.3.1 — Редактировать статический маршрут для моста

ПОЛЕ	ОПИСАНИЕ
Route # (Номер маршрута)	Это порядковый номер маршрута из списка в **Меню 12.3 — Настройка статического маршрута для моста**.
Route Name (Имя маршрута)	Введите имя статического маршрута для моста в целях идентификации.
Active (Активировать)	Это поле показывает включен (**Yes (Да)**) или отключен (**No (Нет)**) данный статический маршрут.
Ether Address (Ethernet адрес)	Введите MAC-адрес компьютера получателя, на который должны пересылаться пакеты по мосту.
IP Address (IP-адрес)	Если применяется, введите IP-адрес компьютера получателя, на который должны пересылаться пакеты по мосту.

Табл. 89 Меню 12.3.1 — Редактировать статический маршрут для моста (продолжение)

ПОЛЕ	ОПИСАНИЕ
Gateway Node (Шлюзовой узел)	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER] для выбора номера удаленного узла (от одного до восьми), который является шлюзом для данного статического маршрута.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Глава 27
Трансляция сетевых адресов (NAT)

В данной главе описывается настройка функции NAT в интернет-центре.

27.1 Применение NAT

Необходимо создать правило межсетевого экрана в дополнение к созданию SUA/NAT для того, чтобы трафик из глобальной сети пересылался через интернет-центр.

27.1.1 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)**. См. Разд. 27.3 на с. 292 или подробное описание функций NAT для реализации SUA. Интернет-центр также поддерживает режим NAT **Full Feature (Полный набор функциональных возможностей)** для отображения нескольких глобальных IP-адресов на несколько частных IP-адресов клиентов или серверов в локальной сети с использованием различных типов отображения.

- Выберите **SUA Only (Только SUA)**, если интернет-центр имеет только один общедоступный IP-адрес в глобальной сети.
- Выберите **Full Feature (Полный набор функциональных возможностей)**, если интернет-центр имеет несколько общедоступных IP-адресов в глобальной сети.

27.2 Применение NAT

Для применения NAT используется Меню 4 или Меню 11.3, как показано ниже. На следующем рисунке показано применение NAT в Меню 4 для доступа в Интернет. В главном меню введите 4 для перехода в **Меню 4 — Настройка доступа в Интернет**.

Рис. 142 Меню 4 — Применение NAT для доступа в Интернет

```
             Menu 4 - Internet Access Setup
                         ISP's Name= MyISP
                         Encapsulation= RFC 1483
                         Multiplexing= LLC-based
                         VPI #= 8
                         VCI #= 35
                         ATM QoS Type= UBR
                           Peak Cell Rate (PCR)= 0
                           Sustain Cell Rate (SCR)= 0
                           Maximum Burst Size (MBS)= 0
                         My Login= N/A
                         My Password= N/A
                         ENET ENCAP Gateway= N/A
                         IP Address Assignment= Static
                           IP Address= 0.0.0.0
                         Network Address Translation= SUA Only
                           Address Mapping Set= N/A

             Press ENTER to Confirm or ESC to Cancel:
```

На следующем рисунке показано применение NAT для удаленного узла в Меню 11.1.

1. В главном меню введите "11".
2. В Меню 11 введите номер удаленного узла, параметры которого необходимо настроить, как показано на следующем рисунке.
3. Переместите курсор в поле **Edit IP/Bridge (Редактировать IP/мост)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**, а затем нажмите [ENTER] для перехода в **Меню 11.3 — Параметры сетевого уровня удаленного узла**.

Рис. 143 Применение NAT в Меню 4 и Меню 11.3

```
             Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment = Static       Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= None
  IP Policies=

             Enter here to CONFIRM or ESC to CANCEL:
```

В следующей таблице представлено описание режимов трансляции сетевых адресов.

Табл. 90 Применение NAT в Меню 4 и Меню 11.3

ПОЛЕ	ОПИСАНИЕ
NAT	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER], чтобы выбрать **Full Feature (Полный набор функциональных возможностей)**, если интернет-центр имеет несколько общедоступных IP-адресов в глобальной сети. В SMT используется набор отображения адресов, который вы настроили в поле **Address Mapping Set (Набор отображения адресов)** (см. Рис. 145 на с. 293).
	Выберите **None (Нет)** для отключения функции NAT.
	Если выбрано значение **SUA Only (Только SUA)**, в SMT используется набор отображения адресов 255 (см. Рис. 146 на с. 293). Выберите **SUA Only (Только SUA)**, если интернет-центр имеет только один общедоступный IP-адрес в глобальной сети.

27.3 Настройка NAT

Меню и подменю наборов отображения адресов предназначены для создания таблицы отображения, которая используется для назначения глобальных адресов компьютерам в локальной сети. **Set 255 (Набор 255)** используется для SUA. Если в Меню 4 или Меню 11.3 выбрано **Full Feature (Полный набор функциональных возможностей)**, в SMT используется **Set 1 (Набор 1)**. Если выбрано **SUA Only (Только SUA)**, в SMT используется стандартный **Набор 255** (только для чтения).

Server Set (Набор серверов) — это список серверов в локальной сети, которые отображаются на внешние порты. Для использования этого набора, необходимо установить правила отображения серверов в наборе отображения адресов NAT. Более подробная информация об этих меню приведена в главе "Трансляция сетевых адресов web-конфигуратора". Для настройки NAT в главном меню введите 15 для перехода к следующему экрану.

Рис. 144 Меню 15 — Настройка NAT

```
Menu 15 - NAT Setup

      1. Address Mapping Sets

      2. NAT Server Sets

Enter Menu Selection Number:
```

27.3.1 Наборы отображения адресов

Введите 1 для вывода **Меню 15.1 — Наборы отображения адресов**.

Рис. 145 Меню 15.1 — Наборы отображения адресов

```
             Menu 15.1 - Address Mapping Sets
                      1.
                      2.
                      3.
                      4.
                      5.
                      6.
                      7.
                      8.
                    255. SUA (read only)

             Enter Menu Selection Number:
```

27.3.1.1 Набор отображения адресов SUA

Введите 255 для отображения следующего меню (см. также Разд. 27.1.1 на с. 290). Поля данного меню не доступны для изменения.

Рис. 146 Меню 15.1.255 — Правила отображения адресов SUA

```
             Menu 15.1.255 - Address Mapping Rules
 Set Name=
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP  Type
---  ---------------  ---------------  ---------------  -------------  ----
 1.  0.0.0.0          255.255.255.255  0.0.0.0                          M-1
 2.                                    0.0.0.0                        Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

               Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Меню 15.1.255 отображается в режиме только для чтения.

Табл. 91 Правила отображения адресов SUA

ПОЛЕ	ОПИСАНИЕ
Set Name (Имя набора)	Здесь отображается имя набора, выбранного в Меню 15.1, или можно ввести имя нового набора, который вы хотите создать.
Idx (Индекс)	Порядковый номер правила.

Табл. 91 Правила отображения адресов SUA (продолжение)

ПОЛЕ	ОПИСАНИЕ
Local Start IP (Начальный локальный IP-адрес)	**Local Start IP** — это начальный локальный IP-адрес (начальный ILA).
Local End IP (Конечный локальный IP-адрес)	**Local End IP** — это конечный локальный IP-адрес (конечный ILA). Если правило предназначено для всех локальных IP-адресов, то начальный адрес равен 0.0.0.0, а конечный адрес равен 255.255.255.255.
Global Start IP (Начальный глобальный IP-адрес)	Это начальный глобальный IP-адрес (начальный IGA). Если вы используете динамический IP-адрес, введите 0.0.0.0 в качестве **начального глобального IP-адреса**.
Global End IP (Конечный глобальный IP-адрес)	Это конечный глобальный IP-адрес (конечный IGA).
Type (Тип)	Здесь показывается тип отображения адресов. Тип Server (Сервер) позволяет определить несколько серверов для различных служб, расположенных за NAT по отношению к модему. См. далее несколько примеров.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

27.3.1.2 Пользовательские наборы отображения адресов

В Меню 15.1 введите 1 для отображения представленного ниже меню. Рассмотрим только отличие этого меню от предыдущего. Здесь присутствуют дополнительные поля **Action (Действие)** и **Select Rule (Выбор правила)**, что означает, что в данном меню можно настраивать правила. Знак [?] в поле **Set Name (Имя набора)** означает, что это обязательное поле и необходимо ввести имя для данного набора.

Рис. 147 Меню 15.1.1 — Первый набор

```
             Menu 15.1.1 - Address Mapping Rules
 Set Name= NAT_SET
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP   Type
---  ---------------  ---------------  ---------------  --------=-----  ---
 1.
 2
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

             Action= Edit          Select Rule=

             Press ENTER to Confirm or ESC to Cancel:
```

Если поле **Set Name (Имя набора)** оставлено пустым, весь набор будет удален.

Тип отображения, а также локальный или глобальный начальный/конечный IP- адреса устанавливаются в Меню 15.1.1.1 (описывается далее), здесь только отображаются значения соответствующих полей.

27.3.1.3 Порядок применения правил

Порядок следования правил имеет большое значение, поскольку интернет-центр применяет правила в указанном порядке. Когда текущий пакет соответствует какому-либо правилу, интернет-центр 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, вы уже настроили правила с 1-го по 6-е в текущем наборе и теперь хотите настроить правило 9. В общем окне набора правил новое правило будет иметь номер 7, но не 9.

Теперь, если удалить правило 4, правила с 5-го по 7-е переместятся вверх на одну позицию, т.о. старое правило 5 станет правилом 4, старое правило 6 станет правилом 5 и старое правило 7 станет правилом 6.

Табл. 92 Меню 15.1.1 — Первый набор

ПОЛЕ	ОПИСАНИЕ
Set Name (Имя набора)	Введите имя для данного набора правил. Это обязательное поле. Если это поле оставлено пустым, весь набор будет удален.
Action (Действие)	По умолчанию установлено **Edit (Редактировать)**. **Edit (Редактировать)** означает, что вы хотите редактировать выбранное правило (см. следующее поле). **Insert Before (Вставить перед)** означает вставку нового правила перед выбранным правилом. Правила после выбранного переместятся вниз на одну позицию. **Delete (Удалить)** означает удаление выбранного правила, после чего все остальные правила после удаленного переместятся вверх на одну позицию. Значение **None (Нет)** отключает поле **Select Rule (Выбор правила)**.
Select Rule (Выбор правила)	При выборе значения **Edit (Редактировать)**, **Insert Before (Вставить перед)** или **Delete (Удалить)** в предыдущем поле курсор автоматически перемещается в данное поле для выбора правила, к которому применяется действие.

Для сохранения всего набора нажмите клавишу **[ENTER]** в нижней части экрана. Необходимо повторить это действие, если после сохранения в данный набор правил вносятся изменения, включая удаление правила. Изменения не вступят в силу, пока не выполнено сохранение набора.

После установки значения **Edit (Редактировать)** в поле **Action (Действие)** и выбора правила открывается **Меню 15.1.1.1 — Правило отображения адресов**, в котором можно редактировать конкретное правило и настраивать поля **Type (Тип)** и **Local** и **Global Start/End IPs (Локальный** и **глобальный начальный/конечный IP-адреса)**.

Конечный IP-адрес должен быть численно больше соответствующего начального IP-адреса.

Рис. 148 Меню 15.1.1.1 — Редактирование/создание конкретного правила в наборе

```
Menu 15.1.1.1 Address Mapping Rule
     Type= One-to-One
     Local IP:
       Start=
       End  = N/A
     Global IP:
       Start=
       End  = N/A
     Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 93 Меню 15.1.1.1 — Редактирование/создание конкретного правила в наборе

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора типа отображения из пяти вариантов. Типы отображения рассматриваются в главе "Трансляция сетевых адресов (NAT)".Тип Server (Сервер) позволяет определить несколько серверов для различных служб, находящихся за NAT по отношению к модему.
Local IP (Локальные IP-адреса)	Для типа отображения "сервер" (Server) только поля локальных IP-адресов являются недоступными (**N/A**); в полях глобальных IP-адресов должен быть задан "**Server**".
Start (Начальный)	Это начальный локальный IP-адрес (начальный ILA).
End (Конечный)	Это конечный локальный IP-адрес (конечный ILA). Если правило предназначено для всех локальных IP-адресов, введите начальный адрес 0.0.0.0, а конечный — 255.255.255.255. Это поле является недоступным (**N/A**) для типов отображения **один-к-одному** и **сервер**.
Global IP (Глобальные IP-адреса):	
Start (Начальный)	Это начальный внутренний глобальный IP-адрес (IGA). Если вы используете динамический IP-адрес, введите 0.0.0.0 в качестве **начального глобального IP-адреса**. Следует отметить, что поле **Начальный глобальный IP-адрес** может иметь значение 0.0.0.0, только если используется тип отображения **много-к-одному** или **сервер**.
End (Конечный)	Это конечный внутренний глобальный IP-адрес (IGA). Это поле является недоступным (**N/A**) для типов отображения **один-к-одному**, **много-к-одному** и **сервер**.
Server Mapping Set (Набор отображения серверов)	Это поле доступно, только если в поле **Type (Тип)** установлено значение **Server (Сервер)**.Введите число от 1 до 10, чтобы выбрать набор серверов, установленный в Меню 15.2.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

27.4 Настройка сервера, расположенного за NAT

Для настройки сервера, расположенного за NAT выполните следующие действия:

1. В главном меню введите 15 для перехода в **Меню 15 — Настройка NAT**.
2. Введите 2 для перехода в **Меню 15.2 — Наборы серверов за NAT**, которое показано ниже.

Рис. 149 Меню 15.2 — Настройка серверов за NAT

```
            Menu 15.2 - NAT Server Sets
                   1. Server Set 1 (Used for SUA Only)
                   2. Server Set 2
                   3. Server Set 3
                   4. Server Set 4
                   5. Server Set 5
                   6. Server Set 6
                   7. Server Set 7
                   8. Server Set 8
                   9. Server Set 9
                  10. Server Set 10

                    Enter Set Number to Edit:
```

3 Введите 1 для перехода в **Меню 15.2.1 — Настройка серверов за NAT**, которое показано ниже.

Рис. 150 Меню 15.2.1 — Настройка серверов за NAT

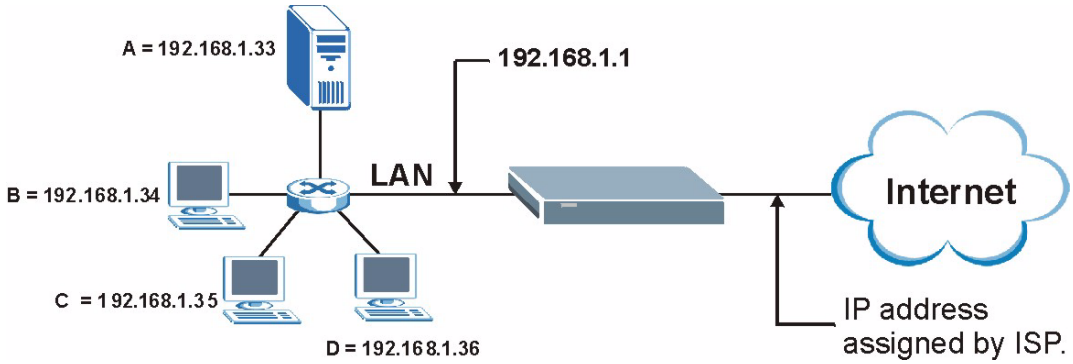
```
            Menu 15.2 - NAT Server Setup
     Rule   Start Port No.   End Port No.   IP Address
    ------------------------------------------------
       1.    Default          Default        0.0.0.0
       2.      21               21           192.168.1.33
       3.      0                0            0.0.0.0
       4.      0                0            0.0.0.0
       5.      0                0            0.0.0.0
       6.      0                0            0.0.0.0
       7.      0                0            0.0.0.0
       8.      0                0            0.0.0.0
       9.      0                0            0.0.0.0
      10.      0                0            0.0.0.0
      11.      0                0            0.0.0.0
      12.      0                0            0.0.0.0

            Press ENTER to Confirm or ESC to Cancel:
```

4 Введите номер порта в свободное поле **Start Port No (Начальный номер порта)**. Для переадресации только одного порта, введите его номер еще раз в поле **End Port No (Конечный номер порта)**. Чтобы установить диапазон портов, введите номер конечного порта для переадресации в поле **End Port No (Конечный номер порта)**.

5 Введите внутренний IP-адрес сервера в поле **IP Address (IP-адрес)**. На следующем рисунке показан компьютер, функционирующий как сервер FTP, Telnet и SMTP (порты 21, 23 и 25) с адресом 192.168.1.33.

6 После определения всех серверов нажмите [ENTER] в строке "`Press ENTER to confirm ...`" для сохранения конфигурации или нажмите [ESC] для отмены внесенных изменений в любое время.

Рис. 151 Пример: Несколько серверов расположены за NAT



27.5 Примеры применения NAT

Далее приводятся несколько примеров конфигурации NAT.

27.5.1 Пример 1: только доступ в Интернет

В следующем примере для доступа в Интернет требуется только одно правило, по которому все внутренние локальные адреса (ILA) отображаются на один динамический внутренний глобальный адрес (IGA), назначаемый Интернет-провайдером.

Рис. 152 Пример применения NAT 1

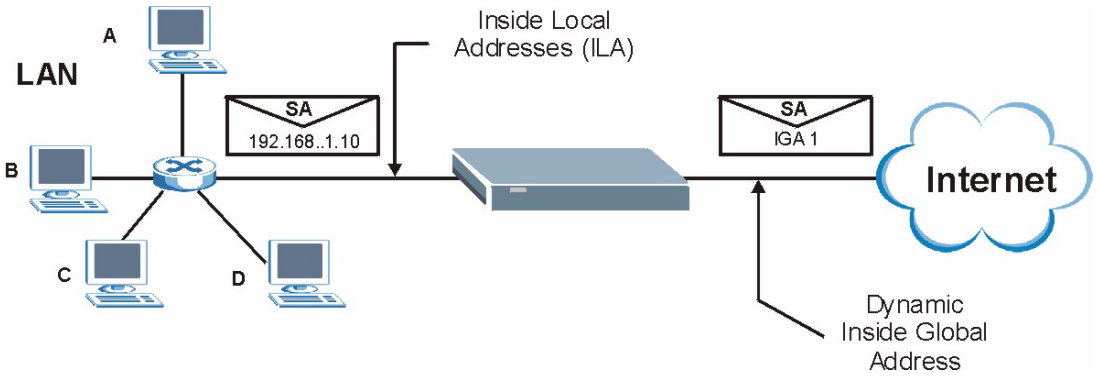


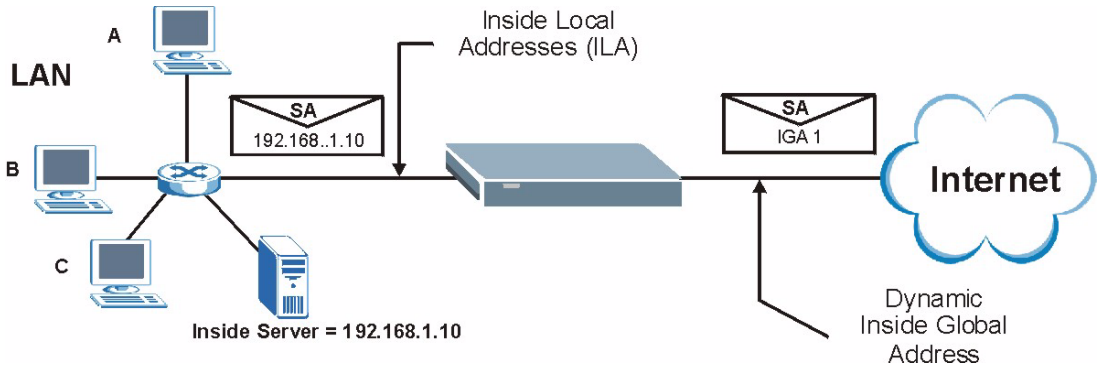
Рис. 153 Меню 4 — Пример доступа в Интернет при использовании NAT

```
                Menu 4 - Internet Access Setup
ISP's Name= MyISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

В Меню 4 в поле **Network Address Translation (Трансляция сетевых адресов)** выберите режим **SUA Only (Только SUA)**. Это тип отображения **Много-к-одному**, рассматриваемый в разделе Разд. 27.5 на с. 299. Доступная только для чтения опция **SUA Only (Только SUA)** в поле **Network Address Translation (Трансляция сетевых адресов)** в Меню 4 и 11.3 специально предустановлена для работы в таком режиме.

27.5.2 Пример 2: доступ в Интернет с внутренним сервером

Рис. 154 Пример применения NAT 2



В данном случае настройка выполняется аналогично описанной выше (используется предустановленная функция **SUA Only (Только SUA)**), далее необходимо перейти в меню 15.2, чтобы определить внутренний сервер, расположенный за NAT, как показано на следующем рисунке.

Рис. 155 Меню 15.2.1 — Определение внутреннего сервера

```
          Menu 15.2.1 - NAT Server Setup (Used for SUA Only)
 Rule    Start Port No.    End Port No.    IP Address
-------------------------------------------------------
   1.     Default           Default         192.168.1.10
   2.       0                 0             0.0.0.0
   3.       0                 0             0.0.0.0
   4.       0                 0             0.0.0.0
   5.       0                 0             0.0.0.0
   6.       0                 0             0.0.0.0
   7.       0                 0             0.0.0.0
   8.       0                 0             0.0.0.0
   9.       0                 0             0.0.0.0
  10.       0                 0             0.0.0.0
  11.       0                 0             0.0.0.0
  12.       0                 0             0.0.0.0

          Press ENTER to Confirm or ESC to Cancel:
```

27.5.3 Пример 3: несколько общедоступных IP-адресов для внутренних серверов

В данном примере существует три адреса IGA, предоставленных Интернет-провайдером. Имеется несколько отделов, и два из них имеют собственные серверы FTP. Все отделы используют один маршрутизатор. В примере каждому отделу с сервером FTP предоставляется по одному IGA, и все отделы используют оставшийся IGA. Адреса серверов FTP отображаются на два первых IGA, а остальной трафик локальной сети отображается на третий IGA. Третий IGA назначается внутреннему web-серверу и почтовому серверу. Для реализации такой конфигурации необходимо создать 4 правила: два для трафика в двух направлениях и два для однонаправленного трафика.

Первый IGA отображается на первый внутренний сервер FTP для трафика FTP в обоих направлениях (отображение **1: 1**, назначается локальный и глобальный IP-адрес).

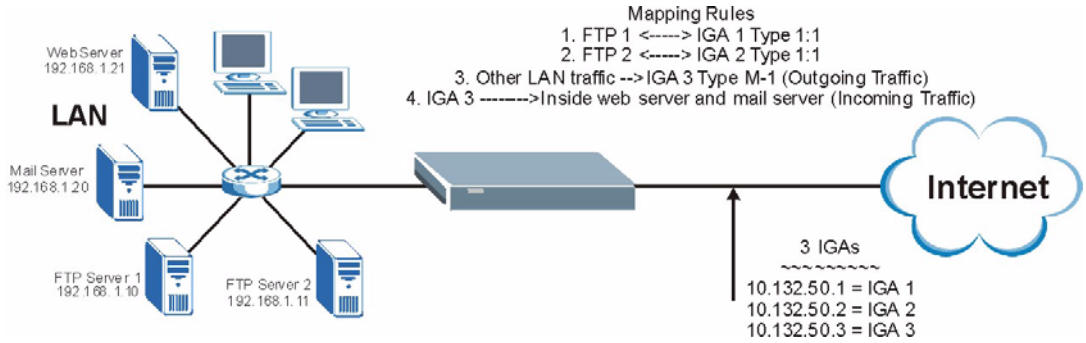
Второй IGA отображается на второй внутренний сервер FTP для трафика FTP в обоих направлениях (отображение **1: 1**, назначается локальный и глобальный IP-адрес).

Третий IGA отображается на другой исходящий трафик локальной сети (отображение **Много: 1**).

Также третий IGA отображается на web-сервер и почтовый сервер локальной сети. Тип отображения **Server (Сервер)** позволяет определить несколько серверов для различных служб для других компьютеров, расположенных за NAT в локальной сети.

Приведенный пример представлен на следующем рисунке:

Рис. 156 Пример применения NAT 3



В данном случае необходимо создать Набор отображения адресов 1 с помощью **Меню 15.1 — Наборы отображения адресов**.Следовательно, необходимо в поле **Network Address Translation (Трансляция сетевых адресов)** (в Меню 4 или 11.3) выбрать значение **Full Feature (Полный набор функциональных возможностей)** Рис. 157 на с. 303.

1. В главном меню введите 15 .
2. Введите 1 для настройки наборов отображения адресов.
3. Введите 1 для настройки нового набора. Введите имя набора, выберите **Edit (Редактировать)** в поле **Action (Действие)** и затем введите 1 в поле **Select Rule (Выбор правила)**. Нажмите клавишу [ENTER] для подтверждения.
4. Выберите в поле **Type (Тип)** режим **One-to-One (Один-к-одному)** (прямое отображение для пакетов, передаваемых в обоих направлениях), и введите локальный **начальный IP-адрес** как 192.168.1.10 (IP-адрес сервера FTP 1), глобальный **начальный IP-адрес** как 10.132.50.1 (первый IGA). (См. Рис. 158 на с. 303).
5. Повторите предыдущие действия для создания правил со 2-го по 4-е, как описано выше.

После завершения настройки Меню 15.1.1 должно выглядеть, как на Рис. 159 на с. 304.

Рис. 157 Пример 3: Меню 11.3

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

            Press ENTER to Confirm or ESC to Cancel:
```

На следующем рисунке показано, как настроить первое правило.

Рис. 158 Пример 3: Меню 15.1.1.1

```
             Menu 15.1.1.1 Address Mapping Rule
                  Type= One-to-One
                  Local IP:
                    Start= 192.168.1.10
                    End  = N/A
                  Global IP:
                    Start= 10.132.50.1
                    End  = N/A
                  Server Mapping Set= N/A

              Press ENTER to Confirm or ESC to Cancel:
```

Рис. 159 Пример 3: Окончательный вид Меню 15.1.1

```
            Menu 15.1.1 - Address Mapping Rules
Set Name= Example3
Idx  Local Start IP   Local End IP   Global Start IP  Global End IP    Type
---  ---------------  -------------  ---------------  --------------   ----
 1. 192.168.1.10                      10.132.50.1                       1-1
 2  192.168.1.11                      10.132.50.2                       1-1
 3. 0.0.0.0          255.255.255.255  10.132.50.3                       M-1
 4.                                  10.132.50.3                     Server
 5.
 6.
 7.
 8.
 9.
10.

            Action= Edit          Select Rule=

            Press ENTER to Confirm or ESC to Cancel:
```

Теперь необходимо настроить отображение третьего IGA на web-сервер и почтовый сервер в локальной сети.

1. В главном меню введите 15 .
2. Введите 2 в **Меню 15 — Настройка NAT**.
3. Введите 1 в **Меню 15.2 — Наборы серверов за NAT** для входа в следующее подменю. Настройте его, как показано ниже.

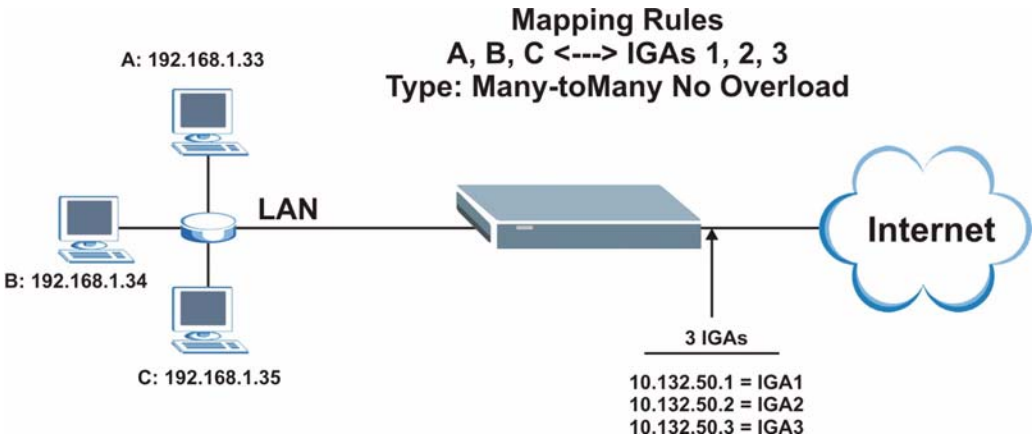
Рис. 160 Пример 3: Меню 15.2.1

```
              Menu 15.2.1 - NAT Server Setup
        Rule   Start Port No.   End Port No.   IP Address
        -------------------------------------------------
           1.    Default          Default        0.0.0.0
           2.      80               80           192.168.1.21
           3.      25               25           192.168.1.20
           4.      0                0            0.0.0.0
           5.      0                0            0.0.0.0
           6.      0                0            0.0.0.0
           7.      0                0            0.0.0.0
           8.      0                0            0.0.0.0
           9.      0                0            0.0.0.0
          10.      0                0            0.0.0.0
          11.      0                0            0.0.0.0
          12.      0                0            0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

27.5.4 Пример 4: прикладные программы, не поддерживающие NAT

Некоторые приложения не поддерживают отображение NAT с использованием преобразования адресов портов TCP или UDP. В таком случае необходимо использовать отображение **Много-ко-многим без перекрытия** , так как при типе отображения NAT **Много-ко-многим без перекрытия** (а также **Один-к-одному**) номера портов *не* изменяются. Применение фильтров показано на следующем рисунке.

Рис. 161 Пример применения NAT 4



Другие приложения, такие как некоторые игры, не поддерживают NAT, поскольку они вставляют информацию об адресации в поток данных. Такие приложения не будут работать через NAT, даже при использовании типов отображения **один-к-одному** и **много-ко-многим без перекрытия**.

Выполните действия, приведенные в примере 3, для настройки тех же двух меню, как показано ниже.

Рис. 162 Пример 4: Меню 15.1.1.1 — Правило отображения адресов

```
Menu 15.1.1.1 Address Mapping Rule
     Type= Many-to-Many No Overload
     Local IP:
       Start= 192.168.1.10
       End  = 192.168.1.12
     Global IP:
       Start= 10.132.50.1
       End  = 10.132.50.3
     Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

После того, как правило настроено, можно проверить настройки в меню 15.1.1, как показано ниже.

Рис. 163 Пример 4: Меню 15.1.1 — Правила отображения адресов

```
             Menu 15.1.1 - Address Mapping Rules
  Set Name= Example4
 Idx  Local Start IP   Local End IP   Global Start IP  Global End IP    Type
 ---  ---------------  ------------   ---------------  ---------------  ----
  1.  192.168.1.10     192.168.1.12   10.132.50.1      10.132.50.3      M:M
NO OV
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.
                   Action= Edit          Select Rule=

               Press ENTER to Confirm or ESC to Cancel:
```

Глава 28
Активация межсетевого экрана

В этой главе дана общая информация по включению межсетевого экрана в интернет-центре P–660HT/HTW EE.

28.1 Удаленное управление и межсетевой экран

Если в меню SMT 24.11 разрешено удаленное управление и включен межсетевой экран:

- Межсетевой экран блокирует удаленное управление из WAN, если не настроено правило межсетевого экрана, разрешающее такое управление.
- Межсетевой экран разрешает удаленное управление из LAN.

28.2 Способы настройки

Web-конфигуратор, несомненно, является наиболее полным средством настройки межсетевого экрана интернет-центра P–660HT/HTW EE. Поэтому рекомендуется настраивать межсетевой экран с помощью Web-конфигуратора (инструкции см. в следующих главах). Меню SMT позволяет активировать межсетевой экран и просматривать журналы.

28.3 Активация межсетевого экрана

В главном меню наберите "21" для перехода в **Меню 21 — Filter Set and Firewall Configuration (Набор фильтров и настройка межсетевого экрана)**. Появится экран, показанный далее.

Выберите опцию "2" в данном меню для вывода на экран следующего меню. Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] и выберите **Yes** в поле **Active**, чтобы активировать межсетевой экран. Межсетевой экран может применяться для защиты от атак типа "Отказ в обслуживании" (DoS). Дополнительные правила можно задать через Web-конфигуратор.

Рис. 164 Меню 21.2 — Firewall Setup (Настройка межсетевого экрана)

```
        Menu 21.2 - Firewall Setup
The firewall protects against Denial of Service (DOS) attacks when
it is active. The default Policy sets
    1. allow all sessions originating from the LAN to the WAN and
    2. deny all sessions originating from the WAN to the LAN
You may define additional Policy rules or modify existing ones but
please exercise extreme caution in doing so
    Active: Yes
    LAN-to-WAN Set Name: ACL Default Set
    WAN-to-LAN Set Name: ACL Default Set
Please configure the Firewall function through Web Configurator.

          Press ENTER to Confirm or ESC to Cancel:
```

Для настройки правил межсетевого экрана используйте Web-конфигуратор или интерпретатор команд.

Глава 29
Настройка фильтров

В этой главе описывается создание и применение фильтров.

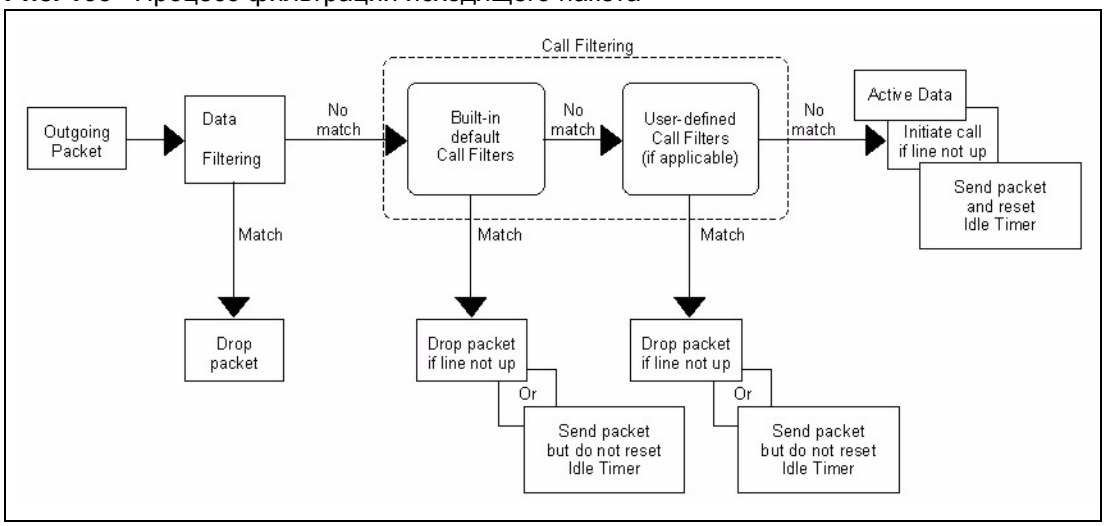
29.1 О фильтрации

Фильтры в интернет-центре используются для принятия решения о разрешении или запрещении пересылки пакета данных и/или выполнения вызова. Фильтры имеют два вида применения: фильтрация данных и фильтрация вызовов. Фильтры подразделяются на фильтры устройств и фильтры протоколов. Далее рассматриваются оба типа фильтров.

Фильтры данных проверяют данные с целью определить разрешение на пересылку пакета. Фильтры данных подразделяются на входящие фильтры и исходящие фильтры в зависимости от направления пакета по отношению к порту. Фильтрация данных может применяться как для порта глобальной сети, так и для порта Ethernet. Фильтрация вызовов используется для определения, разрешить ли пакету инициировать вызов.

Исходящие пакеты сначала подвергаются проверке фильтрами данных, а затем поступают на фильтры вызовов. Фильтры вызовов разделяются на две группы: встроенные фильтры вызовов и фильтры вызовов, определяемые пользователем. Интернет-центр имеет встроенные фильтры вызовов, которые предотвращают инициирование вызовов управляющими пакетами, например, пакетами RIP. Эти фильтры всегда включены и недоступны для пользователя. Интернет-центр сначала применяет встроенные фильтры, а затем — пользовательские фильтры вызовов (если есть), как показано на следующем рисунке.

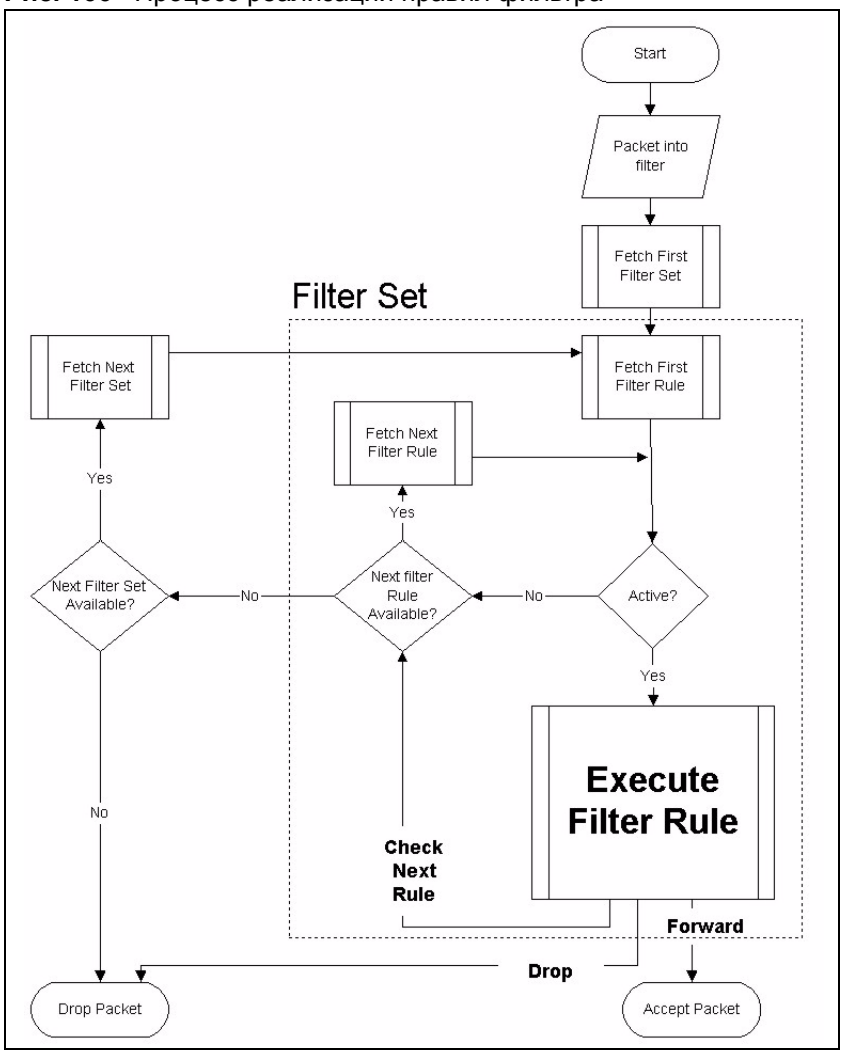
Рис. 165 Процесс фильтрации исходящего пакета



В меню 21 изготовителем по умолчанию установлено два набора правил фильтров для предотвращения инициирования вызовов трафиком NetBIOS. Список правил фильтров показан на рисунках далее.

Следующий рисунок иллюстрирует логическую схему реализации правила фильтра.

Рис. 166 Процесс реализации правил фильтра



К конкретному порту можно применить до четырех наборов фильтров для блокировки пакетов различных типов. Так как в одном наборе может содержаться до шести правил, всего можно установить 24 правила для фильтрации данных каждого конкретного порта.

Для входящих пакетов интернет-центр применяет только фильтры данных. Пакеты обрабатываются в зависимости от соответствия правилам фильтра. В следующих разделах описывается настройка наборов фильтров.

29.1.1 Структура фильтра

Фильтр состоит из одного или нескольких правил, образующих набор фильтра. Обычно связанные правила группируются, например, все правила для NetBIOS создаются в одном наборе, которому присваивается описательное имя. Можно настроить до двенадцати наборов фильтров с шестью правилами в каждом наборе, итого в системе может быть 72 правила фильтрации.

29.2 Настройка набора фильтров

Для настройки набора фильтров выполните следующие действия.

1. Откройте **Меню 21 — Filter and Firewall Setup (Настройка фильтров и межсетевого экрана)**. Для этого наберите цифру 21 в главном меню.
2. Введите 1 для перехода в **Меню 21.1 — Filter Set Configuration (Настройка наборов фильтров)**, которое показано ниже.

Рис. 167 Меню 21 — Filter Set Configuration (Настройка наборов фильтров)

```
            Menu 21.1 - Filter Set Configuration
Filter
 Set #        Comments                Set #        Comments
 ------  -----------------            ------  -----------------
   1      ________________              7      ________________
   2      ________________              8      ________________
   3      ________________              9      ________________
   4      ________________             10      ________________
   5      ________________             11      ________________
   6      ________________             12      ________________

            Enter Filter Set Number to Configure= 0

            Edit Comments= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

3. В поле "Enter filter set number to configure" введите номер набора фильтров, который необходимо настроить (от 1 до 12), и нажмите клавишу [ENTER].
4. Введите описательное имя или комментарий в поле **Edit Comments (Редактировать комментарий)** и нажмите клавишу [ENTER].
5. В поле "**Press [ENTER] to confirm…**" нажмите клавишу [ENTER] для перехода в **Меню 21.1.1 — Filter Rules Summary (Список правил фильтров)** (т. е., если выбран набор фильтров 1 в Меню 21.1).

Рис. 168 Список правил фильтра NetBIOS_WAN

```
              Menu 21.1.2 - Filter Rules Summary
 # A Type                      Filter Rules                            M m n
 - - ---- ------------------------------------------------------------- -
- -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                          N D N
 2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                          N D N
 3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                          N D N
 4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                         N D N
 5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                         N D N
 6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                         N D F

              Enter Filter Rule Number (1-6) to Configure:
```

Рис. 169 Список правил фильтра NetBIOS_LAN

```
             Menu 21.1.3 - Filter Rules Summary
 # A Type                       Filter Rules                           M m n
 - - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                  N D F
 2 N
 3 N
 4 N
 5 N
 6 N
             Enter Filter Rule Number (1-6) to Configure:
```

Рис. 170 Список правил фильтра IGMP

```
             Menu 21.1.4 - Filter Rules Summary
 # A Type                       Filter Rules                           M m n
 - - ---- ------------------------------------------------------------ - - -
 1 Y Gen Off=0, Len=3, Mask=ffffff, Value=01005e                       N D F
 2 N
 3 N
 4 N
 5 N
 6 N

             Enter Filter Rule Number (1-6) to Configure:
```

29.3 Меню "Список правил фильтра"

В следующей таблице приводится краткое описание сокращений, используемых в Меню 21.1.1 и 21.1.2.

Табл. 94 Сокращения, используемые в меню Filter Rules Summary (Список правил фильтра)

ПОЛЕ	ОПИСАНИЕ
#	Номер правила фильтра: от 1 до 6.
A	Active (Активно): “Y” означает, что данное правило фильтра включено. "N" означает, что данное правило фильтра выключено.
Type (Тип)	Тип правила фильтра. Вариантами являются:"GEN" (общего типа) или "IP" (TCP/IP).
Filter Rules (Правила фильтрации)	В этих полях отображаются параметры правила фильтра.

Табл. 94 Сокращения, используемые в меню Filter Rules Summary (Список правил фильтра) (продолжение)

ПОЛЕ	ОПИСАНИЕ
M	More (Дополнительно) "Y" означает, что есть еще правила, которые образуют цепочку правил с текущим правилом. Действие выполняется только после того, как проверена вся цепочка правил. "N" означает, что правил для проверки больше нет. Можно назначить действие, которое должно быть выполнено в результате проверки, например, переслать пакет, сбросить пакет или проверить по следующему правилу. Следующее правило не зависит от только что проверенного правила.
m	(Action Matched) Действие при соответствии. "F" означает немедленную пересылку пакета и пропуск проверки по оставшимся правилам. "D" означает сброс пакета. "N" означает проверку по следующему правилу.
n	Action Not Matched (Действие при несоответствии) "F" означает немедленную пересылку пакета и пропуск проверки по оставшимся правилам. "D" означает сброс пакета. "N" означает проверку по следующему правилу.

Сокращения для правил протокольно-зависимых фильтров представлены в следующей таблице:

Табл. 95 Сокращения, используемые в правилах

ТИП ФИЛЬТРА	ОПИСАНИЕ
IP (Фильтр TCP/IP)	
Pr	Протокол
SA	Source Address (Адрес источника)
SP	Source Port Number (Номер порта источника)
DA	Адрес получателя
DP	Destination Port Number (Номер порта получателя)
GEN (Фильтр общего типа)	
Off	Offset (Смещение)
Len	Length (Длина)

29.4 Настройка правила фильтра

Для настройки правила фильтра введите его номер в **Меню 21.1.x — Filter Rules Summary (Список правил фильтра)** и нажмите клавишу [ENTER] для перехода в Меню 21.1.x.1 для данного правила.

Существует два типа правил фильтров: **TCP/IP** и **Generic (Общий)**. Параметры правил могут отличаться в зависимости от типа. Нажмите клавишу [ПРОБЕЛ] для выбора типа правила, которое необходимо создать, в поле **Filter Type (Тип фильтра)**, затем нажмите клавишу [ENTER] для перехода в соответствующее меню.

Для увеличения скорости фильтрации, все правила в наборе фильтров должны быть одного и того же типа: например, или фильтр протоколов, или фильтр общего типа. Класс набора фильтров определяется по первому созданному правилу. При применении наборов фильтров к порту для наборов фильтров протоколов и наборов фильтров устройств предусмотрены разные поля. Если фильтр протоколов будет включен в набор фильтров устройств или наоборот, интернет-центр выдаст предупреждение и не разрешит сохранить конфигурацию.

29.4.1 Правило фильтра TCP/IP

В этом разделе описывается настройка правил фильтра TCP/IP. Фильтр TCP/IP позволяет создавать правила на основе полей в заголовках IP и протоколов верхнего уровня, например, UDP и TCP.

Для настройки правила TCP/IP, выберите в поле **Filter Type (Тип фильтра)** значение TCP/IP Filter Rule (Правило фильтра TCP/IP) и нажмите [ENTER] для перехода в **Меню 21.1.x.1 — TCP/IP Filter Rule (Правило фильтра TCP/IP)**, как показано ниже.

Рис. 171 Меню 21.1.x.1 — TCP/IP Filter Rule (Правило фильтра TCP/IP)

```
                    Menu 21.1.1.1 - TCP/IP Filter Rule

                Filter #: 1,1
                Filter Type= TCP/IP Filter Rule
                Active= No
                IP Protocol= 0     IP Source Route= No
                Destination: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                     Source: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                TCP Estab= N/A
                More= No           Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

                Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описывается создание правила фильтра TCP/IP.

Табл. 96 Меню 21.1.x.1 — Правило фильтра TCP/IP

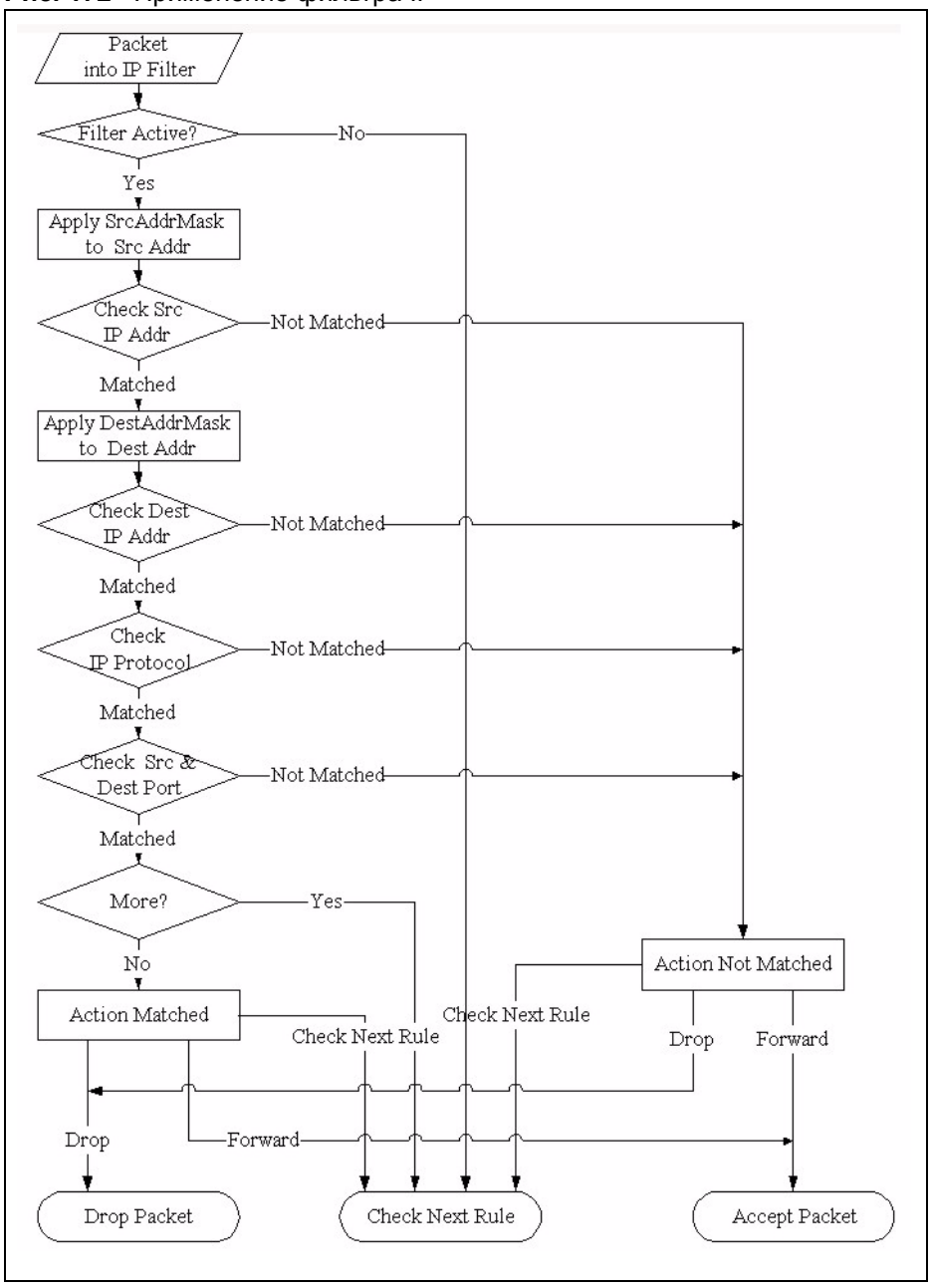
ПОЛЕ	ОПИСАНИЕ
Filter # (Номер фильтра)	Номер набора фильтров и номер правила фильтрации, введенные через запятую (например: 2, 3), означают второй набор фильтров и третье правило фильтра в этом наборе.
Filter Type (Тип фильтра)	Нажмите клавишу [ПРОБЕЛ] и затем клавишу [ENTER] для выбора типа правила. Параметры, отображаемые для каждого типа фильтра, могут различаться. Вариантами являются: **TCP/IP Filter Rule (Правило фильтра TCP/IP)** или **Generic Filter Rule (Правило фильтра общего типа)**.
Active (Активировать)	Выберите **Yes (Да)** для включения или **No (Нет)** для выключения данного правила фильтра.
IP Protocol (Протокол IP)	Это протокол верхнего уровня, например, TCP — 6, UDP — 17 и ICMP — 1. Значение должно быть в диапазоне от 0 до 255. Значение 0 соответствует ЛЮБОМУ протоколу.
IP Source Route (Маршрут источника IP)	Маршрут источника IP является дополнительным заголовком, определяющим маршрут, по которому IP-пакет направляется от источника к получателю. Если установлено **Yes**, правило применяется к любому пакету, имеющему маршрут источника IP. Большинство IP-пакетов не имеют маршрута источника.
Destination (Получатель):	
IP Addr (IP-адрес)	Введите IP-адрес получателя для пакетов, которые вы хотите фильтровать. Данное поле игнорируется, если его значение равно 0.0.0.0.
IP Mask (IP-маска)	Введите IP-маску для применения к полю **Destination: IP Addr. (IP-адрес получателя)**
Port # (Номер порта)	Введите номер порта получателя для фильтруемых пакетов. Значение поля должно находиться в диапазоне от 0 до 65535. Поле со значением 0 игнорируется.

Табл. 96 Меню 21.1.x.1 — Правило фильтра TCP/IP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Port # Comp (Сравнение номера порта)	Выберите критерий сравнения порта получателя в пакете со значением, установленным в поле **Destination: Port # (Получатель: Номер порта).** Вариантами являются: **None (Нет)**, **Less (Меньше)**, **Greater (Больше)**, **Equal (Равно)** или **Not Equal (Не равно)**.
Source (Источник):	
IP Addr (IP-адрес)	Введите IP-адрес источника для фильтруемых пакетов. Поле со значением 0.0.0.0 игнорируется.
IP Mask (IP-маска)	Введите IP-маску для применения к полю **Source: IP Addr. (IP-адрес источника)**.
Port # (Номер порта)	Введите номер порта источника для фильтруемых пакетов. Значение поля должно находиться в диапазоне от 0 до 65535. Поле со значением 0 игнорируется.
Port # Comp (Сравнение номера порта)	Выберите критерий сравнения порта источника в пакете со значением, установленным в поле **Source: Port #** (Номер порта источника). Вариантами являются: **None (Нет)**, **Less (Меньше)**, **Greater (Больше)**, **Equal (Равно)** или **Not Equal (Не равно)**.
TCP Estab (Установить соединение TCP)	Применяется только тогда, когда значение поля IP Protocol (Протокол IP) равно 6, т.е. TCP. Если установлено **Yes (Да)**, правило соответствует пакетам, которые предназначены для установления соединения TCP (SYN=1 и ACK=0); в противном случае правило игнорируется.
More (Дополнительно)	Если установлено значение **Yes (Да)**, соответствующий правилу пакет проверяется по следующему правилу фильтра, перед тем как будет выполнено заданное действие; в противном случае пакет обрабатывается в соответствии с полями, где назначены действия. Если в поле **More (Дополнительно)** установлено **Yes (Да)**, то поля **Action Matched (Действие при соответствии)** и **Action Not Matched (Действие при несоответствии)** являются недоступными (N/A).
Log (Регистрационный журнал)	Выберите режим регистрации пакетов из следующих вариантов: **None (Нет)** — пакеты не регистрируются в журнальном файле. **Action Matched (Действие при соответствии)** — регистрируются только пакеты, соответствующие параметрам правила. **Action Not Matched (Действие при несоответствии)** — регистрируются только пакеты, не соответствующие параметрам правила. **Both (Все)** — все пакеты регистрируются в журнальном файле.
Action Matched (Действие при соответствии)	Выберите действие для применения к пакету, для которого обнаружено соответствие правилу. Вариантами являются: **Check Next Rule (Проверить по следующему правилу)**, **Forward (Переслать)** или **Drop (Сбросить)**.
Action Not Matched (Действие при несоответствии)	Выберите действие для применения к пакету, для которого соответствие правилу не обнаружено. Вариантами являются: **Check Next Rule (Проверить по следующему правилу)**, **Forward (Переслать)** или **Drop (Сбросить)**.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

На следующем рисунке представлена логическая схема фильтра IP.

Рис. 172 Применение фильтра IP



29.4.2 Правило фильтра общего типа

В этом разделе описывается настройка правила фильтра общего типа. Общие фильтры служат для фильтрации не IP-пакетов. Для пакетов IP проще использовать правила IP.

При применении общих правил интернет-центр обрабатывает пакеты как поток байтов в противоположность пакетам IP. Вы определяете размер пакета для проверки с помощью полей **Offset (Смещение)** (от 0) и **Length (Длина)**, оба измеряются в байтах. Интернет-центр применяет маску (побитовое выполнение операции "И") к блоку данных перед сравнением результата со значением поля Value, по которому определяется

соответствие. Поля **Mask (Маска)** и **Value (Значение)** вводятся в шестнадцатиричном формате . Следует отметить, что для записи одного байта требуется две шестнадцатиричные цифры, поэтому если длина равна 4, значение каждого поля будет занимать восемь разрядов, например, FFFFFFFF.

Для настройки общего правила выберите свободный набор фильтров в Меню 21, например, "5". Выберите **Generic Filter Rule (Правило фильтра общего типа)** в поле **Filter Type (Тип фильтра)** и нажмите клавишу [ENTER] для перехода в **Меню 21.1.5.1 — Generic Filter Rule (Правило фильтра общего типа)**, как показано на следующем рисунке.

Рис. 173 Меню 21.1.5.1 — Generic Filter Rule (Правило фильтра общего типа)

```
Menu 21.1.5.1 - Generic Filter Rule

Filter #: 5,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No            Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице приводятся описания полей меню **Правило фильтра общего типа**.

Табл. 97 Меню 21.1.5.1 — Generic Filter Rule (Правило фильтра общего типа)

ПОЛЕ	ОПИСАНИЕ
Filter # (Номер фильтра)	Номер набора фильтров и номер правила фильтрации, введенные через запятую (например: 2, 3), означают второй набор фильтров и третье правило фильтра в этом наборе.
Filter Type (Тип фильтра)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора типа правила. Параметры, отображаемые для каждого типа фильтра, будут различаться. Вариантами являются: **TCP/IP Filter Rule (Правило фильтра TCP/IP)** или **Generic Filter Rule (Правило фильтра общего типа)**.
Active (Активировать)	Выберите **Yes (Да)** для включения или **No (Нет)** для выключения правила фильтра.
Offset (Смещение)	Введите начальный байт блока данных в пакете, для которого будет производиться сравнение. Значение поля должно находиться в диапазоне от 0 до 255.
Length (Длина)	Введите количество байтов для блока данных в пакете, для которого будет производиться сравнение. Значение поля должно находиться в диапазоне от 0 до 8.
Mask (Маска)	Введите маску (в шестнадцатеричном формате) для применения к блоку данных перед сравнением.

Табл. 97 Меню 21.1.5.1 — Generic Filter Rule (Правило фильтра общего типа)

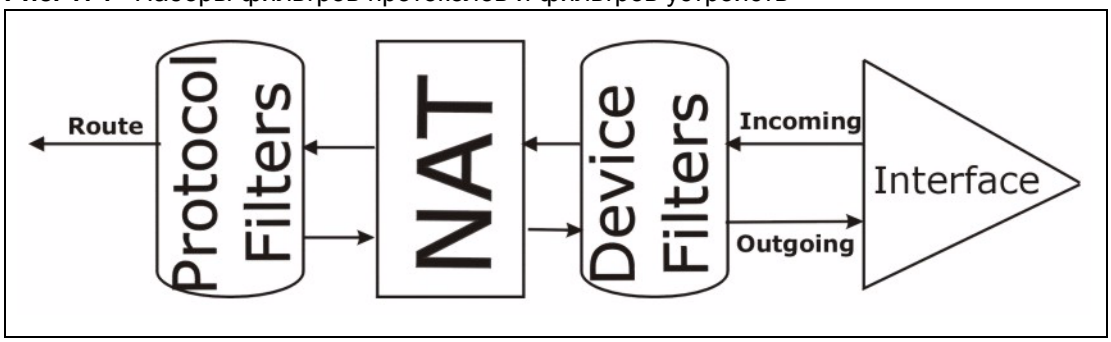
ПОЛЕ	ОПИСАНИЕ
Value (Значение)	Введите значение (в шестнадцатеричном формате) для сравнения с блоком данных.
More (Дополнительно)	Если установлено значение **Yes (Да)**, соответствующий правилу пакет проверяется по следующему правилу фильтра, перед тем как будет выполнено заданное действие; в противном случае пакет обрабатывается в соответствии с полями, где назначены действия. Если в поле **More (Дополнительно)** установлено **Yes (Да)**, то поля **Action Matched (Действие при соответствии)** и **Action Not Matched (Действие при несоответствии)** являются недоступными **(N/A)**.
Log (Регистрационный журнал)	Выберите режим регистрации пакетов из следующих вариантов: **None (Нет)** — пакеты не регистрируются в журнальном файле. **Action Matched (Действие при соответствии)** — регистрируются только пакеты, соответствующие параметрам правила. **Action Not Matched (Действие при несоответствии)** — регистрируются только пакеты, не соответствующие параметрам правила. **Both (Все)** — все пакеты регистрируются в журнальном файле.
Action Matched (Действие при соответствии)	Выберите действие для применения к пакету, для которого обнаружено соответствие правилу. Вариантами являются: **Check Next Rule (Проверить по следующему правилу)**, **Forward (Переслать)** или **Drop (Сбросить)**.
Action Not Matched (Действие при несоответствии)	Выберите действие для применения к пакету, для которого соответствие правилу не обнаружено. Вариантами являются: **Check Next Rule (Проверить по следующему правилу)**, **Forward (Переслать)** или **Drop (Сбросить)**.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "`Press ENTER to Confirm or ESC to Cancel:`" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

29.5 Типы фильтров и NAT

Существуют два класса правил фильтра: правила **фильтра общего типа** для устройстваи правила фильтра протоколов (**TCP/IP**). Правило фильтра общего типа применяются к необработанным данным, передаваемым из/в LAN и WAN. Правила фильтра протоколов применяются к пакетам IP.

Если включена функция NAT (Network Address Translation — Трансляция сетевых адресов), внутренний IP-адрес и номер порта меняются от соединения к соединению, в результате чего становится невозможным выявить точные значения адреса и номера порта. Поэтому, интернет-центр применяет фильтры протоколов к исходному IP-адресу и номеру порта до NAT для исходящих пакетов и после NAT — для входящих пакетов. С другой стороны, общие фильтры (или фильтры устройств), применяются к необработанным пакетам, которые поступают из линии передачи. Такие фильтры применяются в точке, где интернет-центр осуществляет прием или передачу пакетов, например, в порте. Портом может быть порт Ethernet или любой другой аппаратный порт. Применение фильтров показано на следующем рисунке.

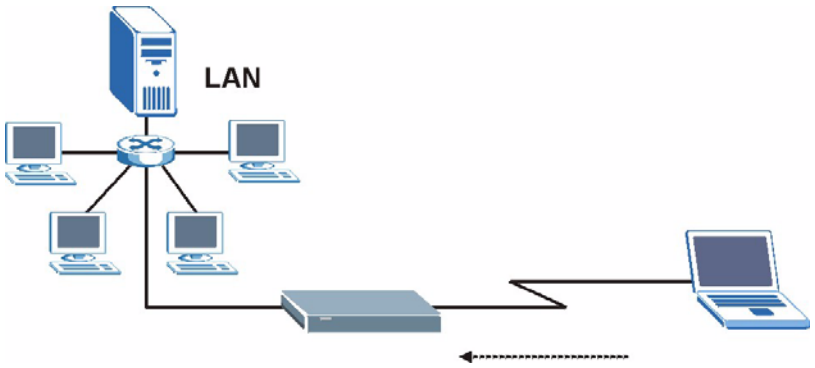
Рис. 174 Наборы фильтров протоколов и фильтров устройств



29.6 Пример фильтра

Рассмотрим пример блокировки подключения к интернет-центру внешних пользователей через Telnet.

Рис. 175 Пример фильтра Telnet



1. В меню 21 введите 1 для перехода в **Меню 21.1 — Filter Set Configuration (Настройка наборов фильтров)**.
2. Введите номер набора фильтров, который необходимо настроить (в данном случае 6).
3. Введите описательное имя или комментарий в поле **Edit Comments (Редактировать комментарий)** (например, TELNET_WAN) и нажмите клавишу [ENTER].
4. Нажмите [ENTER] в строке "`Press [ENTER] to confirm or [ESC] to cancel ...`" для перехода в **Меню 21.1.6 — Filter Rules Summary (Список правил фильтра)**.
5. Введите "1" для создания первого правила фильтра. Настройте параметры в меню, как показано далее.

После нажатия клавиши [ENTER] для подтверждения настроек, появится следующий экран. Обратите внимание, что в этом наборе только одно правило фильтра.

Рис. 176 Меню 21.1.6.1 — Пример фильтра

```
Menu 21.1.6.1 - TCP/IP Filter Rule

Filter #: 6,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 23
Port # Comp= Equal
                Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #=
Port # Comp= Equal
TCP Estab= No
More= No             Log= None
Action Matched= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:
```

После создания набора фильтров его необходимо применить.

1. В главном меню введите "11" для перехода в Меню 11, затем введите номер удаленного узла для редактирования.
2. Переместите курсор в поле **Edit Filter Sets (Редактировать наборы фильтров)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**, затем нажмите клавишу [ENTER].

Появится Меню 11.5. Примените набор фильтров (например, набор фильтров 3) в этом меню, как показано в следующем разделе.

Данное меню показывает, что вы создали и включили (**A = Y**) правило фильтра TCP/IP (**Type = IP**, **Pr = 6**) для портов Telnet (**DP = 23**) получателя.

M = N означает, что действие по фильтру будет выполняться немедленно. Действием является сброс пакета (**m = D**), если пакет соответствует правилу, или немедленная пересылка пакета (**n = F**), если пакет не соответствует правилу, независимо от того, есть ли еще правила для проверки (в данном примере правил больше нет).

Рис. 177 Меню 21.1.6.1 — Список правил фильтра, созданного в примере

```
              Menu 21.1.6 - Filter Rules Summary
 # A Type                      Filter Rules                            M m n
 - - ---- ------------------------------------------------------------- -
- -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                           N D F
 2 N
 3 N
 4 N
 5 N
 6 N

              Enter Filter Rule Number (1-6) to Configure: 1
```

29.7 Применение фильтров и заводских настроек по умолчанию

В данном разделе рассматривается, где следует применять фильтр(ы) после его (их) создания. В Меню 21 изготовителем настроены (но не применены) наборы правил фильтров по умолчанию.

Табл. 98 Таблица наборов фильтров

НАБОРЫ ФИЛЬТРОВ	ОПИСАНИЕ
Наборы входных фильтров:	Фильтры применяются для входящего трафика. Можно применять правила фильтров протоколов или фильтров устройств. Более подробно о типах фильтров см. выше в данной главе.
Наборы выходных фильтров:	Фильтры применяются для исходящего трафика интернет-центра. Можно применять правила фильтров протоколов или фильтров устройств. Более подробно о типах фильтров см. выше в данной главе.
Наборы фильтров вызовов:	Фильтры применяются для проверки, следует ли разрешать конкретному пакету инициировать вызов.

29.7.1 Трафик Ethernet

Необходимость в фильтрации трафика Ethernet возникает редко; тем не менее, наборы фильтров могут быть полезными для блокировки определенных пакетов, снижения объема трафика и предотвращения несанкционированного доступа. Перейдите в Меню 3.1 (показано ниже) и введите номер(а) набора(ов) фильтров, которые вы считаете целесообразным применить. Можно применять до четырех наборов фильтров (из двенадцати) посредством ввода их номеров через запятую, например: 3, 4, 6, 11. Набор фильтров, настроенный изготовителем, `NetBIOS_LAN`, установлен в поле **protocol filters (фильтры протоколов)** в разделе **Input Filter Sets (Наборы входных фильтров)** Меню 3.1 с целью предотвращения генерирования вызовов на сервер DNS локальными сообщениями NetBIOS.

Рис. 178 Фильтрация трафика Ethernet

```
Menu 3.1 – LAN Port Filter Setup


Input Filter Sets:
protocol filters= 3
device filters=
Output Filter Sets:
protocol filters=
device filters=


Press ENTER to Confirm or ESC to Cancel:
```

29.7.2 Фильтры для удаленного узла

Перейдите в Меню 11.5 (показано ниже) и введите номер(а) набора(ов) фильтров для конкретной конфигурации. Можно применить последовательно до четырех наборов фильтров посредством ввода их номеров через запятую. Набор фильтров, настроенный изготовителем, NetBIOS_WAN, установлен в поле **protocol filters (фильтры протоколов)** в разделе **Call Filter Sets (Наборы фильтров вызовов)** Меню 11.5 и служит для блокировки вызовов Интернет-провайдера локальным трафиком NetBIOS.

Рис. 179 Filtering Remote Node Traffic (Фильтрация трафика удаленного узла)

```
Menu 11.5 - Remote Node Filter

          Input Filter Sets:
            protocol filters= 6
            device filters=
          Output Filter Sets:
            protocol filters= 2
            device filters=
          Call Filter Sets:
            Protocol filters=
            Device filters=


Enter here to CONFIRM or ESC to CANCEL:
```

Следует учитывать, что наборы фильтров вызовов доступны, только если выбрана инкапсуляция PPPoA или PPPoE.

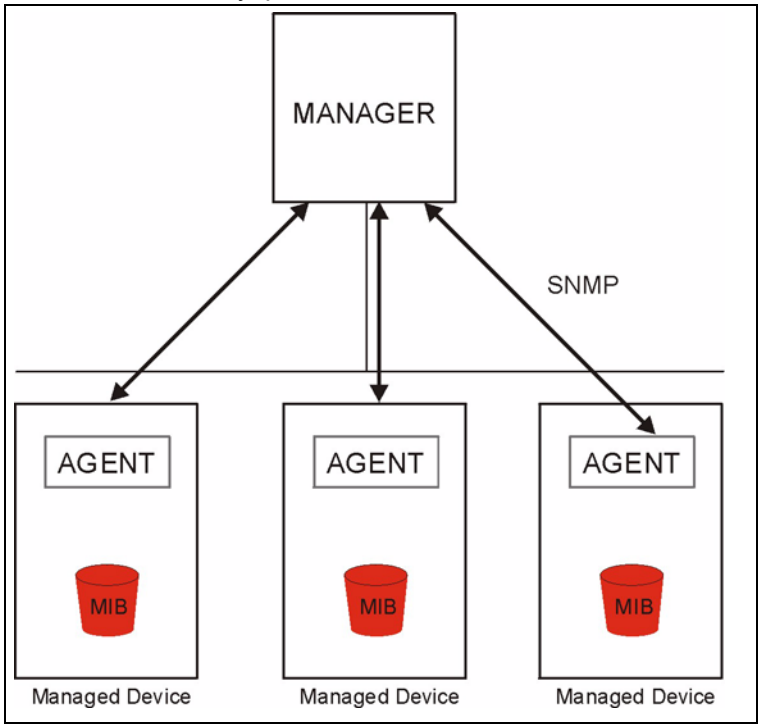
Глава 30
Настройка SNMP

В этой главе описывается Меню 22 — Настройка SNMP.

30.1 О протоколе SNMP

Простой протокол управления сетью (SNMP — Simple Network Management Protocol) используется для осуществления обмена управляющей информацией между сетевыми устройствами. SNMP является одним из элементов стека протоколов TCP/IP. Интернет-центр поддерживает функциональные возможности агента SNMP, что позволяет выполнять мониторинг и управление интернет-центром по сети с управляющего устройства. Интернет-центр поддерживает SNMP версии 1 (SNMPv1) и версии 2 (SNMPv2c). На следующем рисунке показана модель управления по протоколу SNMP. Протокол SNMP является доступным, только если настроен TCP/IP.

Рис. 180 Модель управления SNMP



Сеть, управляемая по протоколу SNMP, состоит из двух основных компонентов: агентов и управляющей программы.

Агент представляет собой модуль программы управления, установленный в управляемом устройстве (в интернет-центре). Агент производит преобразование информации локального управления от управляемого устройства в форму, совместимую с SNMP. Управляющая программа — это консоль управления, с помощью которой сетевые администраторы осуществляют функции управления сетью. С помощью консоли запускаются приложения для контроля и мониторинга управляемых устройств.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют каждую порцию информации, собираемой об этих устройствах. Примерами переменных являются: число принятых пакетов, состояние порта узла и т.д. MIB (Management Information Base — База управляющей информации) — это совокупность данных об управляемых объектах. Протокол SNMP позволяет управляющей программе и агентам взаимодействовать друг с другом с целью доступа к этим объектам.

Протокол SNMP является простым протоколом типа "запрос-ответ" на основе модели "управляющая программа/агент". Управляющее устройство посылает 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 SNMP версии 1 (SNMPv1), если управляющей программе требуется извлечь все элементы из таблицы 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.

30.2 Поддерживаемые базы управляющей информации

Интернет-центр поддерживает RFC-1215 и MIB II, описываемую в RFC-1213, а также собственные MIB корпорации ZyXEL. Базы управляющей информации позволяют сетевым администраторам накапливать статистические данные и выполнять мониторинг состояния и производительности сети.

30.3 Настройка SNMP

Для настройки SNMP в главном меню введите **22** для перехода в **Меню 22 — SNMP Configuration (Настройка SNMP)**, как показано ниже. "Community" для полей "Get", "Set" и "Trap" является просто термином SNMP, обозначающим пароль.

Рис. 181 Меню 22 — SNMP Configuration (Настройка SNMP)

```
Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
  Trap:
    Community= public
    Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются параметры конфигурации SNMP.

Табл. 99 Меню 22 — SNMP Configuration (Настройка SNMP)

ПОЛЕ	ОПИСАНИЕ
SNMP:	
Get Community (Пароль 'Get')	Введите параметр **Get Community (Пароль Get)**, который является паролем для входящих запросов Get- и GetNext- от управляющего устройства.
Set Community (Пароль 'Set')	Введите параметр **Set Community (Пароль Set)**, который является паролем для входящих запросов Set от управляющего устройства.
Trusted Host (Доверенный узел)	Если введен адрес доверенного узла, интернет-центр будет отвечать только на сообщения SNMP, принятые с этого адреса. Если это поле оставлено пустым (по умолчанию), интернет-центр будет отвечать на все принятые сообщения SNMP, независимо от их источника.
Trap (Прерывание):	
Community (Пароль)	Введите пароль Trap, передаваемый с каждым прерыванием на управляющее устройство SNMP.
Destination (Получатель):	Введите IP-адрес устройства, на которое будут посылаться прерывания SNMP.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

30.4 Прерывания SNMP

Интернет-центр посылает прерывания на управляющее устройство SNMP, если произошло какое-либо из следующих событий:

Табл. 100 Прерывания SNMP

НОМЕР ПРЕРЫВАНИЯ #	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
1	coldStart (*описывается в RFC-1215*)	Прерывание посылается после начальной загрузки (включения питания).
2	warmStart (*описывается в RFC-1215*)	Прерывание посылается после загрузки (программная перезагрузка).
3	linkDown (*описывается в RFC-1215*)	Прерывание посылается с указанием номера порта, когда какой-либо из каналов связи не работает. См. следующую таблицу.
4	linkUp (*описывается в RFC-1215*)	Прерывание об установлении соединения посылается с указанием номера порта.
5	authenticationFailure (*описывается в RFC-1215*)	Прерывание посылается на управляющее устройство при приеме запросов get или set SNMP с неверным паролем.
6	whyReboot (описывается в MIB ZYXEL)	Прерывание посылается с указанием кода причины перезапуска перед перезапуском, если система собирается выполнить перезапуск ("горячий" запуск).
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.).

Номером порта является индекс его порта в группе портов.

Табл. 101 Порты и постоянные виртуальные каналы

ПОРТ	PVC (ПОСТОЯННЫЙ ВИРТУАЛЬНЫЙ КАНАЛ)
1	LAN Ethernet
2	1
3	2
…	…
13	12
14	xDSL

Глава 31
Системные функции безопасности

В данной главе описывается порядок установки параметров системных функций безопасности для модели P–660HT/HTW EE.

31.1 Системные функции безопасности

Вы можете настроить системный пароль.

31.1.1 Системный пароль

Введите "23" в главном меню для перехода в **Меню 23 — System Security (Системные функции безопасности)**.

Следует изменить пароль, установленный по умолчанию. Если вы забыли пароль, можно восстановить файл конфигурации по умолчанию.

Рис. 182 Меню 23 — System Security (Системные функции безопасности)

```
Menu 23 - System Security

      1. Change Password
      2. RADIUS Server
      4. IEEE802.1x

Enter Menu Selection Number:
```

31.1.2 Настройка внешнего сервера RADIUS

Откройте **Меню 23.2 — System Security-RADIUS Server (Системные функции безопасности: сервер RADIUS)**. Для этого в **Меню 23 — System Security (Системные функции безопасности)** введите цифру "2".

Рис. 183 Меню 23.2 — System Security (Системные функции безопасности): RADIUS Server (Сервер RADIUS)

```
            Menu 23.2 - System Security - RADIUS Server

                        Authentication Server:
                          Active= No
                          Server Address= 10.11.12.13
                          Port #= 1812
                          Shared Secret= ********
                        Accounting Server:
                          Active= No
                          Server Address= 10.11.12.13
                          Port #= 1813
                          Shared Secret= ********

            Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 102 Меню 23.2 — System Security (Системные функции безопасности): RADIUS Server (Сервер RADIUS)

ПОЛЕ	ОПИСАНИЕ
Authentication Server (Сервер аутентификации)	
Active (Активировать)	Клавишей [ПРОБЕЛ] выберите опцию **Yes (Да)** и нажмите клавишу [ENTER], чтобы включить функцию аутентификации пользователей через внешний сервер аутентификации.
Server Address (Адрес сервера)	Введите в этом поле IP-адрес внешнего сервера аутентификации в десятичном виде с разделительными точками.
Port (Порт)	По умолчанию, для сервера аутентификации RADIUS устанавливается порт **1812**. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.
Shared Secret (Общий секретный ключ)	Введите пароль (до 31 буквенно-цифрового символа) в качестве ключа, общего для внешнего сервера аутентификации и точек доступа. Этот ключ не передается по сети. Интернет-центр и внешний сервер аутентификации должны использовать один и тот же ключ.
Accounting Server (Сервер учета)	
Active (Активировать)	Клавишей [ПРОБЕЛ] выберите опцию **Yes (Да)** и нажмите клавишу [ENTER], чтобы включить функцию аутентификации пользователей через внешний сервер учета.
Server Address (Адрес сервера)	Введите в этом поле IP-адрес внешнего сервера учета в десятичном виде с разделительными точками.
Port (Порт)	По умолчанию, для сервера учета RADIUS устанавливается порт **1813**. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.

Табл. 102 Меню 23.2 — System Security (Системные функции безопасности): RADIUS Server (Сервер RADIUS) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Shared Secret (Общий секретный ключ)	Введите пароль (до 31 буквенно-цифрового символа) в качестве ключа, общего для внешнего сервера учета и точек доступа. Этот ключ не передается по сети. Интернет-центр и внешний сервер учета должны использовать один и тот же ключ.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "`Press ENTER to Confirm or ESC to Cancel:`" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

31.1.3 IEEE 802.1x

Стандарт IEEE 802.1x (Институт инженеров по электротехнике и электронике) описывает расширенные методы обеспечения безопасности для аутентификации беспроводных устройств и управления ключами шифрования.

Чтобы активировать проверку подлинности EAP интернет-центром, выполните указанные ниже операции.

1 Откройте **Меню 23 — System Security (Системные функции безопасности)**. Для этого в главном меню введите "23".

Рис. 184 Меню 23 — System Security (Системные функции безопасности)

```
            Menu 23 - System Security

                   1. Change Password
                   2. RADIUS Server
                   4. IEEE802.1x


            Enter Menu Selection Number:
```

2 Чтобы открыть **Меню 23.4 — System Security (Системные функции безопасности) — IEEE802.802.1x**, введите "4".

Рис. 185 Меню 23.4 — System Security (Системные функции безопасности): IEEE 802.1x

```
            Menu 23.4 - System Security - IEEE 802.1x

                  Wireless Port Control= No Authentication Required
                  ReAuthentication Timer (in second)= N/A
                  Idle Timeout (in second)= N/A
                  Key Management Protocol= N/A
                  Dynamic WEP Key Exchange= N/A
                  PSK= N/A
                  WPA Mixed Mode= N/A
                  Data Privacy for Broadcast/Multicast packets= N/A
                  WPA Broadcast/Multicast Key Update Timer= N/A
                  Authentication Databases= N/A


            Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 103 Меню 23.4 — System Security (Системные функции безопасности): IEEE 802.1x

ПОЛЕ	ОПИСАНИЕ
Wireless Port Control (Управление беспроводной точкой доступа)	Нажатием клавиши [ПРОБЕЛ] выберите режим безопасности для беспроводного доступа к локальной сети. Для того, чтобы открыть доступ пользователю любого беспроводного устройства к проводной сети без ввода имени пользователя и пароля, выберите опцию **No Authentication Required (Аутентификация не требуется)**. Этот вариант является значением по умолчанию. Если выбрать опцию **Authentication Required (Требуется аутентификация),** то для получения доступа к проводной сети пользователь беспроводного устройства должен будет ввести имя пользователя и пароль. Чтобы заблокировать доступ пользователей всех беспроводных устройств к проводной сети, выберите опцию **No Access Allowed (Доступ запрещен)**. Ниже указаны поля, которые недоступны, если выбраны опции **No Authentication Required (Аутентификация не требуется)** или **No Access Allowed (Доступ запрещен)**.
ReAuthentication Timer (Таймер повторной аутентификации в секундах)	Укажите в этом поле периодичность, с которой клиент должен повторно вводить имя пользователя и пароль для того, чтобы сохранять подключение к проводной сети. Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа)**. Укажите отрезок времени в диапазоне значений от 10 до 9999 (в секундах). По умолчанию устанавливается значение в **1800** секунд (или 30 минут).

Табл. 103 Меню 23.4 — System Security (Системные функции безопасности): IEEE 802.1x (продолжение)

ПОЛЕ	ОПИСАНИЕ
Idle Timeout (Макс. время простоя, сек.)	Интернет-центр автоматически отключает клиента от проводной сети по истечении периода простоя. Для того, чтобы вновь получить доступ к проводной сети, клиент должен заново ввести имя пользователя и пароль. Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа)**. По умолчанию устанавливается значение в **3600** секунд (или 1 час).
Key Management Protocol (Протокол управления ключами)	Клавишей [ПРОБЕЛ] выберите **802.1x**, **WPA (Защищенный беспроводной доступ)** или **WPA-PSK (Защищенный беспроводной доступ — Предварительно согласованный ключ)** и нажмите клавишу [ENTER].
Dynamic WEP Key Exchange (Динамический обмен ключами WEP)	Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводной точкой доступа)**. Также в поле **Authentication Databases (Базы данных аутентификации)** установите опцию **RADIUS Only (Только RADIUS)**. Встроенные базы данных пользователей можно не использовать. Чтобы беспроводные устройства могли поддерживать связь с точками доступа без использования динамического обмена ключами WEP, выберите опцию **Disable (Отключить)**. Выберите **64-bit WEP** или **128-bit WEP** для использования шифрования данных соответствующей разрядности. При заданных параметрах динамического обмена ключами WEP, доступ к интернет-центру могут получить до 32 устройств. Это поле недоступно, если **Протокол управления ключами (Key Management Protocol)** установлен на **WPA** или **WPA-PSK**.
PSK (Предварительно согласованный ключ)	Введите предварительно согласованный ключ (от 8 до 63 символов ASCII с учетом регистра, включая пробелы и специальные символы) после выбора **WPA-PSK** в поле **Key Management Protocol (Протокол управления ключами)**.
WPA Mixed Mode (Смешанный режим WPA)	Чтобы активировать смешанный режим WPA, выберите опцию **Enable (Включить)**. В противном случае, выберите опцию **Disable (Отключить)** и установите параметры конфигурации поля **Group Data Privacy (Конфиденциальность групповых данных)**.
Data Privacy for Broadcast/ Multicast packets (Конфиденциальность данных для пакетов широковещательной/ многоадресной рассылки)	В этом поле можно выбрать **TKIP** (рекомендуется) или **WEP** для широковещательного и многоадресного ("группового") трафика, если в **Key Management Protocol** выбран **WPA**, а **WPA Mixed Mode** — отключен. При включении **смешанного режима WPA (WPA Mixed Mode) WEP** задействуется автоматически. При выборе **протокола управления ключами WPA** или **WPA-PSK**, весь одноадресный трафик автоматически шифруется методом **TKIP**.

Табл. 103 Меню 23.4 — System Security (Системные функции безопасности): IEEE 802.1x (продолжение)

ПОЛЕ	ОПИСАНИЕ
WPA Broadcast/ Multicast Key Update Timer (Таймер обновления ключа WPA широковеща-тельной/ многоадресной рассылки)	**Таймер обновления ключа WPA широковещательной/многоадресной рассылки** — это периодичность, с которой точка доступа (если используется управление ключами **WPA-PSK**) или сервер RADIUS (если используется управление ключами **WPA**) отправляет новый групповой ключ всем клиентам. Процесс повторной настройки по ключу является WPA-эквивалентом автоматической замены ключей WEP для точки доступа и всех устройств беспроводной локальной сети на периодической основе. Настройка **таймера обновления ключа WPA для широковещательной/многоадресной рассылки** поддерживается и в режиме WPA-PSK. По умолчанию в интернет-центре установлено значение времени в 1800 секунд (30 минут).
Authentication Databases (Базы данных аутент-ификации)	База данных аутентификации содержит регистрационные сведения о беспроводном устройстве. Локальная база данных пользователей — это встроенная база данных интернет-центра. RADIUS — это внешний сервер. Укажите в этом поле, какую базу данных интернет-центр должен использовать для аутентификации беспроводного устройства (в первую очередь). Прежде, чем выставить приоритет, убедитесь, что соответствующая база данных установлена надлежащим образом. Если для **WPA (Защищенного беспроводного доступа)** используется **Протокол управления ключами (Key Management Protocol),** то в качестве **Баз данных аутентификации (Authentication Databases)** должен использоваться только сервер **RADIUS**. С **Протоколом управления ключами 802.1x** можно использовать только **встроенную базу данных пользователей**. Для того, чтобы интернет-центр выполнял проверку имени пользователя и пароля беспроводного устройства по встроенной базе данных пользователя, выберите опцию **Local User Database Only (Только встроенная база данных пользователей)**. Для того, чтобы интернет-центр выполнял проверку имени пользователя и пароля беспроводного устройства по базе данных пользователя, находящейся на указанном сервере RADIUS, выберите опцию **RADIUS Only (Только RADIUS)**. Для того, чтобы интернет-центр выполнял проверку имени пользователя и пароля беспроводного устройства сначала по базе данных пользователя, находящейся в интернет-центре, выберите опцию **Local first, then RADIUS (Сначала встроенная база, затем RADIUS)**. Если имя пользователя не найдено, интернет-центр производит проверку по базе данных пользователей, находящейся на указанном сервере RADIUS. Для того, чтобы интернет-центр выполнял проверку имени пользователя и пароля беспроводного устройства сначала по базе данных пользователя, находящейся на указанном сервере RADIUS, выберите опцию **RADIUS first, then Local (Сначала RADIUS, затем встроенная база)**. Если интернет-центр не может получить доступ к серверу RADIUS, то он производит проверку по встроенной базе данных пользователей, находящейся в самом интернет-центре. Если имя пользователя не найдено или пароль не соответствует тому, что указано на сервере RADIUS, интернет-центр не производит их проверку по встроенной базе данных пользователей и аутентификация не проходит.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Если функция аутентификации пользователей включена, необходимо указать внешний сервер RADIUS или создать локальные учетные записи пользователей в интернет-центре.

31.2 Создание учетных записей пользователей в интернет-центре

Благодаря локальному сохранению пользовательских профилей, интернет-центр способен определять подлинность беспроводных пользователей, не взаимодействуя с сетевым сервером RADIUS.

Для того, чтобы указать настройки пользователей в интернет-центре, выполните указанные ниже операции.

1 Откройте **Меню14 — Dial-in User Setup (Настройка подключения удаленного пользователя)**. Для этого, в главном меню введите "14".

Рис. 186 Меню 14 — Dial-in User Setup (Настройка подключения удаленного пользователя)

```
                          Menu 14 - Dial-in User Setup

1. ________          9. ________         17. ________         25. ________
2. ________         10. ________         18. ________         26. ________
3. ________         11. ________         19. ________         27. ________
4. ________         12. ________         20. ________         28. ________
5. ________         13. ________         21. ________         29. ________
6. ________         14. ________         22. ________         30. ________
7. ________         15. ________         23. ________         31. ________
8. ________         16. ________         24. ________         32. ________

                                  Enter Menu Selection Number:
```

2 Для изменения настроек пользователя, введите соответствующий номер и нажмите клавишу [ENTER].

Рис. 187 Меню 14.1 — Edit Dial-in User (Редактирование настроек удаленного коммутируемого пользователя)

```
            Menu 14.1 - Edit Dial-in User

                  User Name= test
                  Active= Yes
                  Password= ********


            Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 104 Меню 14.1 — Edit Dial-in User (Редактирование настроек удаленного коммутируемого пользователя)

ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите имя пользователя (не более 31 буквенно-цифрового символа) для данных настроек пользователя. Значения данного поля вводятся с учетом регистра.
Active (Активировать)	Для того, чтобы включить настройки пользователя, при помощи клавиши [ПРОБЕЛ] выберите опцию **Yes (Да)** и нажмите клавишу [ENTER].
Password (Пароль)	Введите пароль (не более 31 буквенно-цифрового символа) для данных настроек пользователя.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "`Press ENTER to Confirm or ESC to Cancel:`" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Глава 32
Информация о системе и диагностика

В этой главе описывается информация о системе и средства диагностики, которые содержатся в Меню SMT с 24.1 по 24.4.

32.1 Обзор

В средства диагностики входит следующее: обновление состояния системы и портов, системные журналы регистрации событий, возможности трассировки, а также обновление программного обеспечения системы. Далее в настоящей главе эти средства описываются более подробно.

В главном меню введите 24 для перехода в **Меню 24 – System Maintenance (Сопровождение системы)** (показано на следующем рисунке).

Рис. 188 Меню 24 — System Maintenance (Сопровождение системы)

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information and Console Port Speed
3.  Log and Trace
4.  Diagnostic
5.  Backup Configuration
6.  Restore Configuration
7.  Upload Firmware
8.  Command Interpreter Mode
9.  Call Control
10.  Time and Date Setting
11.  Remote Management

Enter Menu Selection Number:
```

32.2 Состояние системы

При выборе первого пункта — System Status (Состояние системы) — выводится информация о состоянии и статистике портов (см. ниже). Меню **Состояние системы** можно использовать для контроля функционирования интернет-центра. В частности, отображается информация о состоянии ADSL линии и количестве переданных и принятых пакетов.

Для получения информации о состоянии системы введите 24 (переход в **Меню 24** – **System Maintenance (Сопровождение системы)**).В этом меню выберите пункт 1 **(Состояние системы)**. **Меню 24.1 — System Maintenance (Сопровождение системы): Status (Состояние)** содержит две команды. При вводе "1" сбрасываются счетчики; при нажатии клавиши [ESC] происходит возврат к предыдущему экрану.

В следующей таблице описываются поля **Меню 24.1 — System Maintenance (Сопровождение системы): Status (Состояние)**, которые выводятся в режиме ТОЛЬКО ДЛЯ ЧТЕНИЯ и предназначены для диагностики.

Рис. 189 Меню 24.1 — System Maintenance (Сопровождение системы): Status (Состояние)

```
                  Menu 24.1 - System Maintenance - Status          23:08:47
                                                          Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s     Up
Time
 1-ENET  N/A             0           0           0       0       0     0:00:00
 2       N/A             0           0           0       0       0     0:00:00
 3       N/A             0           0           0       0       0     0:00:00
 4       N/A             0           0           0       0       0     0:00:00
 5       N/A             0           0           0       0       0     0:00:00
 6       N/A             0           0           0       0       0     0:00:00
 7       N/A             0           0           0       0       0     0:00:00
 8       N/A             0           0           0       0       0     0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                        WAN:
      Status: 100M/Full Duplex Tx Pkts: 5731       Line Status: Down
      Collisions: 0           Rx Pkts: 8314       Upstream Speed:     0 kbps
    CPU Load =   25.52%                          Downstream Speed:     0 kbps
                                Press Command:
               COMMANDS: 1-Reset Counters  TAB-Next Page  ESC-Exit
```

В следующей таблице описываются поля **Меню 24.1 — System Maintenance (Сопровождение системы): Status (Состояние)**.

Табл. 105 Меню 24.1 — System Maintenance (Сопровождение системы): Status (Состояние)

ПОЛЕ	ОПИСАНИЕ
Node-Link (Номер — вид соединения)	Порядковый номер удаленного узла и тип соединения. Типы соединений: PPP, ENET, 1483.
Status (Состояние)	Здесь отображается состояние удаленного узла.
TxPkts (Передано пакетов)	Количество пакетов, переданных на данный удаленный узел.

Табл. 105 Меню 24.1 — System Maintenance (Сопровождение системы): Status (Состояние) (продолжение)

ПОЛЕ	ОПИСАНИЕ
RxPkts (Принято пакетов)	Количество пакетов, принятых от данного удаленного узла.
Errors (Ошибки)	Количество пакетов, принятых с ошибками по данному соединению.
Tx B/s (Скорость передачи, байт/с)	Здесь отображается скорость передачи в байтах в секунду.
Rx B/s (Скорость приема, байт/с)	Здесь отображается скорость приема в байтах в секунду.
Up Time (Время соединения)	Время соединения данного канала с текущим удаленным узлом.
My WAN IP (from ISP) (Мой IP адрес в глобальной сети (от Интернет-провайдера)	IP-адрес удаленного узла Интернет-провайдера.
Ethernet	Здесь отображается статистика порта LAN.
Status (Состояние)	Здесь отображается текущее состояние порта LAN.
Tx Pkts (Передано пакетов)	Количество пакетов, переданных в локальную сеть.
Rx Pkts (Принято пакетов)	Количество пакетов, принятых из локальной сети.
Collision (Конфликты)	Количество конфликтов.
WAN	Здесь отображается статистика порта WAN.
Line Status (Состояние линии)	Здесь отображается текущее состояние линии xDSL: Up (Работает) или Down (Не работает).
Upstream Speed (Скорость исходящего трафика)	Здесь отображается скорость передачи исходящего трафика в кбит/с.
Downstream Speed (Скорость входящего трафика)	Здесь отображается скорость передачи входящего трафика в кбит/с.
CPU Load (Загрузка ЦП)	Здесь отображается процент загрузки процессора модема.

32.3 Информация о системе

Для получения информации о системе:

1. Введите "24" для перехода в **Меню 24 — System Maintenance (Сопровождение системы)**.
2. Введите "2" для перехода в **Меню 24.2 — System Information and Console Port Speed (Информация о системе и скорость консольного порта)**.

В этом меню имеется два варианта выбора информации для отображения, как показано на следующем рисунке.

Рис. 190 Меню 24.2 — System Information and Console Port Speed (Информация о системе и скорость консольного порта)

```
Menu 24.2 - System Information and Console Port Speed

1. System Information
2. Console Port Speed

Please enter selection:
```

32.3.1 Информация о системе

В Меню 24.2 введите "1" для отображения следующего экрана.

Рис. 191 Меню 24.2.1 — System Maintenance (Сопровождение системы): Information (Информация)

```
              Menu 24.2.1 - System Maintenance - Information

            Name:
            Routing: IP
            ZyNOS F/W Version: V3.40(ACC.0)| 04/26/2005
            ADSL Chipset Vendor: DMT FwVer: 3.0.11.11_A_TC, HwVer: T14F+
            Standard: Multi-Mode

            LAN
              Ethernet Address: 00:13:49:11:11:35
              IP Address: 192.168.1.1
              IP Mask: 255.255.255.0
              DHCP: Server


                  Press ESC or RETURN to Exit:
```

В следующей таблице описываются поля данного меню.

Табл. 106 Меню 24.2.1 — System Maintenance (Сопровождение системы): Information (Информация)

ПОЛЕ	ОПИСАНИЕ
Name (Имя)	Здесь отображается системное имя интернет-центра. Данный параметр можно изменить в **Меню 1 — General Setup (Настройка общих параметров)**.
Routing (Маршрутизация)	Здесь отображается протокол, который используется для маршрутизации.
ZyNOS F/W Version (Версия микропрограммы ZyNOS)	Здесь отображается версия системной микропрограммы ZyNOS (ZyXEL Network Operating System — Сетевая операционная система ZyXEL). ZyNOS является зарегистрированной торговой маркой ZyXEL Communications Corporation.
ADSL Chipset Vendor (Производитель микросхемы ADSL)	Здесь отображается производитель микросхемы ADSL и версия DSL.
Standard (Стандарт)	Здесь отображается рабочий протокол, используемый интернет-центром и DSL-коммутатором.
LAN (ЛВС)	
Ethernet Address (Ethernet-адрес)	Здесь отображается MAC-адрес интернет-центра (Media Access Control — Управление доступом к среде) или иначе Ethernet-адрес.
IP Address (IP-адрес)	Здесь отображается IP-адрес интернет-центра в десятичном формате с разделительными точками.
IP Mask (IP-маска)	Здесь отображается маска подсети интернет-центра.
DHCP	Здесь отображается режим DHCP интернет-центра: None (Отключить), Relay (Ретранслятор) или Server (Сервер).

32.3.2 Скорость консольного порта

ПРИМЕЧАНИЕ: Консольный порт является внутренним и предназначен только для специалистов.

В **Меню 24.2.2 — System Maintenance (Сопровождение системы): Console Port Speed (Скорость консольного порта)** можно установить различную скорость для консольного порта. Модель P–660HT/HTW EE поддерживает следующие значения: 9600 (по умолчанию), 19200, 38400, 57600 и 115200 бит/с. Нажмие клавишу [ПРОБЕЛ], а затем клавишу [ENTER] для выбора требуемой скорости в Меню 24.2.2 (см. следующий рисунок).

Рис. 192 Меню 24.2.2 — System Maintenance (Сопровождение системы): Change Console Port Speed (Изменение скорости консольного порта)

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

          Console Port Speed: 9600

Press ENTER to Confirm or ESC to Cancel:
```

После изменения скорости консольного порта интернет-центра, также необходимо установить параметр скорости в используемом для соединения с интернет-центром коммуникационном программном обеспечении.

32.4 Журнал регистрации и трассировка

Интернет-центр имеет две функции журнальной регистрации. Первая — ведение журналов регистрации ошибок и результатов трассировок, которые хранятся локально. Вторая — ведение системного журнала для регистрации сообщений.

32.4.1 Просмотр журнала регистрации ошибок

При появлении неполадок сначала необходимо просмотреть журнал регистрации ошибок для установления причин их возникновения. Для просмотра локального журнала регистрации ошибок/трассировки выполните следующие действия:

1. В главном меню введите "24" для перехода в **Меню 24 — System Maintenance (Сопровождение системы)**.
2. В Меню 24 введите "3" для перехода в **Меню 24.3 — System Maintenance (Сопровождение системы): Log and Trace (Журнал регистрации и трассировка)**.

Рис. 193 Меню 24.3 — System Maintenance (Сопровождение системы): Log and Trace (Журнал регистрации и трассировка)

```
            Menu 24.3 - System Maintenance - Log and Trace

                  1. View Error Log
                  2. UNIX Syslog


            Please enter selection
```

3 Введите "1" в **Меню 24.3 — System Maintenance (Сопровождение системы): Log and Trace (Журнал регистрации и трассировка)** для просмотра журнала регистрации ошибок в системе.

После того как интернет-центр отобразит журнал регистрации ошибок, можно очистить журнал, удалив все записи. Примеры типичных сообщений об ошибках и уведомлениях приведены на следующем рисунке.

Рис. 194 Пример уведомлений и сообщений об ошибках

```
 53 Sat Jan 01 00:00:03 2000 PP01 -WARN SNMP TRAP 0: cold start
  54 Sat Jan 01 00:00:03 2000 PP01  INFO  main: init completed
  55 Sat Jan 01 00:00:03 2000 PP01  INFO  Starting Connectivity Monitor
  56 Sat Jan 01 00:00:03 2000 PP20  INFO  adjtime task pause 1 day
  57 Sat Jan 01 00:00:03 2000 PP21  INFO  monitoring WAN connectivity
  58 Sat Jan 01 00:03:06 2000 PP19  INFO  SMT Password pass
  59 Sat Jan 01 00:03:06 2000 PP01  INFO  SMT Session Begin
  60 Sat Jan 01 00:23:21 2000 PP01  INFO  SMT Session End
  62 Sat Jan 01 00:23:38 2000 PP19  INFO  SMT Password pass
  63 Sat Jan 01 00:23:38 2000 PP01  INFO  SMT Session Begin
Clear Error Log (y/n):
```

32.4.2 Системный журнал и учет ресурсов

Интернет-центр использует функцию системного журнала для записи CDR (Call Detail Record — Запись о деталях установления вызова) и системных сообщений на сервере системного журнала (syslog-сервере). Параметры системного журнала и учета ресурсов можно настраивать в **Меню 24.3.2 — System Maintenance (Сопровождение системы): UNIX Syslog (Системный журнал UNIX)**, как показано ниже.

Рис. 195 Меню 24.3.2 — System Maintenance (Сопровождение системы): Syslog and Accounting (Системный журнал и учет ресурсов)

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

UNIX Syslog:
Active= No
Syslog IP Address= ?
Log Facility= Local 1

Press ENTER to Confirm or ESC to Cancel:
```

Необходимо настроить параметры системного журнала UNIX syslog (описаны в следующей таблице), чтобы активировать системный журнал, а затем выбрать события для регистрации.

Табл. 107 Меню 24.3.2 — System Maintenance (Сопровождение системы): Syslog and Accounting (Системный журнал и учет ресурсов)

ПАРАМЕТР	ОПИСАНИЕ
UNIX Syslog (Системный журнал UNIX):	
Active (Активировать)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для включения или отключения системного журнала.
Syslog IP Address (IP-адрес сервера системных журналов)	Введите IP-адрес сервера системного журнала.
Log Facility (Размещение журнала)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора одного из семи локальных режимов. Функция журнальной регистрации позволяет регистрировать сообщения в разных файлах на сервере. См. руководство по UNIX.
После завершения настройки данного меню нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

На следующем рисунке представлены примеры для четырех типов сообщений системного журнала, отправленных интернет-центром:

Рис. 196 Пример системного журнала

```
1 - CDR
SdcmdSyslogSend ( SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
```

Рис. 196 Пример системного журнала (продолжение)

```
call = the call reference number which starts from 1 and increments by 1 for each new
call

str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)

C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)

C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)

L02 Tunnel Connected (L2TP)

C02 OutCall Connected xxxx (= connected speed) xxxxx (= Remote Call ID)

C02 CLID call refused

L02 Call Terminated

C02 Call Terminated

Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing
Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated

2 - Packet Triggered

SdcmdSyslogSend (SYSLOG_PKTTRI, SYSLOG_NOTICE, String);

String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x

Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)

Data: We will send forty-eight Hex characters to the server

Jul 19 11:28:39 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 - Filter Log

SdcmdSyslogSend (SYSLOG_FILLOG, SYSLOG_NOTICE, String);

String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match
(m), drop (D).

Src: Source Address

Dst: Destination Address

prot: Protocol (“TCP”, ”UDP”, ”ICMP”)

spo: Source port

dpo: Destination port

Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP
spo=0208 dpo=0208]} S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF
```

Рис. 196 Пример системного журнала (продолжение)

```
4 - PPP Log

SdcmdSyslogSend (SYSLOG_PPPLOG, SYSLOG_NOTICE, String);

String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown

Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP

Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing
```

32.5 Диагностика

Средства диагностики позволяют проводить тестирование различных функций интернет-центра, чтобы установить, нормально ли работает устройство. Меню 24.4 позволяет выбрать различные типы диагностических тестов для оценки работоспособности системы, как показано на следующем рисунке.

Для перехода в меню **Diagnostic (Диагностика)** выполните следующие действия.

1. В главном меню введите "24" для перехода в **Меню 24 — System Maintenance (Сопровождение системы)**.
2. В данном меню выбрать пункт "4" — "Diagnostic (Диагностика)" чтобы открыть **Меню 24.4 — System Maintenance (Сопровождение системы): Diagnostic (Диагностика)**.

Рис. 197 Меню 24 — System Maintenance (Сопровождение системы): Diagnostic (Диагностика)

```
            Menu 24.4 - System Maintenance - Diagnostic

xDSL                                    System
  1.  Reset xDSL                          21. Reboot System
                                          22. Command Mode
TCP/IP
  12. Ping Host


              Enter Menu Selection Number:

              Host IP Address= N/A
```

В следующей таблице приведено описание диагностических тестов устройства и соединений, доступ к которым осуществляется через Меню 24.4.

Табл. 108 Меню 24 — System Maintenance (Сопровождение системы): Diagnostic (Диагностика)

ПОЛЕ	ОПИСАНИЕ
Reset xDSL (Сброс соединения xDSL)	Повторно инициализирует соединение xDSL с оборудованием телефонной компании.
Ping Host (Эхо-тестирование соединения с узлом)	Выполняет эхо-тестирование узла для определения работоспособности соединений и протокола TCP/IP в обеих системах.
Reboot System (Перезагрузка системы)	Перезагружает интернет-центр.
Command Mode (Режим интерпретатора команд)	Обеспечивает проведение диагностики и тестирования интернет-центра с помощью определенных команд.
Host IP Address (IP-адрес узла)	Если выбрана опция "12" для эхо-тестирования узла, введите адрес компьютера для тестирования.

Глава 33
Сопровождение файлов конфигурации и микропрограммы

В этой главе рассматриваются вопросы резервного копирования и восстановления текущего файла конфигурации, а также обновления файлов конфигурации и микропрограммы.

33.1 Структура имен файлов

Файл конфигурации (часто называемый "romfile" или "rom-0") содержит заводские настройки по умолчанию в некоторых меню: password (пароль), DHCP Setup (Настройка DHCP), TCP/IP Setup (Настройка TCP/IP) и др. Файл конфигурации при поставке имеет расширение "rom". После выполнения пользовательских настроек интернет-центра, файл конфигурации можно сохранить на компьютере в файл с любым именем.

Файл ZyNOS (ZyXEL Network Operating System — Сетевая операционная система ZyXEL), иногда называемый также файлом "ras", является системной микропрограммой и имеет расширение "bin". При использовании большинства клиентов FTP and TFTP, имена файлов имеют вид, показанный далее.

ПРИМЕЧАНИЕ: Необходимо использовать микропрограмму для интернет-центра строго в соответствии с конкретной моделью устройства. См. наклейку, находящуюся на нижней панели интернет-центра.

```
ftp> put firmware.bin ras
```

Это пример сеанса FTP для передачи файла "firmware.bin" с компьютера на интернет-центр.

```
ftp> get rom-0 config.cfg
```

Это пример сеанса FTP для сохранения на компьютере текущей конфигурации модема в файл “`config.cfg`”.

Если ваш клиент (T)FTP не позволяет использовать разные имена для исходного и целевого файлов, то необходимо их переименовать, так как интернет-центр распознает только файлы "rom-0" и "ras". Сохраните исходные копии обоих файлов для дальнейшего использования.

В следующей таблице представлена сводная информация. Обратите внимание, что внутреннее имя файла относится к имени файла в интернет-центре, а внешнее имя файла относится к имени файла вне интернет-центра, то есть на компьютере, в локальной сети или на ftp-сайте, таким образом, имена файлов (но не расширение) могут различаться. После загрузки новой микропрограммы убедитесь, что в поле **ZyNOS F/W Version (Версия микропрограммы ZyNOS)** в **Меню 24.2.1 — System Maintenance (Сопровождение системы): Information (Информация)** отображается правильная версия микропрограммы. В ответ на приглашение перейти в режим отладки в меню SMT, нажмите "Y", а затем введите команду AT.

Табл. 109 Структура имен файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл конфигурации	Rom-0	Это имя файла конфигурации интернет-центра. При загрузке файла rom-0 производится замена всей файловой системы ПЗУ, включая конфигурацию интернет-центра, параметры системы (включая пароль по умолчанию), журнала ошибок и журнала трассировки.	*.rom
Firmware (Микро-программа)	ras	Это базовое имя микропрограммы ZyNOS для интернет-центра.	*.bin

33.2 Резервное сохранение конфигурации

Опция "5" в **Меню 24 — System Maintenance (Сопровождение системы)** позволяет сохранять текущую конфигурацию интернет-центра на компьютере. После того, как получена работающая конфигурация интернет-центра, настоятельно рекомендуется выполнить ее резервное копирование. Наиболее предпочтительным способом для копирования текущей конфигурации на компьютер является сеанс FTP вследствие его высокой скорости. Также может быть использована любая коммуникационная программа, однако для загрузки/выгрузки микропрограммы необходимо использовать протокол Xmodem, в этом случае переименовывать файлы не нужно.

Следует отметить, что термины "загрузка" и "выгрузка" относятся к компьютеру. "Загрузка" означает передачу файла из интернет-центра в компьютер, а "выгрузка" — из компьютера в интернет-центр.

33.2.1 Резервное сохранение конфигурации

Выполните действия, как показано в следующем меню.

Рис. 198 Сеанс Telnet в Меню 24.5

```
              Menu 24.5 - System Maintenance - Backup Configuration
To transfer the configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and SMT
password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current Prestige configuration to
   your workstation.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.



              Press ENTER to Exit:
```

33.2.2 Использование команд FTP в командной строке

1 Запустите клиент FTP на компьютере.

2 Введите "`open`", а затем через пробел — IP-адрес интернет-центра.

3 При появлении запроса на ввод имени пользователя нажмите клавишу [ENTER].

4 Введите пароль (по умолчанию "1234").

5 Введите "`bin`" для установки двоичного режима передачи.

6 Введите команду "`get`" для передачи файлов с интернет-центра на компьютер, например, команда "`get rom-0 config.rom`" передает файл конфигурации с интернет-центра на компьютер и переименовывает его в "`config.rom`". Более подробно о структуре имен файлов см. выше в этой главе.

7 Введите "`quit`" для выхода из режима FTP.

33.2.3 Пример использования команд FTP в командной строке

Рис. 199 Пример сеанса FTP

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

33.2.4 Клиенты FTP на основе графического интерфейса

В следующей таблице описываются некоторые команды, которые могут встретиться в программах клиента FTP на основе GUI (Graphical User Interface — Графический интерфейс пользователя).

Табл. 110 Основные команды для клиентов FTP на основе GUI

КОМАНДА	ОПИСАНИЕ
Host Address (Адрес узла)	Введите адрес узла.
Login Type (Тип регистрации)	Анонимная. В этом случае серверу автоматически предоставляется идентификатор пользователя и пароль для анонимного доступа. Анонимная регистрация возможна только, если эта функция включена Интернет-провайдером или администратором услуг. Обычная. Для регистрации требуется ввести уникальный идентификатор пользователя и пароль.
Transfer Type (Тип передачи)	Передача файлов либо в формате ASCII (формат открытого текста), либо в режиме binary (двоичный).
Initial Remote Directory (Исходный удаленный каталог)	Укажите удаленный каталог по умолчанию (путь).
Initial Local Directory (Исходный локальный каталог)	Укажите локальный каталог по умолчанию (путь).

33.2.5 Ограничение управления через глобальную сеть по TFTP и FTP

TFTP, FTP и Telnet через глобальную сеть не будут работать , если:

- Служба Telnet отключена в Меню 24.11.

- В Меню 3.1 (локальная сеть) или Меню 11.5 (глобальная сеть) применен фильтр для блокировки службы Telnet.
- IP-адрес в поле **Secured Client IP (IP-адрес доверенного клиента)** Меню 24.11 не совпадает с IP-адресом клиента. Если адреса не совпадают, интернет-центр немедленно разрывает сеанс Telnet.
- Уже выполняется сеанс управления с помощью SMT.

33.2.6 Резервное сохранение конфигурации с помощью TFTP

Интернет-центр поддерживает загрузку/выгрузку микропрограммы и файла конфигурации с помощью протокола TFTP (Trivial File Transfer Protocol — Простейший протокол передачи данных) по локальной сети. Хотя TFTP также работает и по глобальной сети, этого делать не рекомендуется.

Для использования TFTP на компьютере должны быть установлены клиенты Telnet и TFTP. Для сохранения файла конфигурации выполните следующие действия:

1. Подключитесь к интернет-центру с помощью Telnet и зарегистрируйтесь в системе. Так как в TFTP не предусмотрена проверка на безопасность, интернет-центр регистрирует IP-адрес клиента Telnet и принимает запросы TFTP только с этого адреса.
2. Переведите SMT в режим интерпретатора команд посредством ввода "8" в **Меню 24 — System Maintenance (Сопровождение системы)**.
3. Введите команду "`sys stdio 0`" для отключения времени простоя SMT, чтобы сеанс TFTP не прерывался. После завершения передачи файла введите команду "`sys stdio 5`", чтобы заново установить время простоя SMT 5 минут (по умолчанию).
4. Запустите на компьютере клиент TFTP и подключитесь к интернет-центру. Перед началом передачи данных установите двоичный режим передачи.
5. Используйте клиент TFTP для передачи файлов между интернет-центром и компьютером (см. пример далее). Для файла конфигурации используется имя "`rom-0`" (rom-ноль, а не заглавная буква O).

Следует помнить, что перед началом и в процессе передачи данных по TFTP, должно быть установлено соединение Telnet, а SMT должен находиться в режиме интерпретатора команд. Для получения подробной информации о командах TFTP (см. следующий пример) следует обратиться к документации по используемой программе клиента TFTP. В операционной системе UNIX используется команда "`get`" для передачи файлов с интернет-центра на компьютер и команда "binary" — для установки двоичного режима передачи.

33.2.7 Пример команды TFTP

Далее приводится пример команды TFTP:

```
tftp [-i] host get rom-0 config.rom
```

где "i" обозначает двоичный режим передачи (этот режим используется при передаче файлов в двоичном коде), "host" — IP-адрес интернет-центра, "get" выполняет передачу файла источника, находящегося в интернет-центре, (rom-0 — имя файла конфигурации интернет-центра) на компьютер и переименовывает его в config.rom.

33.2.8 Клиенты TFTP на основе графического интерфейса

В следующей таблице описываются некоторые команды, которые могут встретиться в программах клиента TFTP на основе GUI.

Табл. 111 Основные команды клиентов TFTP на основе GUI

ПОЛЕ	ОПИСАНИЕ
Host (Имя узла)	Введите IP-адрес интернет-центра. IP-адрес интернет-центра по умолчанию при поставке — 192.168.1.1.
Send/Fetch (Отправить/ Получить)	"Send" используется для загрузки файла в интернет-центр, а "Fetch" — для резервного копирования файла на компьютер.
Local File (Локальный файл)	Введите путь и имя файла микропрограммы (*.bin) или файла конфигурации (*.rom) на компьютере.
Remote File (Файл на удаленном узле)	Имя файла в интернет-центре. Для файла микропрограммы используется имя "ras", а для файла конфигурации — "rom-0".
Binary (Двоичный)	Используется для передачи файла в двоичном режиме.
Abort (Отказ)	Прекращение передачи файла.

Информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети, см. в Разд. 33.2.5 на с. 355.

33.3 Восстановление конфигурации

В данном разделе описывается восстановление предварительно сохраненной конфигурации. Следует помнить, что при восстановлении конфигурации стирается текущая конфигурация; поэтому перед началом восстановления предыдущей конфигурации следует сохранить текущий файл конфигурации на компьютере.

Более предпочтительным способом восстановления конфигурации с компьютера на интернет-центр является сеанс FTP вследствие его высокой скорости. После завершения передачи файла следует подождать, пока система автоматически перезапустится.

ПРИМЕЧАНИЕ: Не прерывайте процесс загрузки файла, поскольку это может привести к ПОЛНОМУ ВЫХОДУ ИЗ СТРОЯ интернет-центра.

33.3.1 Восстановление конфигурации с помощью FTP

Более подробно о резервном копировании с помощью (T)FTP см. в предыдущих разделах этой главы, где описывается загрузка файлов с помощью FTP и TFTP.

Рис. 200 Установка соединения Telnet в Меню 24.6

```
             Menu 24.6 -- System Maintenance - Restore Configuration
To transfer the firmware and configuration file to your workstation, follow
the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and SMT
password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-0 is the
   remote file name on the Prestige. This restores the configuration   to
your Prestige.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.


             Press ENTER to Exit:
```

1. Запустите клиент FTP на компьютере.
2. Введите "`open`", а затем через пробел — IP-адрес интернет-центра.
3. При появлении запроса на ввод имени пользователя нажмите клавишу [ENTER].
4. Введите пароль (по умолчанию "1234").
5. Введите "`bin`" для установки двоичного режима передачи.
6. Найдите файл "`rom`" (на компьютере), который вы хотите восстановить в интернет-центр.
7. Введите команду "`put`" для передачи файлов с компьютера в интернет-центр, например, "`put config.rom rom-0`" передает файл конфигурации "`config.rom`" с компьютера в интернет-центр. Более подробно о структуре имен файлов см. выше в этой главе.
8. Введите "`quit`" для выхода из режима FTP. После успешного завершения процесса восстановления конфигурации интернет-центр автоматически перезапускается.

33.3.2 Пример восстановления конфигурации с помощью сеанса FTP

Рис. 201 Пример восстановления конфигурации с помощью сеанса FTP

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети, см. в Разд. 33.2.5 на с. 355.

33.4 Загрузка файлов конфигурации и микропрограммы

В этом разделе рассматривается загрузка файлов конфигурации и микропрограммы. Для загрузки файла конфигурации можно использовать процедуру, описываемую в Разд. 33.2 на с. 353, или выполнить следующие действия в **Меню 24.7.2 — System Maintenance (Сопровождение системы): Upload System Configuration File (Загрузка файла конфигурации системы)**.

ПРИМЕЧАНИЕ: Не прерывайте процесс загрузки файла, поскольку это может привести к ПОЛНОМУ ВЫХОДУ ИЗ СТРОЯ интернет-центра.

33.4.1 Загрузка микропрограммы

FTP является наиболее предпочтительным методом для загрузки файлов конфигурации и микропрограммы. Для использования данной функции на компьютере должен быть установлен FTP-клиент.

При подключении к интернет-центру через Telnet используются следующие меню для загрузки файла конфигурации и микропрограммы при помощи сеанса FTP.

Рис. 202 Подключение Telnet в Menu 24.7.1 — Upload System Firmware (Загрузка системной микропрограммы)

```
             Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:
  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put firmware filename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

             Press ENTER to Exit:
```

33.4.2 Загрузка файла конфигурации

При подключении через Telnet с помощью Меню 24.7.2 появляется следующий экран.

Рис. 203 Подключение с помощью Telnet в Меню 24.7.2 — System Maintenance (Сопровождение системы)

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configuration filename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.


             Press ENTER to Exit:
```

Для загрузки файлов конфигурации и микропрограммы выполните действия, показанные в приведенных ниже примерах.

33.4.3 Пример загрузки файлов по FTP из командной строки DOS

1. Запустите клиент FTP на компьютере.
2. Введите "`open`", а затем через пробел — IP-адрес интернет-центра.
3. При появлении запроса на ввод имени пользователя нажмите клавишу [ENTER].
4. Введите пароль (по умолчанию "1234").
5. Введите "`bin`" для установки двоичного режима передачи.
6. Введите команду "`put`" для передачи файлов с компьютера на интернет-центр, например, "`put firmware.bin ras`" передает файл микропрограммы (firmware.bin) с компьютера на интернет-центр и переименовывает его в "`ras`". Аналогично команда "`put config.rom rom-0`" передает файл конфигурации (config.rom) с компьютера на интернет-центр и переименовывает его в "`rom-0`". Подобным образом, команда "`get rom-0 config.rom`" передает файл конфигурации с интернет-центра на компьютер и переименовывает его в "`config.rom`". Более подробно о структуре имен файлов см. выше в этой главе.
7. Введите "`quit`" для выхода из режима FTP.

После успешной загрузки файла, интернет-центр автоматически перезапускается.

33.4.4 Пример загрузки микропрограммы с помощью сеанса FTP

Рис. 204 Пример загрузки микропрограммы с помощью сеанса FTP

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Другие команды (для клиентов FTP с графическим интерфейсом пользователя) перечислены в этой главе ранее.

Информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети, см. в Разд. 33.2.5 на с. 355.

33.4.5 Загрузка файлов с помощью TFTP

Интернет-центр поддерживает загрузку файлов микропрограммы с помощью протокола TFTP (Trivial File Transfer Protocol — Простейший протокол передачи данных) по локальной сети. Хотя TFTP также работает и по глобальной сети, этого делать не рекомендуется.

Для использования TFTP на компьютере должны быть установлены клиенты Telnet и TFTP. Для передачи микропрограммы и файла конфигурации выполните следующие действия.

1. Подключитесь к интернет-центру с помощью Telnet и зарегистрируйтесь в системе. Так как в TFTP не предусмотрена проверка на безопасность, интернет-центр регистрирует IP-адрес клиента Telnet и принимает запросы TFTP только с этого адреса.
2. Переведите SMT в режим интерпретатора команд посредством ввода "8" в **Меню 24 — System Maintenance (Сопровождение системы)**.
3. Введите команду "`sys stdio 0`" для отключения времени простоя SMT, чтобы сеанс TFTP не прерывался. После завершения передачи файла введите команду “`sys stdio 5`”, чтобы заново установить время простоя SMT 5 минут (по умолчанию).
4. Запустите на компьютере клиент TFTP и подключитесь к интернет-центру. Перед началом передачи данных установите двоичный режим передачи.
5. Используйте клиент TFTP для передачи файлов между интернет-центром и компьютером (см. пример далее). Имя файла микропрограммы: "`ras`".

Следует помнить, что перед началом и в процессе передачи данных по TFTP, должно быть установлено соединение Telnet, а SMT должен находиться в режиме интерпретатора команд. Для получения подробной информации о командах TFTP (см. следующий пример) следует обратиться к документации по используемой программе клиента TFTP. В операционной системе UNIX используется команда "`get`" для передачи файлов с интернет-центра на компьютер, "`put`" — для передачи в обратном направлении и "`binary`" — для установки двоичного режима передачи.

33.4.6 Пример команды для загрузки файла с помощью сеанса TFTP

Далее приводится пример команды TFTP:

```
tftp [-i] host put firmware.bin ras
```

где "`i`" обозначает двоичный режим передачи (этот режим используется при передаче двоичных файлов), "`host`" — IP-адрес интернет-центра, "`put`" выполняет передачу файла с компьютера (`firmware.bin`– имя файла микропрограммы на компьютере) в целевой файл на удаленном узле (`ras` — имя файла микропрограммы в интернет-центре).

Команды для клиентов TFTP на основе GUI перечислены ранее в этой главе.

Глава 34
Сопровождение системы

В данной главе описываются меню SMT с 24.8 до 24.10.

34.1 Режим интерпретатора команд

Интерпретатор команд CI (Command Interpreter) является частью основной микропрограммы. CI обеспечивает большинство функций SMT, а также некоторые возможности настройки и диагностики более низкого уровня. Для входа в режим CI используется Меню SMT 24.8. Более подробную информацию о командах CI можно найти на компакт-диске, входящем в комплект поставки или на Web-сайте www.zyxel.ru. Введите "8" в **Меню 24 — System Maintenance (Сопровождение системы)**. Для отображения списка доступных команд введите `help` или `?` в командной строке. После завершения работы введите `exit` для возврата в **Главное меню SMT**.

Рис. 205 Режим интерпретатора команд в Меню 24

```
                Menu 24 - System Maintenance

                   1.  System Status
                   2.  System Information and Console Port Speed
                   3.  Log and Trace
                   4.  Diagnostic
                   5.  Backup Configuration
                   6.  Restore Configuration
                   7.  Upload Firmware
                   8.  Command Interpreter Mode
                   9.  Call Control
                   10. Time and Date Setting
                   11. Remote Management

             Enter Menu Selection Number:
```

Рис. 206 Доступные команды

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             poe             config          pci
wlan            ip              ppp             bridge
hdap            bm              lan             radius
8021x
ras>
```

34.2 Контроль вызовов

Функция контроля вызовов является доступной, только если в поле **Encapsulation (Инкапсуляция)** Меню 4 или Меню 11.1 установлено значение **PPPoE**.

Функция управления бюджетом позволяет установить ограничение на общую продолжительность исходящих соединений интернет-центра за определенный период времени. Если общая продолжительность исходящих вызовов превысит установленный предел, текущий вызов будет сброшен, а все последующие исходящие вызовы будут заблокированы.

Для доступа к меню контроля вызовов в Меню 24 введите "9" для перехода в **Меню 24.9 — System Maintenance (Сопровождение системы): Call Control (Контроль вызовов)**, как показано в следующей таблице.

Рис. 207 Меню 24.9 — System Maintenance (Сопровождение системы): Call Control (Контроль вызовов)

```
            Menu 24.9 - System Maintenance - Call Control

            1. Budget Management

            Enter Menu Selection Number:
```

34.2.1 Управление бюджетом

В Меню 24.9.1 отображается статистика управления бюджетом для исходящих вызовов. Введите "1" в **Меню 24.9 — System Maintenance (Сопровождение системы): Call Control (Контроль вызовов)** для перехода в следующее меню.

Рис. 208 Меню 24.9.1 — System Maintenance (Сопровождение системы): Budget Management (Управление бюджетом)

```
              Menu 24.9.1 - System Maintenance - Budget Management


Remote Node        Connection Time/Total Budget  Elapsed Time/Total Period
1.MyIsp                        No Budget                     No Budget
2.--------                     ---                           ---
3.--------                     ---                           ---
4.--------                     ---                           ---
5.--------                     ---                           ---
6.--------                     ---                           ---
7.--------                     ---                           ---
8.--------                     ---                           ---



              Reset Node (0 to update screen):
```

Общий бюджет представляет собой ограничение на суммарное время исходящих вызовов к удаленному узлу. Достижение данного лимита времени приводит к сбрасыванию текущего вызова, а последующие исходящие вызовы на этот удаленный узел блокируются. По истечении каждого периода общий бюджет сбрасывается. По умолчанию для общего бюджета установлено 0 минут, а для периода — 0 часов, т. е. функция управления бюджетом отключена. Пользователь может сбросить суммарное время соединения, посредством ввода порядкового номера удаленного узла. Введите 0 для обновления экрана. Бюджет и период сброса бюджета для удаленного узла устанавливаются в Меню 11.1, если выбрана инкапсуляция PPPoE.

Табл. 112 Меню 24.9.1 — System Maintenance (Сопровождение системы): Budget Management (Управление бюджетом)

ПОЛЕ	ОПИСАНИЕ
Remote Node (Удаленный узел)	Введите порядковый номер удаленного узла, для которого требуется сбросить время соединения (только один в данном случае).
Connection Time/Total Budget (Время соединения/Общий бюджет)	Общее время соединения, прошедшее в рамках выделенного бюджета, установленного в Меню 11.1.
Elapsed Time/Total Period (Истекшее время/Общий период)	Период — это цикл времени в часах, через который сбрасывается выделенный бюджет (см. *меню 11.1.*). Истекшее время — это общее время соединения за этот период.
Введите “0” для обновления экрана или нажмите клавишу [ESC] для возврата к предыдущему экрану.	

34.3 Установка времени и даты

Интернет-центр ведет счет времени и дат. Устройство оснащено программным механизмом для установки времени вручную, а также для получения текущего времени и даты от внешнего сервера при включении интернет-центра. Меню 24.10 позволяет обновить параметры времени и даты интернет-центраа.После этого в журналах регистрации ошибок и журналах межсетевого экрана интернет-центра будет указываться реальное время.

В главном меню выберите Меню 24 для перехода в **Меню 24 — System Maintenance (Сопровождение системы)**, как показано ниже.

Рис. 209 Меню 24 — System Maintenance (Сопровождение системы)

```
Menu 24 - System Maintenance

                1.  System Status
                2.  System Information and Console Port Speed
                3.  Log and Trace
                4.  Diagnostic
                5.  Backup Configuration
                6.  Restore Configuration
                7.  Upload Firmware
                8.  Command Interpreter Mode
                9.  Call Control
                10. Time and Date Setting
                11. Remote Management

Enter Menu Selection Number:
```

Введите "10" для перехода в **Меню 24.10 — System Maintenance (Сопровождение системы): Time and Date Setting (Установка времени и даты)** для обновления в интернет-центре параметров времени и даты (см. следующий рисунок).

Рис. 210 Меню 24.10 — System Maintenance (Сопровождение системы): Time and Date Setting (Установка времени и даты)

```
        Menu 24.10 - System Maintenance - Time and Date Setting
  Use Time Server when Bootup= None
  Time Server Address= N/A
  Current Time:                          00 : 51 : 24
  New Time (hh:mm:ss):                   00 : 51 : 19
  Current Date:                          2000 - 01 - 01
  New Date (yyyy-mm-dd):                 2000 - 01 - 01
  Time Zone= GMT
  Daylight Saving= No
  Start Date (mm-dd):                          01 - 00
  End Date (mm-dd):                            01 - 00

          Press ENTER to Confirm or ESC to Cancel:
```

Табл. 113 Меню 24.10 — System Maintenance (Сопровождение системы): Time and Date Setting (Установка времени и даты)

ПОЛЕ	ОПИСАНИЕ
Use Time Server when Bootup (Использовать сервер времени при загрузке)	Введите протокол сервиса времени по которому ваш сервер времени передает информацию при включении интернет-центра. Не все серверы времени поддерживают любые протоколы, поэтому следует проконсультироваться с Интернет-провайдером/сетевым администратором, или попытаться определить работающий протокол методом проб и ошибок. Основные отличия между протоколами заключаются в формате представления времени. Формат **Daytime (RFC 867)** содержит 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. Формат **NTP (RFC-1305)** аналогичен формату **Time (RFC-868)**. **None (Нет)**. Это значение установлено по умолчанию, введите время вручную.
Time Server Address (Адрес сервера времени)	Введите IP-адрес или доменное имя сервера времени. Если вы не обладаете этой информацией, следует обратиться к Интернет-провайдеру/сетевому администратору.
Current Time (Текущее время)	В данном поле после повторного входа в меню отображается обновленное время.
New Time (Новое время)	Введите новое время в формате часы, минуты и секунды.
Current Date (Текущая дата)	В данном поле после повторного входа в меню отображается обновленная дата.
New Date (Новая дата)	Введите новую дату в формате год, месяц и день.
Time Zone (Часовой пояс)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для установки разницы во времени между вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time — GMT).
Daylight Saving (Переход на летнее время)	Если используется переход на летнее время, выберите **Yes (Да)**.

Табл. 113 Меню 24.10 — System Maintenance (Сопровождение системы): Time and Date Setting (Установка времени и даты) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Start Date (Дата начала)	Если используется переход на летнее время, введите месяц и день начала летнего времени.
End Date (Конечная дата)	Если используется переход на летнее время, введите месяц и день окончания летнего времени.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

34.3.1 Обновление времени

- Интернет-центр обновляет время в следующих трех случаях:
- При выходе из Меню 24.10 после внесения изменений.
- При загрузке интернет-центра, если в Меню 24.10 настроен сервер времени.
- Каждые 24 часа после запуска.

Глава 35
Удаленное управление

В этой главе описывается удаленное управление модемом (Меню SMT 24.11).

35.1 Удаленное управление — общая информация

Функция удаленного управления позволяет определить, каким службам/протоколам разрешен доступ к интерфейсу управления интернет-центром (если таковые имеются), и с каких компьютеров.

При установке параметров конфигурации удаленного управления, предназначенного для реализации функций управления через глобальную вычислительную сеть (WAN), необходимо также настроить правило межсетевого экрана для получения доступа. Более подробно о настройках правил межсетевого экрана см. главы, посвященные межсетевому экрану.

35.2 Удаленное управление

Чтобы отключить удаленное управление конкретной службой, выберите **Disable (Отключить)** в соответствующем поле **Server Access (Доступ к серверу)**.

Введите "11" в Меню 24 для перехода в **Меню 24.11 — Remote Management Control (Контроль удаленного управления)**.

35.2.1 Настройка удаленного управления

Возможны следующие варианты удаленного управления интернет-центром P–660HT/HTW EE:

через глобальную сеть (**WAN only**), через локальную сеть (**LAN only**), через локальную и глобальную сеть (**ALL**), либо удаленное управление может быть запрещено (**Disable**).

- через глобальную сеть (Интернет)
- отовсюду (через локальную и глобальную сеть)
- только через локальную сеть
- отключение функции

Если функция удаленного управления для конкретной службы включена, но при этом применен фильтр блокировки этой службы, то выполнять удаленное управление интернет-центром с помощью этой службы будет нельзя.

Введите "11" в Меню 24 для перехода в **Меню 24.11 — Remote Management Control (Контроль удаленного управления)** (показано далее).

Рис. 211 Меню 24.11 — Remote Management Control (Контроль удаленного управления)

```
            Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                  Server Access = LAN only
  Secured Client IP = 0.0.0.0
FTP Server:
  Server Port = 21                  Server Access = LAN only
  Secured Client IP = 0.0.0.0
Web Server:
  Server Port = 80                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

            Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 114 Меню 24.11 — Remote Management Control (Контроль удаленного управления)

ПОЛЕ	ОПИСАНИЕ
Telnet Server (Telnet-сервер) FTP Server (FTP-сервер) Web Server (Web-сервер)	Каждое из этих полей только для чтения обозначает службу или протокол.
Port (Порт)	В данном поле отображается номер порта для службы или протокола. Если требуется, вы можете здесь изменить номер порта, но для доступа к интернет-центру будет необходимо использовать этот же номер порта.
Access (Доступ)	При необходимости выберите, откуда разрешено управления, нажав клавишу [ПРОБЕЛ]. Вариантами являются: **LAN only (Только через локальную сеть)**, **WAN only (Только через глобальную сеть)**, **All (Через локальную и глобальную сеть)** или **Disable (Отключить)**. По умолчанию установлено **LAN only** (только через локальную сеть).
Secured Client IP (IP-адрес доверенного клиента)	По умолчанию используется адрес 0.0.0.0, что позволяет любому клиенту использовать данную службу или протокол для удаленного управления интернет-центром. Введите IP-адрес, чтобы предоставить доступ только клиентам с совпадающим IP-адресом.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

35.2.2 Ограничения на удаленное управление

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

- Применен фильтр для блокировки службы Telnet, FTP или Web в Меню 3.1 (LAN — локальная сеть) или Меню 11.5 (WAN — глобальная сеть) .
- Эта служба отключена в Меню 24.11.
- IP-адрес, установленный в поле **Secured Client IP (IP-адрес доверенного клиента)** Меню 24.11 не совпадает с IP-адресом клиента. В случае несовпадения адресов интернет-центр немедленно разрывает сеанс управления.
- Уже выполняется другой сеанс удаленного управления, имеющий равный или более высокий приоритет. Одновременно допускается проведение только одного сеанса удаленного управления.
- Имеется правило межсетевого экрана, блокирующее удаленное управление.

35.3 Удаленное управление и NAT

При включении функции NAT:

- При настройке через глобальную сеть следует использовать IP-адрес интернет-центра в глобальной сети.
- При настройке через локальную сеть следует использовать IP-адрес интернет-центра в локальной сети.

35.4 Время бездействия системы

Максимальное время бездействия системы во время сеанса управления по умолчанию установлено на 5 минут (300 секунд). Интернет-центр автоматически завершает сеанс управления при бездействии более этого периода. Сеанс управления не разрывается, если выполняется непрерывное обновление состояния системы в Меню 24.1, или если время бездействия было изменено с помощью команды `sys stdio` в командной строке.

Глава 36
Политика маршрутизации IP (IPPR)

В этой главе рассматривается настройка и применение политик, используемых для маршрутизации IP.

36.1 Описание политики маршрутизации IP (IP Policy Routing)

Как правило, маршрутизация производится только на основе адреса получателя, поэтому интегрированное устройство доступа выбирает самый короткий путь для пересылки пакета. Политика маршрутизации IP (IPPR) обеспечивает механизм замены схемы маршрутизации по умолчанию, и позволяет изменить правила для пересылки пакета на основе политики, определяемой сетевым администратором. Маршрутизация на основе политики, применяемая к входящим пакетам каждого порта, имеет приоритет перед стандартной маршрутизацией.

36.2 Преимущества политики маршрутизации IP

Маршрутизация на базе источника (Source-Based Routing) — сетевые администраторы могут использовать такую политику для направления трафика от разных пользователей через различные соединения.

Качество обслуживания предоставляемых услуг передачи данных (QoS) — организации могут дифференцировать трафик с помощью установки приоритетов или значения TOS (Type of Service — Тип услуги) в IP-заголовке на периферии сети для включения функции распределения трафика в магистрали в соответствии с приоритетом.

Сокращение расходов (Cost Savings) — IPPR позволяет организациям использовать дорогостоящие каналы с высокой пропускной способностью для интерактивного трафика, а дешевые каналы — для пакетного трафика.

Распределение нагрузки (Load Sharing) — сетевые администраторы могут использовать IPPR для распределения трафика по нескольким каналам.

36.3 Политика маршрутизации

Конкретные политики маршрутизации используются как часть общего процесса IPPR. Политика определяет критерии соответствия и действие, которое должно быть выполнено, если пакет отвечает этим критериям. Действие выполняется только в случае, если достигнуто соответствие всем критериям. Критериями служат адрес и порт источника, протокол IP (ICMP, UDP, TCP и т.д.), адрес и порт получателя, TOS и приоритет (поля в IP-заголовке), а также длина пакета. Критерий длины используется для разделения интерактивного трафика и трафика массивов данных. Интерактивные приложения, например, Telnet, обычно используют короткие пакеты, тогда как трафик массивов данных, например, передача файлов, — длинные.

Действия, выполняемые при соответствии критериям:

- маршрутизация пакета на другой шлюз (и, следовательно, выходной порт)
- установка полей TOS и приоритета в IP-заголовке.

По характеру и реализации IPPR аналогична существующей функции фильтрации пакетов RAS (Remote access service — Служба удаленного доступа). Политики группируются в наборы, каждый из которых состоит из родственных политик. Прежде чем применять политики к порту или удаленному узлу, их необходимо создать, аналогично созданию фильтров. Существует возможность создания 12 наборов политик по шесть политик в каждом.

36.4 Настройка политики маршрутизации IP

В Меню 25 отображаются все заданные политики.

Рис. 212 Меню 25 — IP Routing Policy Setup (Настройка политики маршрутизации IP)

```
                Menu 25 - IP Routing Policy Setup

Policy
Set #         Name                    Set #         Name
------  -----------------             ------  -----------------
  1      _________________               7      _________________
  2      _________________               8      _________________
  3      _________________               9      _________________
  4      _________________              10      _________________
  5      _________________              11      _________________
  6      _________________              12      _________________

            Enter Policy Set Number to Configure= 0

            Edit Name= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

Для создания политики маршрутизации выполните следующие действия:

1. В главном меню ведите "25" для перехода в **Меню 25 — IP Routing Policy Setup (Настройка политики маршрутизации IP)**.
2. Введите номер набора политик, который необходимо настроить, для перехода в **Меню 25.1 — IP Routing Policy Setup (Настройка политики маршрутизации IP)**.

Меню 25.1 содержит сводную информацию о наборе политик, включая критерии и действие для каждой конкретной политики, а также ее состояние: включена или нет. Каждая политика состоит из двух строк. В первой части определяются критерии для входящего пакета, а во второй — применяемое действие. Разделитель "|", стоящий между двумя частями, означает, что действие применяется при соответствии пакета критериям, а разделитель "=" — при несоответствии.

Рис. 213 Меню 25.1 — IP Routing Policy Setup (Настройка политики маршрутизации IP)

```
Menu 25.1 - IP Routing Policy Setup

 # A                          Criteria/Action
 - - ------------------------------------------------------------------------
 1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
     SP=20-25,DP=20-25,P=6,T=NM,PR=0              |GW=192.168.1.1,T=MT,PR=0
 2 N ____________________________________________________________________________
     ____________________________________________________________________________
 3 N ____________________________________________________________________________
     ____________________________________________________________________________
 4 N ____________________________________________________________________________
     ____________________________________________________________________________
 5 N ____________________________________________________________________________
     ____________________________________________________________________________
 6 N ____________________________________________________________________________
     ____________________________________________________________________________

Enter Policy Rule Number (1-6) to Configure:
```

Табл. 115 Меню 25.1 — IP Routing Policy Setup (Настройка политики маршрутизации IP)

СОКРАЩЕНИЕ		ЗНАЧЕНИЕ
Критерий	SA	IP-адрес источника
SP		Порт источника
DA		IP-адрес получателя
DP		Порт получателя
P		Номер протокола IP уровня 4 (TCP=6, UDP=17…)
T		Тип услуги для входящего пакета
Pr		Приоритет входящего пакета
Действие	GW	IP-адрес шлюза
T		Тип услуги для исходящего пакета
P		Приоритет исходящего пакета
Услуга	NM	Стандартный режим
MD		Минимальная задержка
MT		Максимальная пропускная способность
MR		Максимальная надежность
MC		Минимальная стоимость

Введите число от "1" до "6" для перехода в **Меню 25.1.1 — IP Routing Policy (Политика маршрутизации IP)** (см. следующий рисунок).Это меню позволяет настраивать правила политики.

Рис. 214 Меню 25.1.1 — IP Routing Policy (Политика маршрутизации IP)

```
            Menu 25.1.1 - IP Routing Policy

Policy Set Name= test
Active= No
Criteria:
  IP Protocol    = 0
  Type of Service= Don't Care           Packet length= 0
  Precedence     = Don't Care             Len Comp= N/A
  Source:
    addr start= 0.0.0.0                 end= N/A
    port start= N/A                     end= N/A
  Destination:
    addr start= 0.0.0.0                 end= N/A
    port start= N/A                     end= N/A
Action= Matched
  Gateway addr   = 0.0.0.0              Log= No
  Type of Service= No Change
  Precedence     = No Change

            Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля данного меню.

Табл. 116 Меню 25.1.1 — IP Routing Policy (Политика маршрутизации IP)

ПОЛЕ	ОПИСАНИЕ
Policy Set Name (Имя набора политик)	Имя набора политик, присвоенное в **Меню 25 — IP Routing Policy Setup (Настройка политики маршрутизации IP)**.
Active (Активировать)	Нажмите клавишу [ПРОБЕЛ] и затем клавишу [ENTER] для выбора **Yes**, чтобы включить данную политику, или **No**, чтобы отключить. Неактивные политики отображаются в Меню 25 SMT со знаком минуса ("–").
Criteria (Критерии)	
IP Protocol (Протокол IP)	Протокол IP уровня 4, например, **UDP**, **TCP**, **ICMP** и т. д.
Type of service (Тип услуги)	Определите тип услуги для входящего сетевого трафика. Вариантами являются: **Don't Care (Не определен)**, **Normal (Стандартное)**, **Min Delay (Минимальная задержка)**, **Max Thruput (Максимальная пропускная способность)**, **Min Cost (Минимальная стоимость)** или **Max Reliable (Максимальная надежность)**.
Precedence (Приоритет)	Значение приоритета входящего пакета. Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора значения от **0** до **7** или **Don't Care (Не определен)**.
Packet Length (Размер пакета)	Введите размер входящих пакетов (в байтах). Операторы в поле **Len Comp (Сравнение размера)** (следующее поле) применяются к пакетам для сравнения по этому размеру.
Len Comp (Сравнение размера)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора оператора сравнения. Вариантами являются: **Equal (Равно)**, **Not Equal (Не равно)**, **Less (Меньше)**, **Greater (Больше)**, **Less or Equal (Меньше или равно)** или **Greater or Equal (Больше или равно)**.
Source (Источник):	

Табл. 116 Меню 25.1.1 — IP Routing Policy (Политика маршрутизации IP)

ПОЛЕ	ОПИСАНИЕ
addr start / end (начальный/ конечный адрес)	Диапазон IP-адресов источника от начального до конечного.
port start / end (начальный/ конечный порт)	Диапазон номеров портов источника от начального до конечного; применяется только для TCP/UDP.
Destination:	
addr start / end (начальный/ конечный адрес)	Диапазон IP-адресов получателя от начального до конечного.
port start / end (начальный/ конечный порт)	Диапазон номеров портов получателя от начального до конечного; применяется только для TCP/UDP.
Action (Действие)	Определяет, условие выполнения действия: при соответствии пакета критериям (**Matched**) или несоответствии (**Not Matched**).
Gateway addr (Адрес шлюза)	Определяет адрес исходящего шлюза. Если шлюз находится в локальной сети, он должен принадлежать к той же подсети, что и интернет-центр, в противном случае шлюзу должен быть назначен IP-адрес удаленного узла. Для шлюза по умолчанию установлено значение 0.0.0.0.
Type of service (Тип услуги)	Установите новое значение типа услуги для исходящего пакета. Вариантами являются: **No Change** (Не изменять), **Normal** (Стандартный), **Min Delay** (С минимальной задержкой), **Max Thruput** (Максимальная пропускная способность) или **Max Reliable** (Максимальная надежность) или **Min Cost** (Минимальная стоимость).
Precedence (Приоритет)	Установите новое значение приоритета для исходящего пакета. Значение приоритета может быть от **0** до **7** или **No Change** (Без изменения).
Log (Регистрационный журнал)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора **Yes**, чтобы после создания политики в системном журнале была сделана запись.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "`Press ENTER to Confirm or ESC to Cancel:`" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

36.5 Применение политики IP

В этом разделе описывается применение политик IP после их создания.

36.5.1 Политики IP для Ethernet

В **Меню 3 — Ethernet Setup (Настройка Ethernet)** введите 2 для перехода в **Меню 3.2 — TCP/IP and DHCP Ethernet Setup (Настройка TCP/IP и DHCP для Ethernet)**.

Можно применить до четырех наборов политик IP (из 12), посредством ввода их номеров через запятую, например: 2, 4, 7, 9.

Рис. 215 Меню 3.2 — Настройка TCP/IP и DHCP для Ethernet

```
            Menu 3.2 - TCP/IP and DHCP Setup

                    DHCP Setup
                      DHCP= Server
                      Client IP Pool Starting Address= 192.168.1.33
                      Size of Client IP Pool= 32
                      Primary DNS Server= 0.0.0.0
                      Secondary DNS Server= 0.0.0.0
                      Remote DHCP Server= N/A
                    TCP/IP Setup:
                      IP Address= 192.168.1.1
                      IP Subnet Mask= 255.255.255.0
                      RIP Direction= Both
                        Version= RIP-1
                      Multicast= None
                      IP Policies=
                      Edit IP Alias= No

            Press ENTER to Confirm or ESC to Cancel:
```

Перейдите в Меню 11.3 (показано ниже) и введите номер(а) набора(ов) политик маршрутизации IP по мере необходимости. Можно последовательно применить до четырех наборов политик посредством ввода их номеров через запятую.

Рис. 216 Меню 11.3 — Remote Node Network Layer Options (Параметры сетевого уровня удаленного узла)

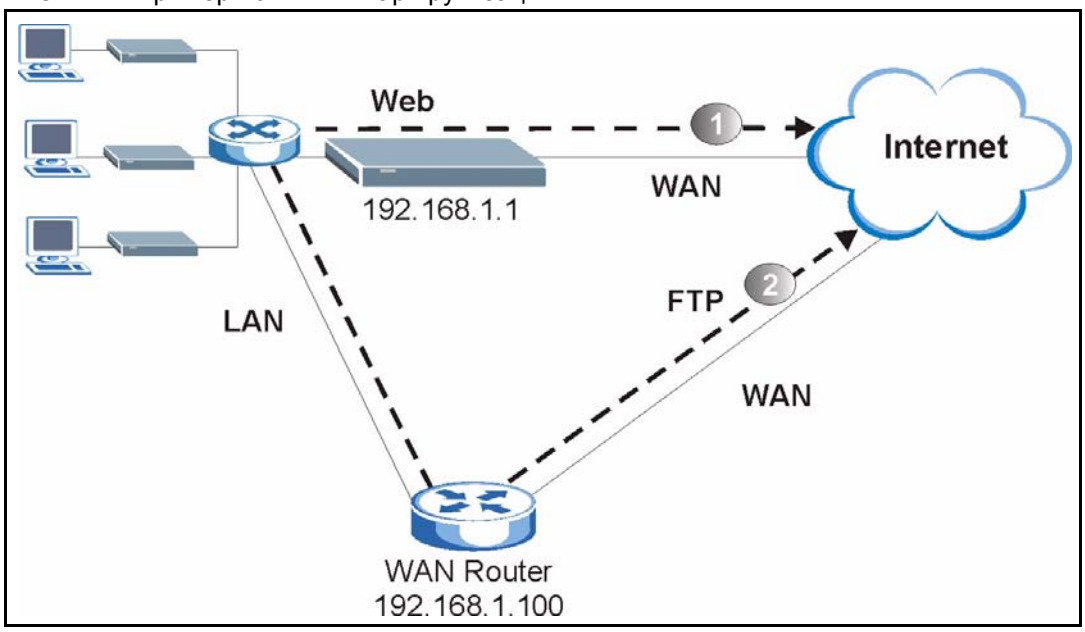
```
            Menu 11.3 - Remote Node Network Layer Options

IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

            Press ENTER to Confirm or ESC to Cancel:
```

36.6 Пример политики маршрутизации IP

Если сеть одновременно имеет два соединения — с Интернетом и с удаленным узлом — Web-пакеты можно пересылать в Интернет с использованием одной политики, а FTP-пакеты в удаленную сеть — с использованием другой. См. следующий рисунок.

Маршрут 1 является маршрутом IP по умолчанию, а маршрут 2 представляет собой созданный маршрут IP.

Рис. 217 Пример политики маршрутизации IP



Для принудительного направления пакетов от клиентов с IP-адресами от 192.168.1.33 до 192.168.1.64 в Интернет через порт WAN интернет-центра, выполните следующие действия:

1. Создайте набор политик маршрутизации в Меню 25.
2. Создайте правило в этом наборе в **Меню 25.1.1 — IP Routing Policy (Политика маршрутизации IP)**, как показано ниже.

Рис. 218 Пример политики маршрутизации IP

```
                Menu 25.1.1 - IP Routing Policy

  Policy Set Name= set1             Packet length= 10
  Active= Yes                         Len Comp= N/A
  Criteria:
    IP Protocol    = 6              end= 192.168.1.64
    Type of Service= Don't Care     end= N/A
    Precedence     = Don't Care     end= N/A
    Source:                         end= 80
      addr start= 192.168.1.2       Log= No
   port start= 0
    Destination:
   addr start= 0.0.0.0
   port start= 80
  Action= Matched
 Gateway addr  = 192.168.1.1
    Type of Service= No Change
    Precedence     = No Change


     Press ENTER to Confirm or ESC to Cancel:
```

1. Проверьте в **Меню 25.1 — IP Routing Policy Setup (Настройка политики маршрутизации IP)**, правильно ли создано новое правило.
2. Создайте еще один набор политик маршрутизации в Меню 25.
3. Создайте в Меню 25.1 правило в этом наборе, предназначенное для маршрутизации пакетов от любого узла (`IP=0.0.0.0` обозначает любой узел) с помощью протокола TCP и для доступа к порту FTP через другой шлюз (192.168.1.100).

Рис. 219 Пример политики маршрутизации IP

```
            Menu 25.1.1 - IP Routing Policy

        Policy Set Name= set2          Packet length= 10
        Active= Yes                      Len Comp= N/A
        Criteria:
          IP Protocol    = 6           end= N/A
          Type of Service= Don't Care  end= N/A
          Precedence     = Don't Care  end= N/A
          Source:                      end= 21
            addr start= 0.0.0.0        Log= No
         port start= 0
          Destination:
        addr start= 0.0.0.0
        port start= 20
        Action= Matched
    Gateway addr =192.168.1.100
         Type of Service= No Change
         Precedence     = No Change



            Press ENTER to Confirm or ESC to Cancel:
```

4 Проверьте в **Меню 25.1 — IP Routing Policy Setup (Настройка политики маршрутизации IP)**, правильно ли создано новое правило.

5 Примените оба набора политик в Меню 3.2, как показано ниже.

Рис. 220 Пример применения политик IP

```
            Menu 3.2 - TCP/IP and DHCP Ethernet Setup

                 DHCP Setup
                   DHCP= Server
                   Client IP Pool Starting Address= 192.168.1.33
                   Size of Client IP Pool= 64
                   Primary DNS Server= 0.0.0.0
                   Secondary DNS Server= 0.0.0.0
                   Remote DHCP Server= N/A
                 TCP/IP Setup:
                   IP Address= 192.168.1.1
                   IP Subnet Mask= 255.255.255.0
                   RIP Direction= Both
                     Version= RIP-1
                   Multicast= None
                   IP Policies= 1,2
                   Edit IP Alias= No


            Press ENTER to Confirm or ESC to Cancel:
```

Глава 37
Расписание вызовов

Функция расписания вызовов (применяется только для инкапсуляции PPPoA или PPPoE) позволяет устанавливать время и продолжительность вызовов на удаленный узел.

37.1 Введение

Функция расписания вызовов позволяет интернет-центру управлять удаленным узлом и определять время и продолжительность вызовов на удаленный узел. Эта функция аналогична таймеру записи видеомагнитофона (где можно установить период времени для записи). Можно применять до 4 наборов расписаний с помощью **Меню 11.1 — Remote Node Profile (Профиль удаленного узла)**. В главном меню, введите "26" для перехода в **Меню 26 — Schedule Setup (Создание расписания)**, как показано ниже.

Рис. 221 Меню 26 — Schedule Setup (Создание расписания)

```
            Menu 26 - Schedule Setup

  Schedule
  Set #           Name                    Set #           Name
  ------  ------------------              ------  ------------------
    1       ________________                7       ________________
    2       ________________                8       ________________
    3       ________________                9       ________________
    4       ________________               10       ________________
    5       ________________               11       ________________
    6       ________________               12       ________________

            Enter Schedule Set Number to Configure= 0

            Edit Name= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

Расписание с меньшим номером имеет приоритет над расписанием с более высоким номером, благодаря чему исключаются конфликты между расписаниями. Например, если для удаленного узла применены наборы 1, 2, 3 и 4, то набор 1 будет иметь приоритет над наборами 2, 3 и 4, так как интернет-центр по умолчанию применяет сначала наборы с более низкими номерами. Набор 2 будет иметь приоритет над наборами 3 и 4 и так далее.

Для одного удаленного узла можно создавать до 12 наборов расписаний, но применять — не более четырех.

Для удаления расписания введите номер набора и нажмите клавишу **[ПРОБЕЛ]** и затем **[ENTER]** (или [delete]) в поле **Edit Name** (Редактировать имя).

Для создания набора расписания, выберите набор в Меню 26 (1-12) и нажмите клавишу [ENTER] для перехода в **Меню 26.1 — Schedule Set Setup (Создание набора расписания)**, как показано ниже.

Рис. 222 Меню 26.1 — Schedule Set Setup (Создание набора расписания)

```
            Menu 26.1 Schedule Set Setup

               Active= Yes
               Start Date(yyyy-mm-dd)= 2000 - 01 - 01
               How Often= Once
               Once:
                 Date(yyyy-mm-dd)= 2000 - 01 - 01
               Weekdays:
                 Sunday= N/A
                 Monday= N/A
                 Tuesday= N/A
                 Wednesday= N/A
                 Thursday= N/A
                 Friday= N/A
                 Saturday= N/A
               Start Time(hh:mm)= 00: 00
               Duration(hh:mm)= 00: 00
               Action= Forced On

            Press ENTER to Confirm or ESC to Cancel:
```

Если соединение уже установлено, интернет-центр не будет его разрывать. После разрыва соединения вручную или вследствие превышения времени простоя, к удаленному узлу нельзя будет обратиться до истечения периода **Duration (Продолжительность)**.

Табл. 117 Меню 26.1 — Schedule Set Setup (Создание набора расписания)

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Нажмите клавишу [ПРОБЕЛ] для выбора **Yes** или **No**. Выберите **Yes** и нажмите клавишу [ENTER] для включения данного расписания.
Start Date (Дата начала)	Введите дату начала применения данного расписания, в формате "год-месяц-день". Допускаются даты, начиная с текущей даты и до 5 февраля 2036 г.
How Often (Периодичность)	Применяется ли данное расписание еженедельно или будет выполняться только один раз? Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора **Once (Однократно)** или **Weekly (Еженедельно)**. Оба эти варианта взаимно исключают друг друга. Если выбрано **Once (Однократно)**, выбор дня недели недоступен (**N/A**). Если выбрано **Once (Однократно)**, правило расписания автоматически удаляется после того, как указанное время прошло.
Once (Однократно): Date (Дата)	Если в указанном выше поле **How Often (Периодичность)** выбрано **Once (Однократно)**, введите дату активирования расписания в формате "год-месяц-день".

Табл. 117 Меню 26.1 — Schedule Set Setup (Создание набора расписания)

ПОЛЕ	ОПИСАНИЕ
Weekday (День недели): Day (День)	Если в указанном выше поле **How Often (Периодичность)** выбрано **Weekly (Еженедельно)**, выберите день (дни), когда необходимо активировать набор (или повторить), т. е. перейдите к нужному дню(дням) и нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**, а затем нажмите клавишу [ENTER].
Start Time (Время начала)	Введите время начала применения расписания в формате "часы-минуты".
Продолжи-тельность	Введите максимально допустимую продолжительность соединения в формате "часы-минуты".
Action (Действие)	Значение **Forced On (Принудительно поддерживать)** означает, что соединение поддерживается независимо от наличия запроса в линии и сохраняется в течение времени, заданного в поле **Duration (Продолжительность)**. **Forced Down (Принудительно разрывать)** означает, что соединение блокируется независимо от наличия запроса в линии. **Enable Dial-On-Demand (Разрешить вызов по требованию)** означает, что данное расписание разрешает соединение по запросу в линии. **Disable Dial-On-Demand (Запретить вызов по требованию)** означает, что данное расписание не разрешает соединение по запросу в линии.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения “`Press ENTER to Confirm or ESC to Cancel:`” (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

После настройки расписаний их нужно применить к требуемому удаленному узлу(ам). Введите "11" в **Главном меню**, а затем введите индекс удаленного узла. Используя клавишу [ПРОБЕЛ] выберите **PPPoE** или **PPPoA** в поле **Encapsulation (Инкапсуляция)**, а затем нажмите клавишу [ENTER] для того, чтобы сделать доступными поля расписаний, как показано ниже.

Рис. 223 Применение расписания к удаленному узлу (PPPoE)

```
            Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                    Route= IP
Active= Yes                             Bridge= No
Encapsulation= PPPoA                    Edit IP/Bridge= No
Multiplexing= LLC-based                 Edit ATM Options= No
Service Name= N/A                       Edit Advance Options= N/A
Incoming:                               Telco Option:
  Rem Login=                              Allocated Budget(min)= 0
  Rem Password= ********                  Period(hr)= 0
Outgoing:                                 Schedule Sets=
  My Login= ChangeMe                      Nailed-Up Connection= No
  My Password= ********                 Session Options:
  Authen= CHAP/PAP                        Edit Filter Sets= No
                                          Idle Timeout(sec)= 0

            Press ENTER to Confirm or ESC to Cancel:
```

Для одного удаленного узла можно применить до четырех расписаний, посредством ввода их номеров через запятую. Измените номера расписаний в соответствии с требованиями.

Глава 38
Поиск и устранение неисправностей

В данной главе рассматриваются возможные неисправности и способы их устранения.

38.1 Неисправности при запуске интернет-центра

Табл. 118 Устранение неполадок при запуске интернет-центра P–660HT/HTW EE

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
При включении электропитания интернет-центра ни один из светодиодов не загорается.	Убедитесь, что адаптер питания подключен к интернет-центру и к соответствующему источнику питания. Проверьте, включен ли OMNI ADSL и источник питания. Выключите и снова включите интернет-центр. Если проблема не устранена, возможно, имеет место аппаратная неисправность. В этом случае следует связаться с поставщиком оборудования.

38.2 Проблемы с локальной сетью

Табл. 119 Устранение неисправностей в локальной сети

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Светодиод LAN не горит.	Проверьте тип кабеля Ethernet и его подключение (более подробную информацию см. в *Кратком руководстве*). Проверьте исправность кабеля Ethernet.
	Убедитесь, что карта Ethernet компьютера работает нормально.
Отсутствует доступ к интернет-центру из локальной сети.	Если опция **Any IP (Любой IP)** отключена, то проверьте, находятся ли IP-адрес и маска подсети интернет-центра и Ваших компьютеров в одной и той же подсети.

38.3 Проблемы с глобальной сетью (WAN)

Табл. 120 Поиск и устранение неполадок с WAN

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Светодиод DSL не горит.	Проверьте телефонный провод и соединение между портом DSL интернет-центра и телефонной розеткой.
	Убедитесь, что телефонная компания проверила вашу телефонную линию и установила оборудование для услуг DSL.
	Сбросьте ADSL линию, а затем повторно установите соединение с DSL-коммутатором. Более подробную информацию см. в Табл. 68 на с. 235 (web-конфигуратор) или Табл. 108 на с. 350 (SMT).
Невозможно получить IP-адрес в глобальной сети от Интернет-провайдера.	Интернет-провайдер предоставляет IP-адрес в глобальной сети после проведения аутентификации. Аутентификация может проводиться с использованием имени пользователя и пароля, MAC-адреса или имени узла. Имя пользователя и пароль применяются только при инкапсуляции PPPoE и PPPoA. Убедитесь, что вы правильно ввели **Service Type (Тип услуги)**, **User Name (Имя пользователя)** и **Password (Пароль)** (убедитесь в правильном использовании регис. символов). См. главу "Настройка глобальной сети" (web-конфигуратор или SMT).
Невозможно получить доступ в Интернет.	Убедитесь, что интернет-центр включен и подключен к сети. Проверьте настройки глобальной сети. См. главу по настройке глобальной сети (Web-конфигуратор) или раздел о доступе в Интернет (SMT). Убедитесь, что вы ввели правильное имя пользователя и пароль. При использовании транзита PPPoE-соединений, убедитесь, что включена функция моста.
Подключение к Интернету разрывается.	Проверьте правила расписания вызовов. См. Гл. 37 на с. 384 (SMT). Если используется инкапсуляция PPPoA или PPPoE, проверьте значение времени простоя. См. Гл. 6 на с. 102 (Web-конфигуратор) или Гл. 24 на с. 270 (SMT). Свяжитесь с вашим Интернет-провайдером.

38.4 Проблемы с доступом к интернет-центру

Табл. 121 Проблемы с доступом к интернет-центру

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Невозможно получить доступ к интернет-центру.	Имя пользователя для доступа — “admin”. По умолчанию установлен пароль "1234". Поля **Password (Пароль)** и **Username (Имя пользователя)** необходимо заполнять с учетом регистра. Убедитесь, что вы ввели правильный пароль и имя пользователя в соответствующем регистре. Если вы изменили пароль и забыли его, то необходимо загрузить файл конфигурации по умолчанию. При этом восстанавливаются заводские настройки по умолчанию, включая пароль.
Нет доступа к Web-конфигуратору.	Убедитесь, что не проводится сеанс управления с помощью SMT. При настройке через глобальную сеть следует использовать IP-адрес интернет-центра в глобальной сети. См. инструкции по проверке подключения к глобальной сети. При настройке через локальную сеть следует использовать IP-адрес интернет-центра в локальной сети. См. указания для выполнения проверки подключения к локальной сети. Проверьте, что доступ к службе web включен. Если установлен IP-адрес доверенного клиента, IP-адрес вашего компьютера должен совпадать с ним. Более подробную информацию см. в главе об удаленном управлении. Для доступа через локальную сеть, IP-адреса вашего компьютера и интернет-центра должны находиться в одной подсети. Если вы изменили IP-адрес интернет-центра в локальной сети, то в поле URL необходимо ввести новый адрес. Удалите все фильтры в меню SMT 3.1 (LAN) или 11.5 (WAN), которые блокируют службу web. Проверьте в следующем разделе, разрешены ли всплывающие окна, сценарии и разрешения Java.

38.4.1 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).

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

38.4.1.1 Блокирование всплывающих окон в Internet Explorer

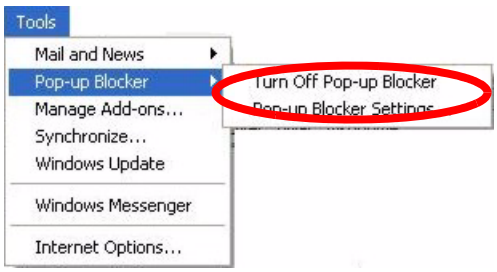
Чтобы зарегистрироваться на Вашем устройстве, Вам возможно придется отключить блокирование всплывающих окон.

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.

38.4.1.1.1 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)**.

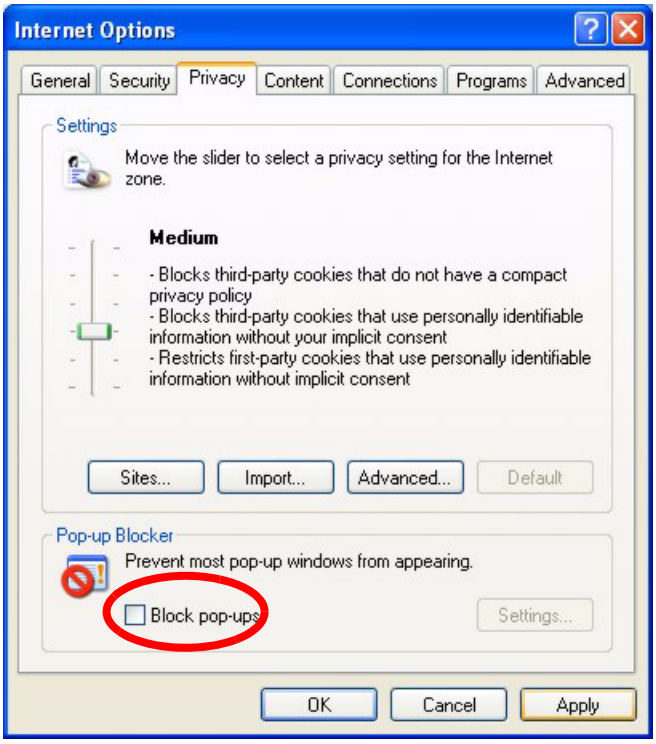
Рис. 224 Блокирование всплывающих окон



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

1. Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Privacy (Конфиденциальность)**.
2. Уберите галочку из окошка **Block pop-ups (Блокировать всплывающие окна)** в разделе **Pop-up Blocker (Блокирование всплывающих окон)** в нижней части окна. Это отключит блокирование всплывающих окон.

Рис. 225 Свойства обозревателя



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

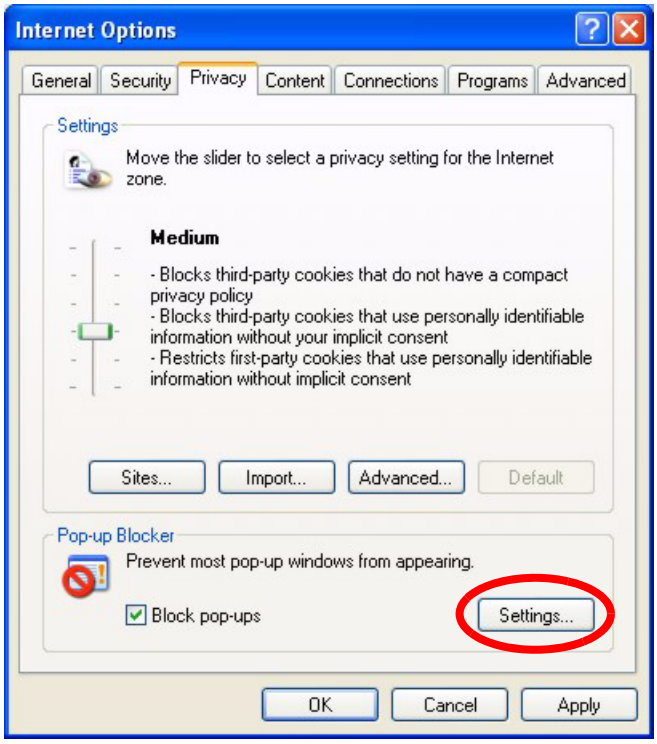
38.4.1.1.2 Включение блокировки всплывающих окон с исключениями

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)**, **Privacy (Конфиденциальность)**.

2 Выберите **Settings… (Параметры...)** — откроется окно **Pop-up Blocker Settings (Параметры блокирования всплывающих окон)**.

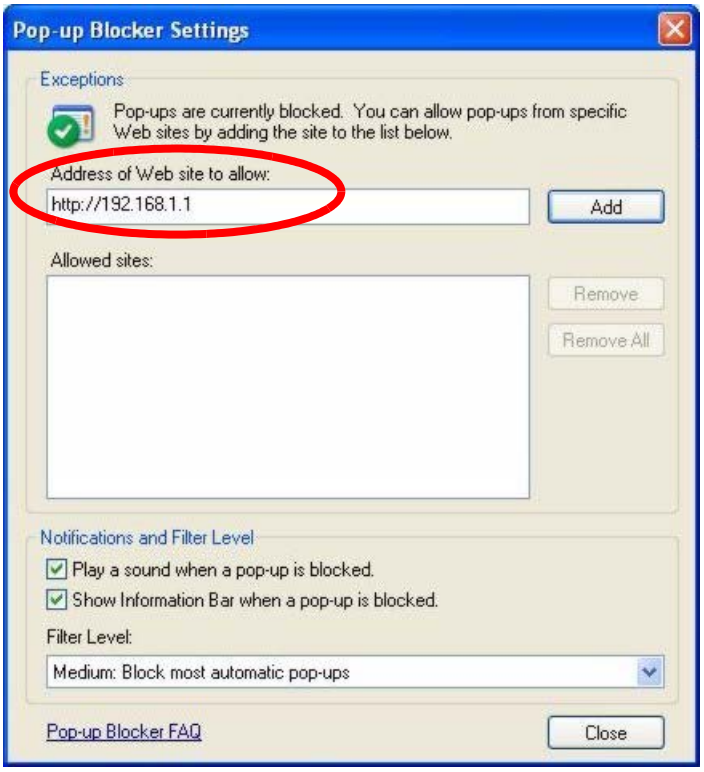
Рис. 226 Свойства обозревателя



3 Введите IP-адрес Вашего устройства (web-сайт, который Вы не хотите блокировать) с приставочкой “http://”. Например, введите http://192.168.1.1

4 Нажмите кнопку **Add (Добавить)** для переноса IP-адреса в список **Allowed sites (Разрешенные веб-узлы)**.

Рис. 227 Параметры блокирования всплывающих окон



5 Для возврата на вкладку **Privacy (Конфиденциальность)** нажмите кнопку **Close (Закрыть)**.

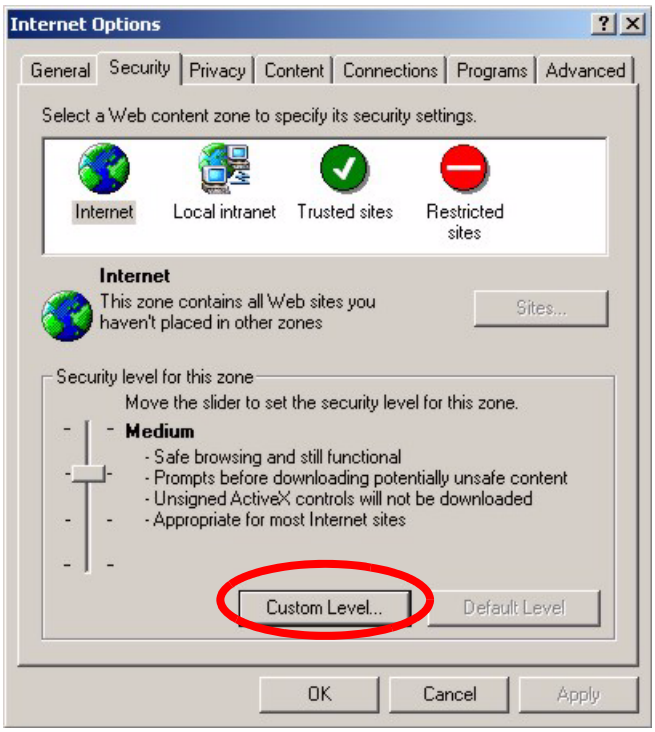
6 Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки.

38.4.1.2 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)**, **Security (Безопасность)**.

Рис. 228 Свойства обозревателя



2 Нажмите кнопку **Custom Level... (Другой...)**.

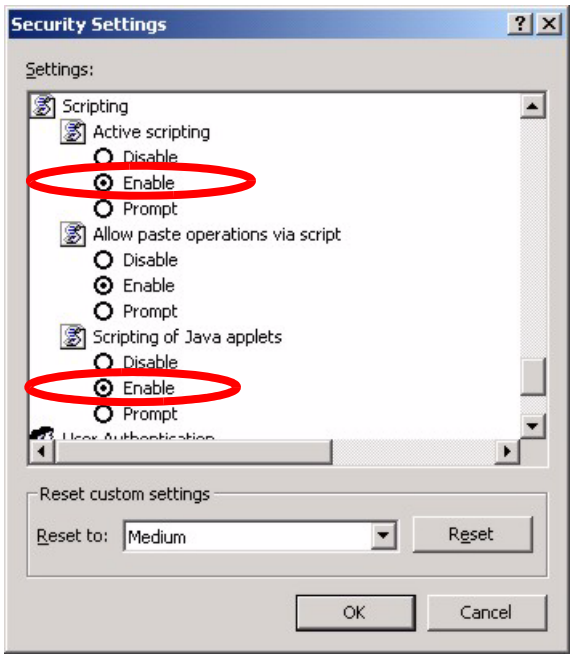
3 Пролистайте до раздела **Scripting (Сценарии)**.

4 Для **Active scripting (Активные сценарии)** должно быть выбрано **Enable (Разрешить)** (значение по умолчанию).

5 Для **Scripting of Java applets (Выполнять сценарии приложений Java)** также должно быть выбрано **Enable (Разрешить)** (значение по умолчанию).

6 Нажмите **OK**, чтобы закрыть окно.

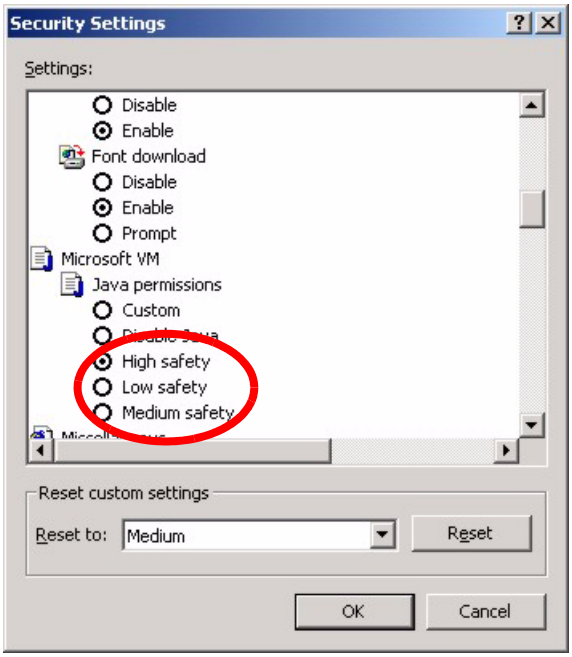
Рис. 229 Параметры безопасности — Выполнение сценариев приложений Java



38.4.1.3 Разрешения Java

1. Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Security (Безопасность)**.
2. Нажмите кнопку **Custom Level... (Другой...)**.
3. Спуститесь вниз к разделу **Microsoft VM**.
4. Для **Java permissions (Разрешения Java)** должен быть выбран уровень безопасности.
5. Нажмите **OK**, чтобы закрыть окно.

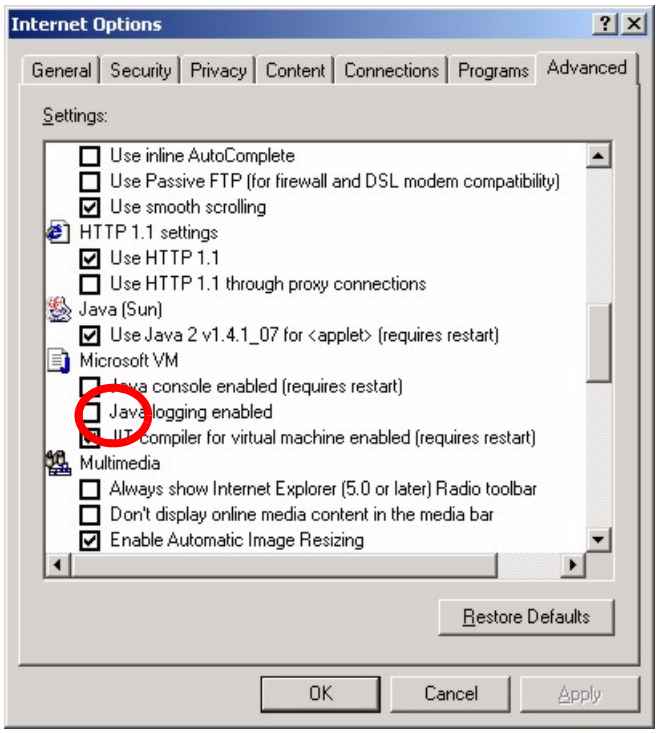
Рис. 230 Параметры безопасности — Java



38.4.1.3.1 JAVA (Sun)

1. Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Advanced (Дополнительно)**.
2. Убедитесь, что под **Java (Sun)** выбрана опция **Use Java 2 for <applet> (Использовать Java 2 для приложения)**.
3. Нажмите **OK**, чтобы закрыть окно.

Рис. 231 Java (Sun)



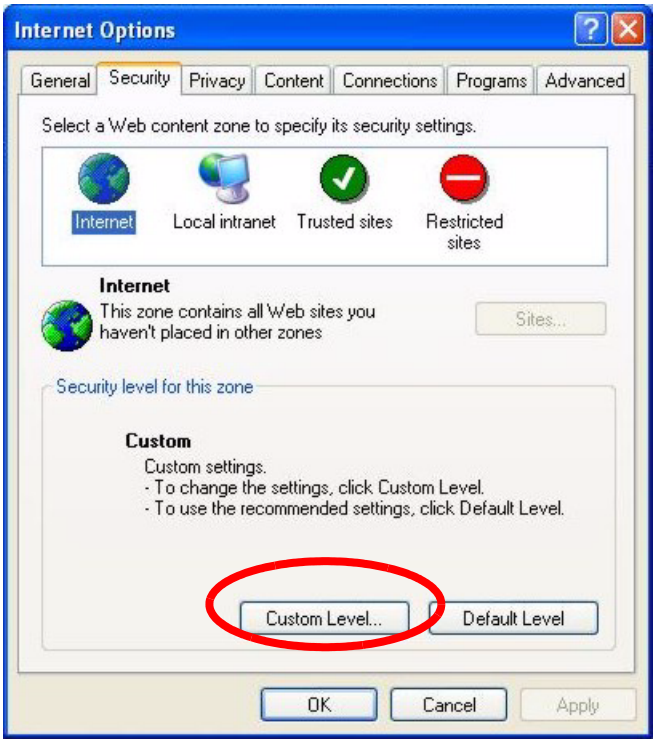
38.4.2 Управление элементами ActiveX Internet Explorer

Если элементы ActiveX отключены, то Вы не сможете загружать элементы ActiveX и пользоваться услугами Trend Micro Security. Убедитесь, что в Internet Explorer у Вас разрешены ActiveX.

Показаны снимки окон Internet Explorer 6. Последовательность действий может быть разной, в зависимости от версии обозревателя.

1. Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Security (Безопасность)**.
2. В окне **Internet Options (Свойства обозревателя)** нажмите кнопку **Custom Level (Другой)**.

Рис. 232 Свойства обозревателя — Безопасность



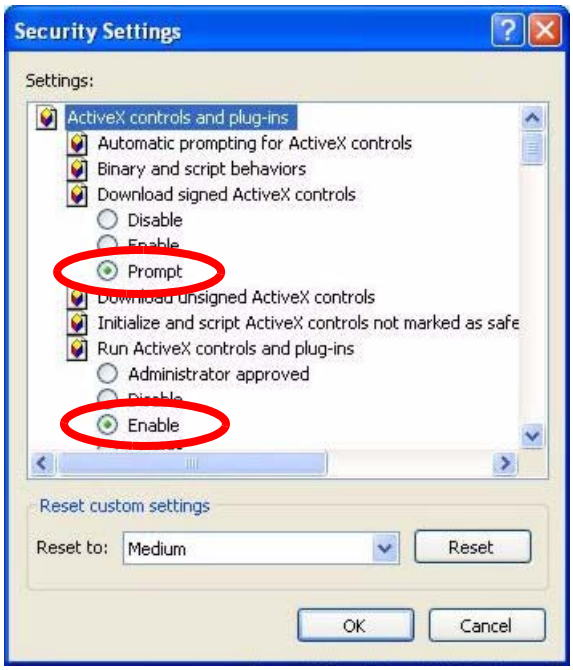
3 Спуститесь вниз к **ActiveX controls and plug-ins (Элементы ActiveX и модули подключения)**.

4 Под **Download signed ActiveX controls (Загрузка подписанных элементов ActiveX**) выберите **Prompt (Предлагать)**.

5 Под **Run ActiveX controls and plug-ins (Запуск элементов ActiveX и модулей подключения)** нужно выбрать **Enable (Разрешить)**.

6 Затем нажмите **OK**.

Рис. 233 Параметры безопасности — элементы ActiveX



Приложение A
Характеристики устройства

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

Таблицы характеристик

Табл. 122 Фильтры

IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Пароль по умолчанию	1234
Диапазон DHCP	от 192.168.1.32 до 192.168.1.64
Размеры (Ш x Г x В)	180 x 128 x 36 мм
Питание	12 В DC (постоянный ток), 1A
Встроенный коммутатор (P–660HT/ HTW EE)	Четыре порта Ethernet MDI/MDI-X 10/100 Мбит/с RJ-45 с автоматическим выбором скорости
Рабочая температура	0 ºC ~ 40 ºC
Температура хранения	-20 ºC ~ 60 ºC
Рабочая влажность	20 % ~ 85 %
Влажность при хранении	10 % ~ 90 %

Табл. 123 Firmware (Микропрограмма)

Стандарты ADSL	Поддержка многорежимного стандарта (ANSI T1.413,Issue 2; G.dmt(G.992.1); G.lite(G992.2)). ADSL2 G.dmt.bis (G.992.3). ADSL2 G.lite.bis (G.992.4). ADSL2+ (G.992.5). Расширенный ADSL (RE ADSL). 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. Прозрачная передача (Transparent bridging) для неподдерживаемых протоколов сетевого уровня. Сервер/Клиент/Ретранслятор DHCP. Протокол RIP I/RIP II (Routing Information Protocol — Протокол обмена информацией о маршрутизации). ICMP (Протокол межсетевых управляющих сообщений). ATM QoS (Качество услуг ATM). SNMP v1 и v2c с поддержкой MIB II (RFC 1213). Многоадресная рассылка IP IGMP v1 и v2. Proxy-сервер IGMP (Internet Group Management Protocol — Протокол управления группами сети Интернет). UPnP (Универсальная функция Plug and Play).
Управление	Встроенный Web-конфигуратор. Управление с помощью команд меню SMT (System Management Terminal — Системная консоль). CLI (Command Line Interpreter — Интерпретатор командной строки). Удаленное управление по протоколу Telnet или Web. Управление по протоколу SNMP. FTP/TFTP для загрузки микропрограммного обеспечения, архивирования и восстановления конфигурации. Системный журнал 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) (P–660HTW EE).

Табл. 123 Firmware (Микропрограмма) (продолжение)

Беспроводной доступ (P–660HTW EE).	Соответствует стандарту IEEE 802.11g. Диапазон частот: 2,4 ГГц. Расширенное ортогональное мультиплексирование с разделением частот (OFDM). Скорость передачи данных: 54 Мбит/с, автоматическое исправление ошибок. WEP-шифрование 64/128/256 бит. Мост WLAN–LAN. До 32 фильтров MAC-адресов. WPA(2), WPA(2)-PSK (Предварительно согласованный ключ). IEEE 802.1x. Возможность сохранения до 32 пользовательских профилей с помощью EAP-MD5 (встроенная база данных пользователей). Внешний сервер RADIUS, использующий EAP-MD5, TLS, TTLS.
Межсетевой экран	Комплексное обследование пакетов. Предотвращение внешних атак, вызывающих отказ системы, таких как "Ping of Death", "SYN Flood", "LAND", "Smurf" и т.д. Отправка уведомлений об атаках по электронной почте в режиме реального времени. Создание отчетов и журнальных записей.
NAT/SUA (Трансляция сетевых адресов/ Учетная запись одиночного пользователя)	Переадресация портов. Сеансы 1024 NAT. Мультимедийные приложения. PPTP под NAT/SUA. Транзитная пересылка IPSec. Транзитная пересылка SIP ALG. Транзитная пересылка VPN.
Фильтрация на основе содержания (контентная фильтрация)	Блокировка Web-сайтов по ключевому слову в URL.
Статическая маршрутизация.	16 IP и 4 моста.
Прочие функции	Any IP (Любой IP). Автоматическая настройка модема (автоматическое отслеживание виртуальных каналов). Перенаправление трафика. Динамическая система доменных имен (DYNDNS). Псевдоним IP. Политика маршрутизации IP (IPPR). MBM QoS (Качество обслуживания — управление пропускной способностью среды передачи).

Приложение B

Инструкции по настенному монтажу

Для установки интернет-центра P–660HT/HTW EE на стену проделайте следующее:

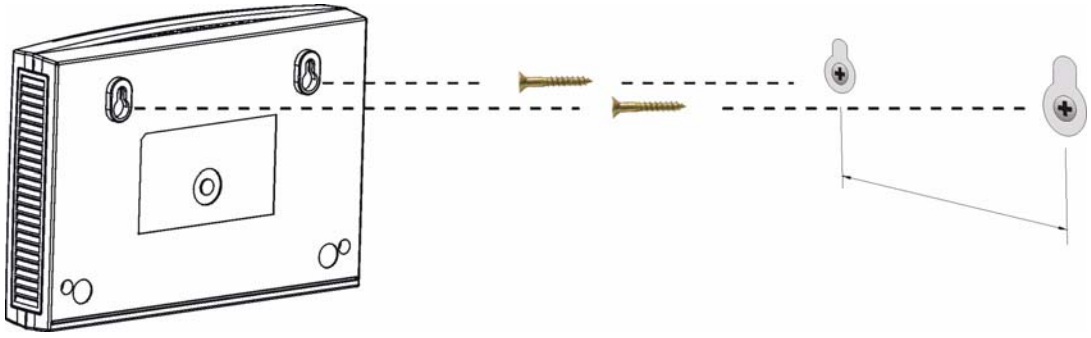
ПРИМЕЧАНИЕ: Посмотрите размер используемых саморезов и расстояние между центрами в Приложении "Технические характеристики изделия".

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".

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

3. Не вкручивайте саморезы полностью. Оставьте небольшой зазор (около 5 мм) между головками саморезов и стеной.
4. Убедитесь, что саморезы надежно закреплены в стене. Они должны выдерживать вес интернет-центра и соединительных проводов.
5. Совместите отверстия на задней панели интернет-центра с вкрученными в стену саморезами. Повесьте интернет-центр на саморезы.

Рис. 234 Пример настенного монтажа



Приложение C
Настройка IP-адреса компьютера

На все компьютеры должны быть установлены сетевые платы Ethernet 10 Мбит/с 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.

TCP/IP должен быть уже инсталлирован на компьютерах с системами Windows NT/ 2000/XP, Macintosh OS 7 или более поздними операционными системами.

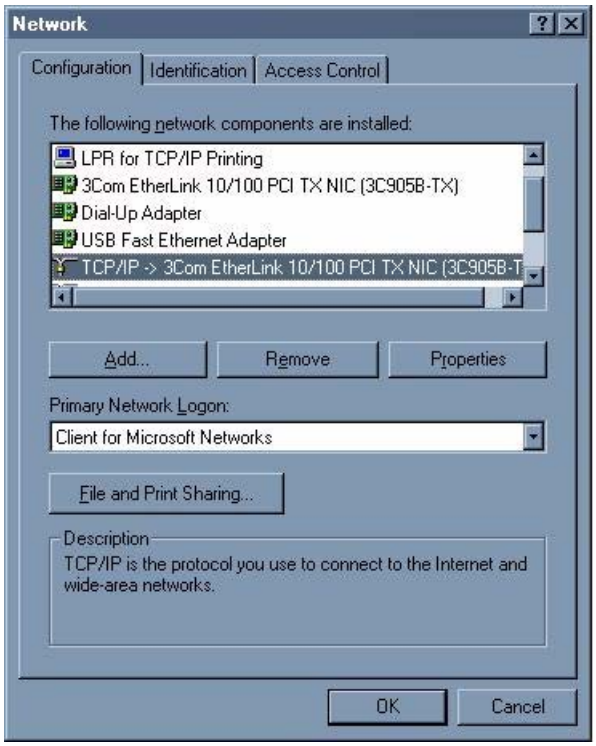
После соответствующей установки компонентов TCP/IP, настройте параметры TCP/IP для взаимодействия с вашей сетью.

Если параметры IP назначаются вручную вместо динамического назначения, убедитесь, что ваши компьютеры имеют IP-адреса, относящиеся к той же подсети, что и порт LAN интернет-центра.

Windows 95/98/Me

Нажмите **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)** и дважды щелкните на иконке **Network (Сеть)**, чтобы открыть окно **Network (Сеть)**.

Рис. 235 Windows 95/98/Me: Network (Сеть): Configuration (Конфигурация)



Установка компонентов

В окне **Network (Сеть)** на закладке **Configuration (Конфигурация)** отображается список установленных компонентов. Вам необходима сетевая плата, протокол TCP/IP и Client for Microsoft Networks (Клиент для сетей Microsoft).

Если необходимо установить сетевую плату:

1. В окне **Network (Сеть)** нажмите **Add (Добавить)**.
2. Выберите **Adapter (Сетевая плата)** и нажмите **Add (Добавить)**.
3. Выберите производителя и модель вашей сетевой платы и нажмите **OK**.

Если необходимо установить протокол TCP/IP:

1. В окне **Network (Сеть)** нажмите **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. Нажмите кнопку **Add (Добавить)**.

2 Выберите **Client (Клиент)** и нажмите **Add (Добавить)**.

3 Выберите **Microsoft** из списка производителей.

4 Выберите **Client for Microsoft Networks (Клиент для сетей Microsoft)** из списка сетевых клиентов и нажмите **OK**.

5 Перезагрузите компьютер, чтобы произведенные изменения вступили в силу.

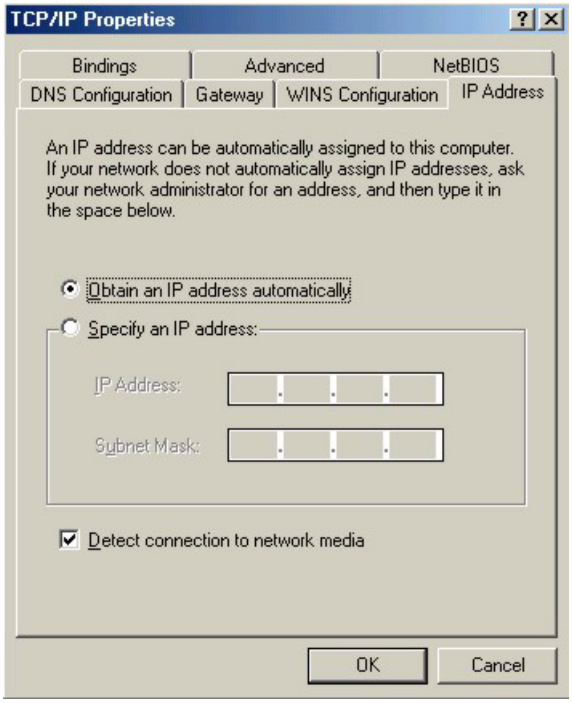
Настройка

1 В окне **Network (Сеть)** выберите закладку **Configuration (Конфигурация)**, выберите пункт TCP/IP для вашей сетевой платы и нажмите **Properties (Свойства)**

2 Выберите закладку **IP Address (IP-адрес)**.

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

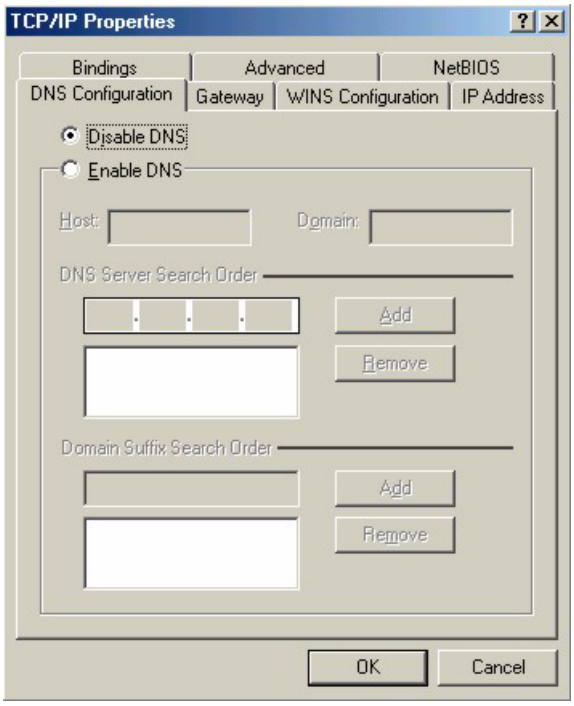
Рис. 236 Windows 95/98/Me: TCP/IP Properties (Свойства: TCP/IP): IP Address (IP-адрес)



3 Выберите закладку **DNS Configuration (Конфигурация DNS)**.

- Если вы не знаете параметры DNS, выберите **Disable DNS (Отключить DNS)**.
- Если вам известны параметры DNS, выберите **Enable DNS (Включить DNS)** и заполните поля, расположенные ниже (возможно, потребуется заполнять не все поля).

Рис. 237 Windows 95/98/Me: TCP/IP Properties (Свойства: TCP/IP): DNS Configuration (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 Нажмите **OK**, чтобы сохранить сделанные изменения и закрыть окно **TCP/IP Properties (Свойства: TCP/IP)**.

6 Нажмите кнопку **OK**, чтобы закрыть окно **Network (Сеть)**. При появлении запроса вставьте компакт-диск Windows.

7 Включите интернет-центр и перезагрузите компьютер при появлении запроса.

Проверка конфигурации

1 Нажмите **Start (Пуск)**, а затем **Run (Выполнить)**.

2 В окне **Run (Выполнить)** введите команду "winipcfg", а затем нажмите **OK** для отображения окна **IP Configuration (Конфигурация IP)**.

3 Выберите свою сетевую плату. При этом должны отображаться IP-адрес и маска подсети вашего компьютера, а также шлюз по умолчанию.

Windows 2000/NT/XP

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

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

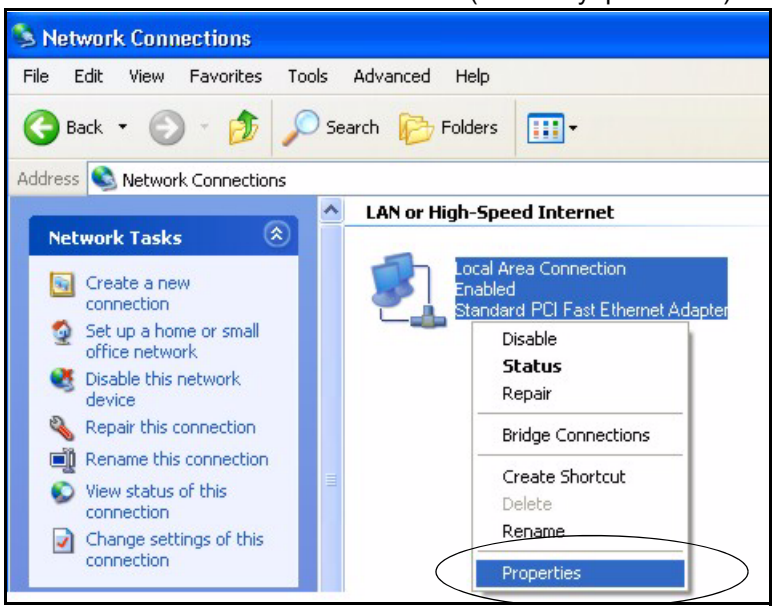
Рис. 238 Windows XP: Меню **start (пуск)**

2 На **Панели управления** дважды щелкните **Network Connections (Сетевые подключения)** (**Network and Dial-up Connections (Сеть и удаленный доступ к сети)** в Windows 2000/NT).

Рис. 239 Windows XP: Control Panel (Панель управления)

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

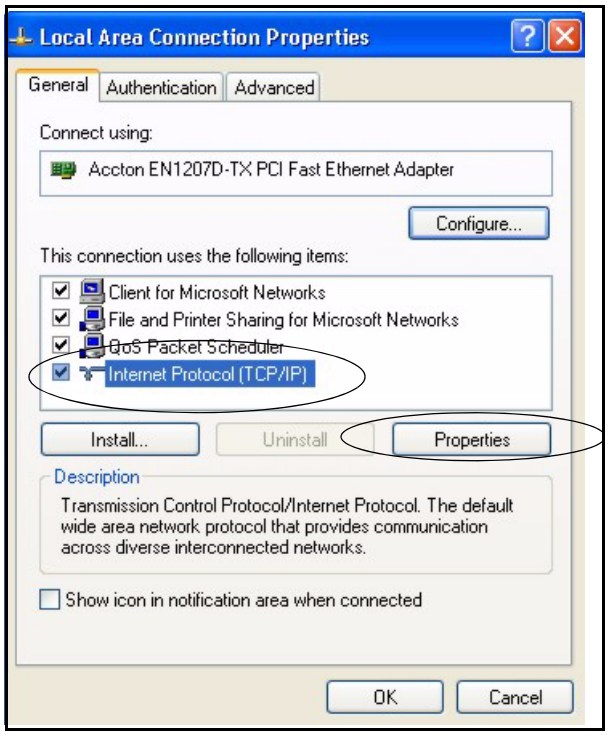
Рис. 240 Windows XP: Control Panel (Панель управления): Network Connections



(Сетевые подключения): Properties (Свойства)

4 На вкладке **General (Общие)** в WinXP выберите **Internet Protocol (TCP/IP) (Протокол Интернета (TCP/IP))** и нажмите **Properties (Свойства)**.

Рис. 241 Windows XP: Local Area Connection Properties (Подключение по локальной

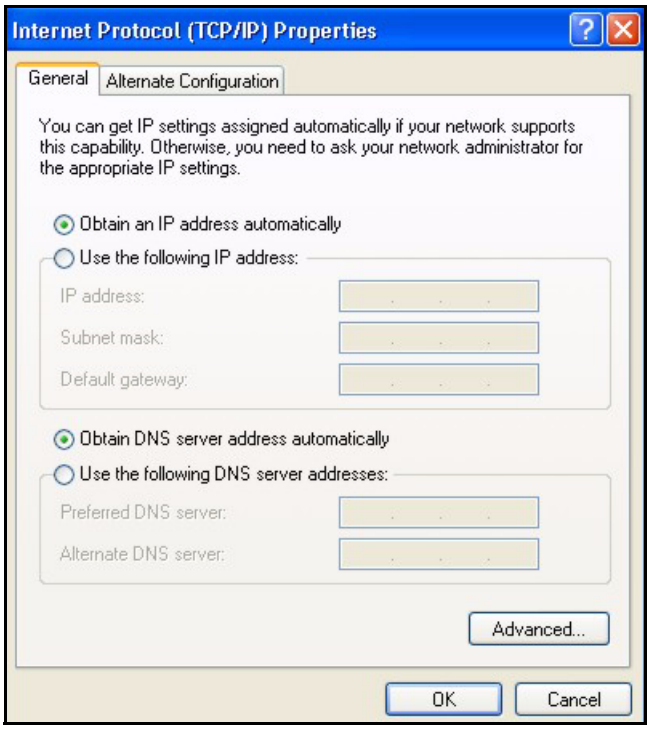


сети — свойства)

5 Появится 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)**.
- Нажмите **Advanced (Дополнительно)**.

Рис. 242 Windows XP: Internet Protocol TCP/IP Properties (Свойства: Протокол



Интернета (TCP/IP))

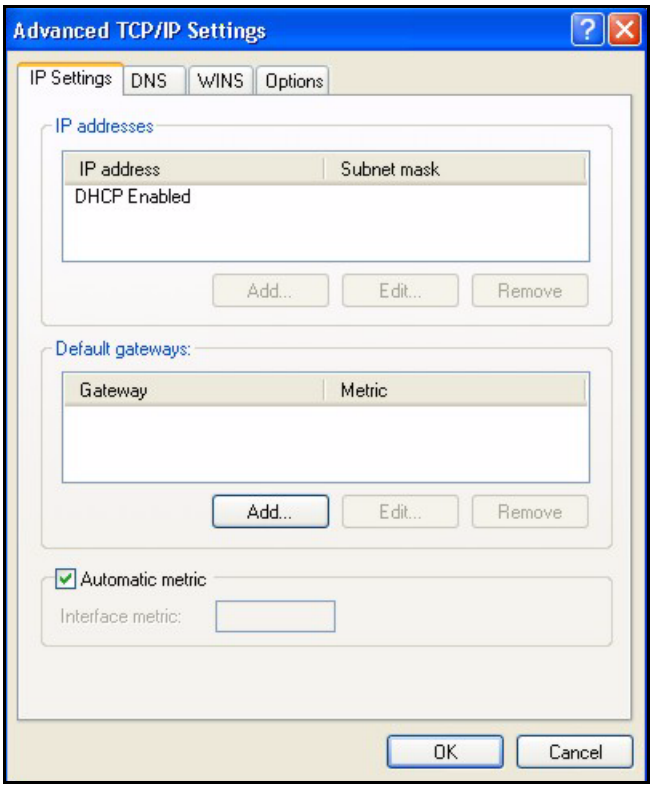
6 Если Вы не знаете IP-адрес шлюза, удалите все предварительно настроенные шлюзы на закладке **IP Settings (Параметры IP)** и нажмите **OK**.

Для настройки дополнительных IP-адресов выполните одно или более из следующих действий:

- На закладке **IP Settings (Параметры IP)** в поле для IP-адресов нажмите **Add (Добавить)**.
- В окошке **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 два предыдущих действия для каждого IP-адреса, который вы хотите добавить.
- Настройте дополнительные основные шлюзы 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)**.
- Нажмите кнопку **Add (Добавить)**.
- Повторите предыдущие три действия для всех шлюзов, которые необходимо добавить.
- Нажмите **OK** после завершения настройки.

Рис. 243 Windows XP: Advanced TCP/IP Properties (Дополнительные параметры TCP/IP)

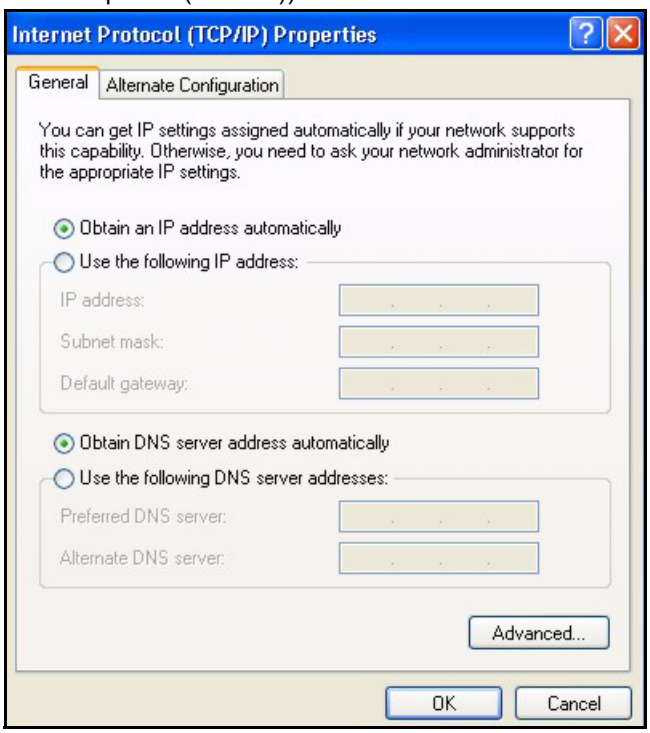


7 В окне **Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP))** на закладке **General (Общие)** в Windows XP:

- 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 DNS-серверов)**, и введите их в поля **Preferred DNS server (Предпочитаемый DNS-сервер)** и **Alternate DNS server (Альтернативный DNS-сервер)**.

  Если серверы DNS были настроены ранее, нажмите **Advanced (Дополнительно)** и затем закладку **DNS** для определения порядка их использования.

Рис. 244 Windows XP: Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP))



8 Нажмите **OK**, чтобы закрыть окно **Internet Protocol (TCP/IP) Properties (Свойства: Протокол Интернета (TCP/IP))**.

9 Нажмите **OK**, чтобы закрыть окно **Local Area Connection Properties (Подключение по локальной сети — свойства)**.

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

11 Включите интернет-центр и перезагрузите компьютер при появлении запроса.

Проверка конфигурации

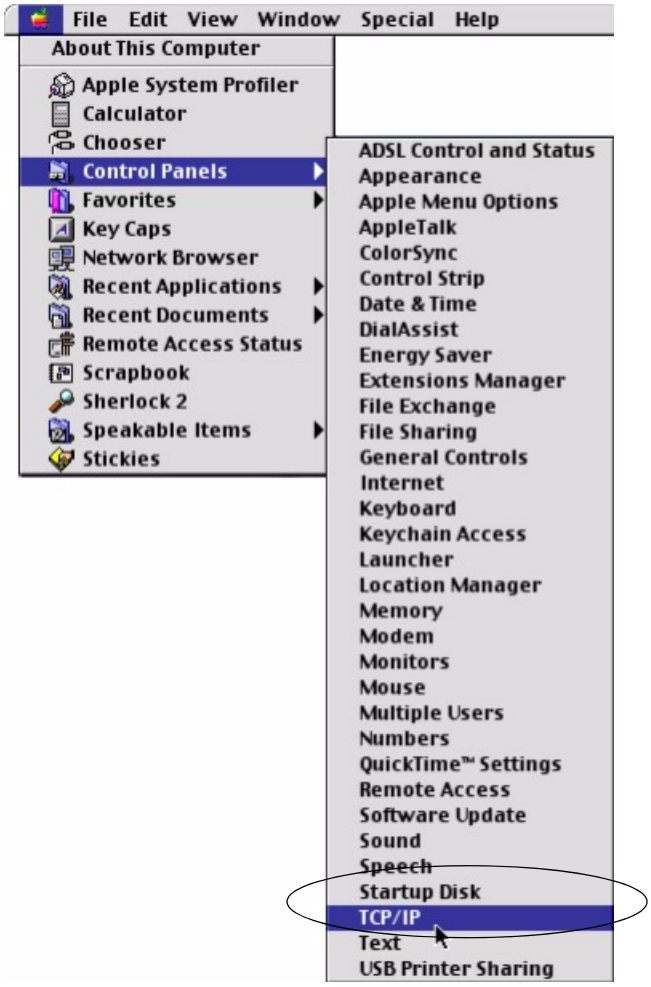
1 Нажмите **Start (Пуск)**, **All Programs (Все программы)**, **Accessories (Стандартные)**, **Command Prompt (Командная строка)**.

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 закладку **Support (Поддержка)**.

Macintosh OS 8/9

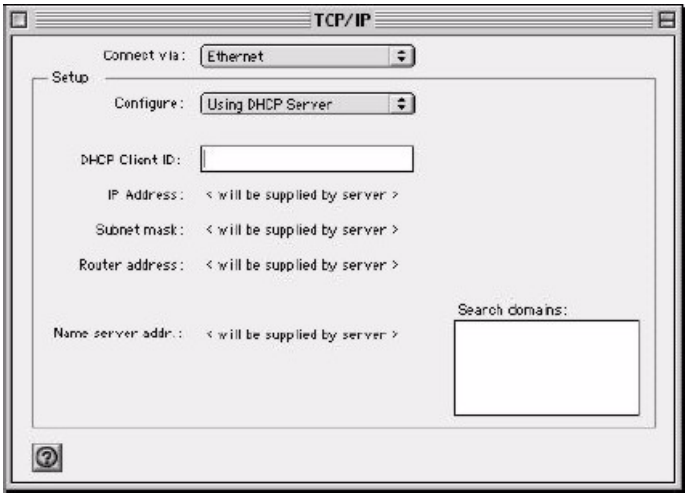
1 Нажмите кнопку меню **Apple**, выберите **Control Panel (Панель управления)**, а затем дважды щелкните **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.

Рис. 245 Macintosh OS 8/9: Меню Apple



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

Рис. 246 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 окне **IP Address (IP-адрес)**.
- Введите маску подсети в окне **Subnet mask (Маска подсети)**.
- Введите IP-адрес интернет-центра в поле **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 интернет-центр и перезагрузите компьютер при появлении запроса.

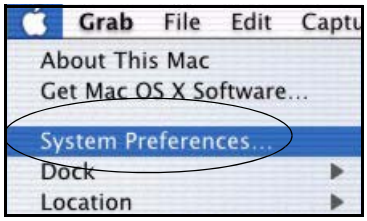
Проверка конфигурации

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. 247 Macintosh OS X: Меню Apple

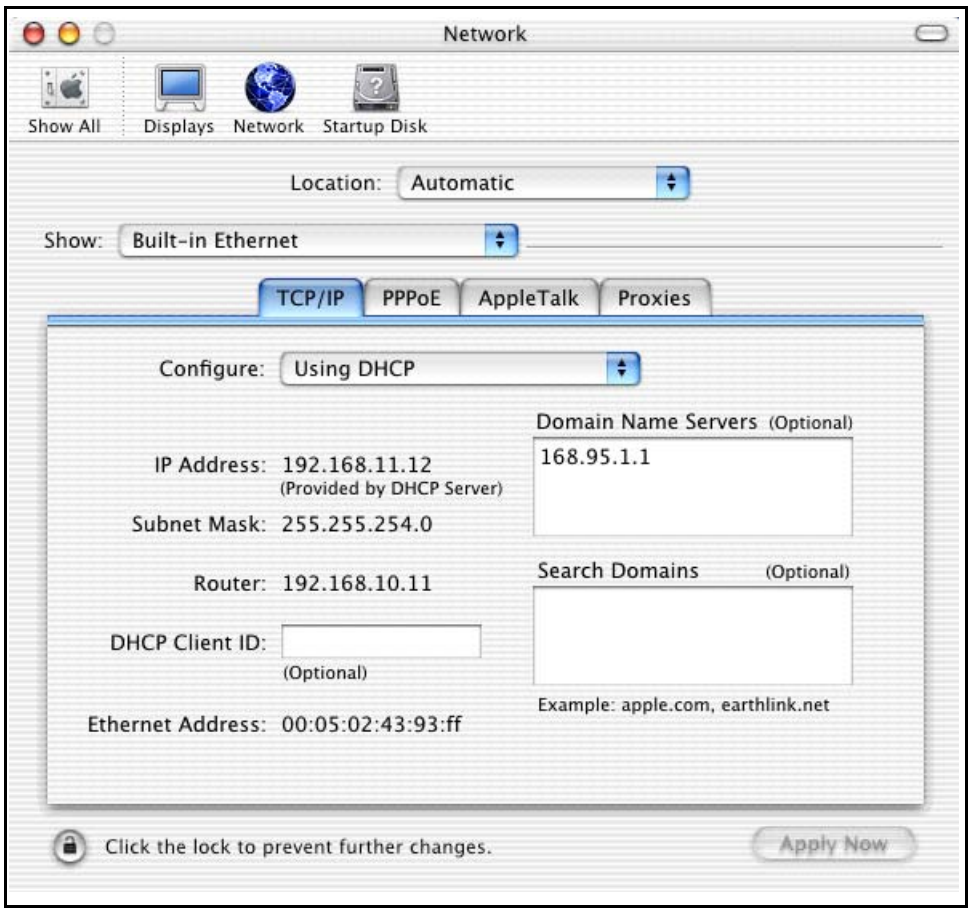


2 Нажмите **Network (Сеть)** на панели иконок.

- 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. 248 Macintosh OS X: Сеть



4 Для настройки статических параметров выполните следующие действия:

- В разделе **Configure (Настроить)**, выберите **Manually (Настроить вручную)**.
- Введите IP-адрес в окне **IP Address (IP-адрес)**.
- Введите маску подсети в окне **Subnet mask (Маска подсети)**.

- Введите IP-адрес интернет-центра в поле **Router address (Адрес маршрутизатора)**.

5 Нажмите **Apply Now (Применить)** и закройте окно.

6 Включите интернет-центр и перезагрузите компьютер при появлении запроса.

Проверка конфигурации

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.

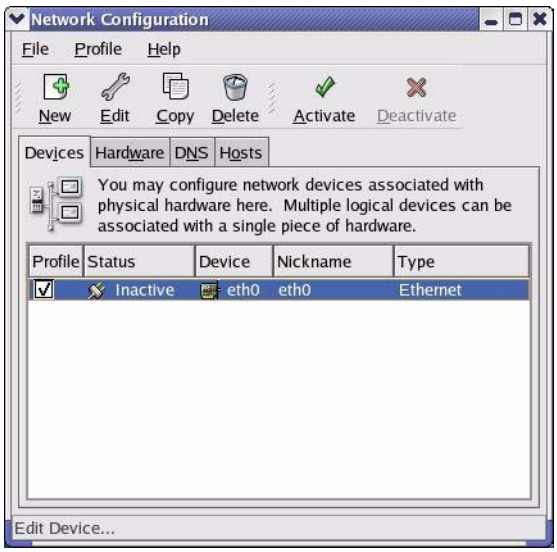
ПРИМЕЧАНИЕ: Вы должны быть зарегистрированы в системе в качестве корневого администратора.

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. 249 Red Hat 9.0: KDE: Network Configuration (Конфигурация сети): Devices (Устройства)



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

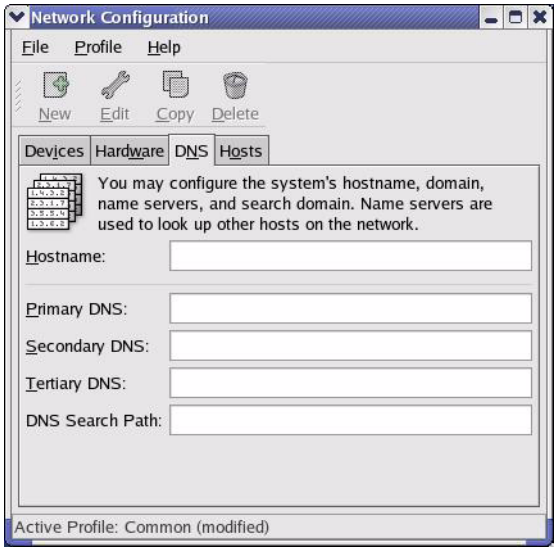
Рис. 250 Red Hat 9.0: KDE: Ethernet Device (Устройство Ethernet): General (общие)

- 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**.

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.

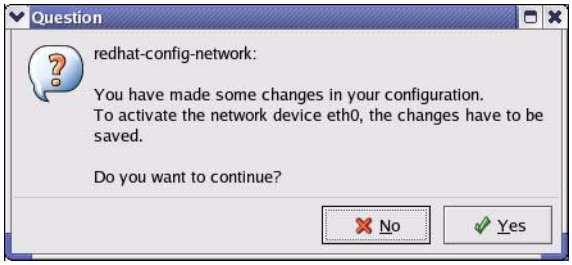
Рис. 251 Red Hat 9.0: KDE: Network Configuration (Конфигурация сети): DNS



5 Выберите закладку **Devices (Устройства)**.

6 Нажмите кнопку **Activate (Активировать)** для вступления изменений в силу. Появится следующее окно. Нажмите **Yes (Да)** для сохранения изменений во всех окнах.

Рис. 252 Red Hat 9.0: KDE: Network Configuration (Конфигурация сети): Activate (Активировать)



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=`". Далее приводится пример текстового вывода для этого процесса.

Рис. 253 Red Hat 9.0: Настройка динамического IP-адреса (Dynamic IP Address Setting) 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. 254 Red Hat 9.0: Настройка статического IP-адреса (Dynamic IP Address Setting) 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. 255 Red Hat 9.0: Настройки 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`". Далее приводится пример текстового вывода для этого процесса.

Рис. 256 Red Hat 9.0: Restart Ethernet Card (Перезагрузить карту 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 конфигурации

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

Рис. 257 Red Hat 9.0: Checking TCP/IP Properties (Проверка свойств 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]#
```

Приложение D
Организация подсетей IP

Адресация IP

Маршрутизаторы выбирают “маршрут” на основе номера сети. При доставке пакета данных соответствующему получателю маршрутизатор использует идентификатор узла.

Классы IP

IP-адрес состоит их четырех байтов (8 бит каждый), записанных в десятичном формате с разделительными точками, например: 192.168.1.1. IP-адреса подразделяются на различные классы. Класс адреса зависит от значения первого байта.

- Адреса класса “A” имеют значение 0 в самом левом бите. В адресах класса “A” первый байт является номером сети, а остальные три байта составляют идентификатор узла.
- Адреса класса “B” имеют 1 в самом левом бите и 0 в следующем. В адресах класса “B” первые два байта являются номером сети, а остальные два байта составляют идентификатор узла.
- Адреса класса “C” начинаются (слева направо) с последовательности 1 1 0. В адресах класса “C” первые три байта составляют номер сети, а последний байт является идентификатором узла.
- Адреса класса “D” начинаются с последовательности 1 1 1 0. Адреса класса “D” используются для многоадресных рассылок. (Еще существуют адреса класса “E”. Они зарезервированы для будущего использования.)

Табл. 124 Классы IP-адресов

IP-АДРЕС:		БАЙТ 1	БАЙТ 2	БАЙТ 3	БАЙТ 4
Класс A	0	Номер сети	Идентификатор узла	Идентификатор узла	Идентификатор узла
Класс B	10	Номер сети	Номер сети	Идентификатор узла	Идентификатор узла
Класс C	110	Номер сети	Номер сети	Номер сети	Идентификатор узла

ПРИМЕЧАНИЕ: Идентификатор узла не может содержать только нули или только единицы.

Поэтому:

В сети класса “C” (8 бит для узлов) может быть 2^8 –2, т. е. 254 узла.

В сети класса “B” (16 бит для узлов) может быть 2^{16}–2, т. е. 65534 узла.

В сети класса “A” (24 бита для узлов) может быть 2^{24}–2 узлов (примерно 16 миллионов узлов).

Поскольку первый байт IP-адреса класса “A” должен начинаться с “0”, первый байт адреса класса “A” может принимать значения от 0 до 127.

Аналогично, первый байт адреса класса “B” должен начинаться с “10”, поэтому первый байт адреса класса “B” может принимать значения от 128 до 191. Первый байт адреса класса “C” начинается с “110”, и поэтому имеет диапазон значений от 192 до 223.

Табл. 125 Допустимые диапазоны IP-адресов для каждого класса

КЛАСС	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО БАЙТА (В ДВОИЧНОЙ ЗАПИСИ)	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО БАЙТА (В ДЕСЯТИЧНОЙ ЗАПИСИ)
Класс A	от **00000000** до **01111111**	от 0 до 127
Класс B	от **10000000** до **10111111**	от 128 до 191
Класс C	от **11000000** до **11011111**	от 192 до 223
Класс D	от **11100000** до **11101111**	от 224 до 239

Маска подсети

С помощью маски подсети можно определить, какие биты являются частью номера сети, а какие — частью идентификатора узла (используя операцию логического "И"). 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.

Маски подсети записываются в десятичном формате с разделительными точками, так же, как и IP-адреса. “Естественные” маски для классов IP-адресов A, B и C приведены ниже.

Табл. 126 “Естественные” маски

КЛАСС	ЕСТЕСТВЕННАЯ МАСКА
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Организация подсетей

При организации подсетей распределение IP-адресов по классам игнорируется. Например, адрес класса C не обязательно должен иметь номер сети из 24 бит и идентификатор узла из 8 бит. При организации подсетей некоторые биты идентификатора узла можно использовать в качестве битов номера сети. По договоренности маска подсети всегда состоит из непрерывной последовательности единиц в начале маски (слева), за которой следует непрерывная последовательность нулей, и имеет общую длину 32 бита.

Поскольку маска всегда состоит из непрерывной последовательности единиц в начале и непрерывной последовательности нулей в оставшихся битах и имеет длину 32 бита, можно просто указывать количество единиц вместо того, чтобы записывать значение каждого байта. Это обычно обозначается посредством записи после адреса символа “/” и количества бит с единицами.

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

В следующей таблице приведены все возможные маски подсети для адресов класса “C”, записанные в двух вариантах.

Табл. 127 Альтернативные варианты записи маски подсети

МАСКА ПОДСЕТИ	МАСКА ПОДСЕТИ ПРИ ЗАПИСИ КОЛИЧЕСТВА ЕДИНИЦ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

Первая маска — это естественная маска класса “C”. Обычно, если маска подсети не указана, то считается, что используется естественная маска.

Пример: две подсети

В качестве примера рассмотрим адрес класса “C” 192.168.1.0 с маской подсети 255.255.255.0.

Табл. 128 Пример организации 2-х подсетей

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ИДЕНТИФИКАТОР УЗЛА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	00000000
Маска подсети	255.255.255.	0
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	00000000

Первые три байта адреса образуют номер сети (класс “C”). Необходимо иметь две отдельные сети.

Разделите сеть 192.168.1.0 на две отдельных подсети, преобразовав один бит идентификатора узла в IP-адресе в бит номера сети. “Заимствованный” бит идентификатора узла может принимать значение “0” или “1”, что позволяет организовать две подсети: 192.168.1.0 с маской подсети 255.255.255.128 и 192.168.1.128 с маской подсети 255.255.255.128.

ПРИМЕЧАНИЕ: В следующих таблицах затененные/выделенные жирным шрифтом значения битов последнего байта обозначают биты идентификатора узла, "заимствованные" для образования дополнительных битов номера сети. Количество “заимствованных” битов идентификатора узла определяет число подсетей, которые Вы можете создать. Оставшееся (после “заимствования”) количество битов идентификатора узла определяет максимально возможное количество узлов в каждой подсети.

Табл. 129 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**0**0000000
Маска подсети	255.255.255.	128
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**1**0000000
Адрес подсети: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Широковещательный адрес: 192.168.1.127	Highest Host ID: 192.168.1.126	

Табл. 130 Подсеть 2

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	128
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**1**0000000
Маска подсети	255.255.255.	128
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**1**0000000
Адрес подсети: 192.168.1.128	Младший идентификатор узла: 192.168.1.129	
Широковещательный адрес: 192.168.1.255	Старший идентификатор узла: 192.168.1.254	

Оставшиеся 7 бит определяют максимально возможное количество узлов в каждой подсети. Идентификаторы узлов, состоящие только из нулей, представляют собственно подсеть, а идентификаторы узлов, состоящие только из единиц, являются адресами широковещательной рассылки для каждой подсети, поэтому реальное количество доступных узлов для каждой подсети для данного примера равно $2^7 – 2$, т.е. 126 узлов в каждой подсети.

192.168.1.0 с маской 255.255.255.128 это сама сеть, а 192.168.1.127 с маской 255.255.255.128 является адресом направленной широковещательной рассылки первой подсети. Следовательно, самый младший IP-адрес, который может быть назначен действительному узлу для первой подсети — 192.168.1.1, а старший — 192.168.1.126. Аналогично диапазон адресов для узлов второй подсети — от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В примере выше демонстрируется использование 25-битной маски подсети для разделения адресного пространства класса “C” на две подсети. Аналогично для разделения адреса класса “C” на четыре подсети, потребуется “позаимствовать” два бита от 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 бит для идентификатора узла, при этом получается 2^6-2 или 62 узла в каждой подсети (все 0 обозначают саму подсеть, все 1 являются широковещательным адресом этой подсети).

Табл. 131 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**00**000000

Табл. 131 Подсеть 1 (продолжение)

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.0	Младший идентификатор узла: 192.168.1.1	
Широковещательный адрес: 192.168.1.63	Старший идентификатор узла: 192.168.1.62	

Табл. 132 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	Младший идентификатор узла: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Старший идентификатор узла: 192.168.1.126	

Табл. 133 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	Младший идентификатор узла: 192.168.1.129	
Широковещательный адрес: 192.168.1.191	Старший идентификатор узла: 192.168.1.190	

Табл. 134 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

Табл. 134 Подсеть 4 (продолжение)

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
Адрес подсети: 192.168.1.192	Младший идентификатор узла: 192.168.1.193	
Широковещательный адрес: 192.168.1.255	Старший идентификатор узла: 192.168.1.254	

Пример: восемь подсетей

Аналогично используется 27-битная маска для создания 8-ми подсетей (001, 010, 011, 100, 101, 110).

В следующей таблице приведены значения битов последнего байта адреса класса C для каждой подсети.

Табл. 135 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

В следующей таблице приведены сводные данные по организации подсетей класса “C”.

Табл. 136 Организация подсетей класса C

КОЛИЧЕСТВО “ЗАИМСТВОВАННЫХ” БИТОВ 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

Организация подсетей в сетях класса A и класса B.

Для адресов класса “A” и класса “B” маска подсети также определяет, какие биты являются частью номера сети, а какие — частью идентификатора узла.

Адрес класса “B” имеет два байта идентификаторов узлов для организации подсетей, а адрес класса “A” — три байта идентификаторов узлов (см. Табл. 124 на с. 426) для организации подсетей.

В следующей таблице приведены сводные данные по организации подсетей класса “B”.

Табл. 137 Организация подсетей класса B

КОЛИЧЕСТВО “ЗАИМСТВОВАННЫХ” БИТОВ 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

Приложение E
Команды начальной загрузки

AT-команды модуля начальной загрузки выполняются из загрузочного ПО маршрутизатора при переходе в режим отладки до запуска микропрограммного обеспечения маршрутизатора. По желанию, при запуске интернет-центра можно перейти в режим отладки, нажав соответствующую клавишу при появлении сообщения в следующей экранной форме. В режиме отладки появляется доступ к серии команд модуля начальной загрузки, например ATUR (для загрузки микропрограммного обеспечения) или ATLC (для загрузки файла конфигурации). Об этих командах было рассказано в главе **Сопровождение микропрограммного обеспечения и файла конфигурации**.

Рис. 258 Функция входа в режим отладки

```
Bootbase Version: V1.02 | 08/08/2001 15:40:50
RAM: Size = 16384 Kbytes
DRAM Post: Testing: 16384K OK
FLASH: Intel 16M
RAS Version: V3.50(WB.0)b3 | 08/08/2001 16:21:27
Press any key to enter debug mode within 3
seconds.
.................................................
```

Введите ATHE для просмотра всех команд модуля начальной загрузки интернет-центра (показаны в следующей экранной форме). Команда ATBAx позволяет изменять скорость консольного порта. "x" означает порядковый номер перед двоеточием, которому соответствует значение скорости консольного порта (указано после двоеточия); например, ATBA3 устанавливает скорость консольного порта 9.6 Кбит/с. Команда ATSE выводит шаблон, который используется для создания пароля на включение флажка отладки в микропрограмме. Команда ATSH выдает данные об устройстве, такие как версия модуля начальной загрузки, имя поставщика, модель изделия, код RAS (Сервис Удаленного Доступа) и т.д. ATGO позволяет продолжить загрузку системы. Большинство остальных команд используются для детального поиска/устранения неисправностей и должны использоваться только компетентными специалистами.

Рис. 259 Команды модуля начальной загрузки

```
AT             just answer OK
ATHE           print help
ATBAx         change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k
5:115.2k
ATENx,(y)      set BootExtension Debug Flag (y=password)
ATSE           show the seed of password generator
ATTI(h,m,s)    change system time to hour:min:sec or show
current time
ATDA(y,m,d)    change system date to year/month/day or show
current date
ATDS           dump RAS stack
ATDT           dump Boot Module Common Area
ATDUx,y        dump memory contents from address x for length y
ATRBx          display the 8-bit value of address x
ATRWx          display the 16-bit value of address x
ATRLx          display the 32-bit value of address x
ATGO(x)        run program at addr x or boot router
ATGR           boot router
ATGT           run Hardware Test Program
ATRTw,x,y(,z) RAM test level w, from address x to y (z
iterations)
ATSH           dump manufacturer related data in ROM
ATDOx,y        download from address x for length y to PC via
XMODEM
ATTD           download router configuration to PC via XMODEM
ATUR           upload router firmware to flash ROM
ATLC           upload router configuration file to flash ROM
ATXSx          xmodem select: x=0: CRC mode(default); x=1:
checksum mode
ATSR           system reboot
```

Приложение F
Интерпретатор команд

Ниже приводятся инструкции по работе с интерпретатором команд. В **главном меню** введите "24" для перехода в меню обслуживания системы. Затем введите "8" для перехода в **Меню 24.8 — Режим интерпретатора команд**. Более подробная информация по этим командам находится на компакт-диске, входящем в комплект поставки, а также на web-сайте www.zyxel.ru.

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

Синтаксис команд

- Ключевые слова команд выделены шрифтом `courier new`.
- Ключевые слова команды необходимо вводить в точности так, как показано, без использования 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. Команды необходимо набирать полностью. После завершения работы введите `exit` для возврата в **Главное меню SMT**.

Приложение G
Команды управления межсетевым экраном

Ниже дается описание команд управления межсетевым экраном.

Табл. 138 Команды управления межсетевым экраном

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
Firewall (Настройка межсетевого экрана)	`config edit firewall active <yes | no>`	Включить/выключить межсетевой экран.
	`config retrieve firewall`	Вернуться к ранее сохраненным настройкам межсетевого экрана.
	`config save firewall`	Сохранить текущие настройки межсетевого экрана.
Display (Отобразить)	`config display firewall`	Показать настройки межсетевого экрана: электронная почта, атаки, наборы правил.
	`config display firewall set <set #>`	Показать текущую конфигурацию набора правил, о том числе время ожидания, имя, разрешение по умолчанию и т.д. Если после слова “set” не указано число (#), то будет выведена информация обо всех наборах правил.
	`config display firewall set <set #> rule <rule #>`	Показать текущие данные по одному из правил в наборе.
	`config display firewall attack`	Показать настройки ответов на атаки.
	`config display firewall e-mail`	Показать настройки электронной почты.
	`config display firewall?`	Показать все имеющиеся подкоманды межсетевого экрана.
Edit (Редактировать)		
E-mail (Электронная почта)	`config edit firewall e-mail mail-server <ip address of mail server>`	Указать IP-адрес, на который отсылаются электронные сообщения.
	`config edit firewall e-mail return-addr <e-mail address>`	Указать адрес электронной почты, с которого будут отсылаться сообщения межсетевого экрана.
	`config edit firewall e-mail email-to <e-mail address>`	Указать адрес электронной почты, на который будут отсылаться сообщения межсетевого экрана.
	`config edit firewall e-mail policy <full | hourly | daily | weekly>`	Указать частоту рассылки журнала сообщений межсетевого экрана по электронной почте.
	`config edit firewall e-mail day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>`	Указать день недели, в который журнал сообщений межсетевого экрана будет отсылаться по электронной почте, если интернет-центр настроен на еженедельную рассылку сообщений.

Табл. 138 Команды управления межсетевым экраном (продолжение)

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
E-mail (Электронная почта)	`config edit firewall e-mail hour <0-23>`	Указать час для рассылки по электронной почте журнала сообщений межсетевого экрана, если интернет-центр настроен на еженедельную, ежедневную рассылку или на рассылку по часам.
	`config edit firewall e-mail minute <0-59>`	Указать минуту для рассылки по электронной почте журнала сообщений межсетевого экрана, если интернет-центр настроен на еженедельную, ежедневную рассылку сообщений или на рассылку по часам.
Attack (Атака)	`config edit firewall attack send-alert <yes | no>`	Включить или отключить немедленное уведомление об атаках DOS по e-mail.
	`config edit firewall attack block <yes | no>`	Установить yes (да) для блокирования нового трафика после превышения порога tcp-max-incomplete. Установить no (нет) для удаления самых старых полуоткрытых сессий в случае, если трафик превышает допустимый порог tcp-max-incomplete.
	`config edit firewall attack block-minute <0-255>`	Установить время в минутах, по истечении которого блокируются новые сессии при превышении допустимого порога tcp-max-incomplete. Данная команда действительна только если в поле block (блокировать) установлено yes (да).
	`config edit firewall attack minute-high <0-255>`	Установить максимально допустимое количество новых полуоткрытых сессий в минуту, при котором интернет-центр начинает удалять старые до достижения минимального значения (minute-low).
	`config edit firewall attack minute-low <0-255>`	Установить допустимое количество полуоткрытых сессий, при котором интернет-центр прекращает удаление полуоткрытых сессий.
	`config edit firewall attack max-incomplete-high <0-255>`	Установить допустимое количество разрешенных полуоткрытых сессий, при котором интернет-центр начинает удалять старые до достижения минимального значения (max-incomplete-low).
	`config edit firewall attack max-incomplete-low <0-255>`	Установить порог, при котором интернет-центр прекращает удаление полуоткрытых сессий.
	`config edit firewall attack tcp-max-incomplete <0-255>`	Установить допустимое количество полуоткрытых TCP-сессий с одинаковым адресом назначения, при котором интернет-центр начинает удаление полуоткрытых сессий с данным адресом.

Табл. 138 Команды управления межсетевым экраном (продолжение)

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
Sets (Наборы)	`config edit firewall set <set #> name <desired name>`	Указать идентификационное имя конкретного набора.
	`Config edit firewall set <set #> default-permit <forward | block>`	Сбрасывать или разрешать пакет, не удовлетворяющий правилам в наборе.
	`Config edit firewall set <set #> icmp-timeout <seconds>`	Установить время ожидания ответа ICMP во время сессии ICMP.
	`Config edit firewall set <set #> udp-idle-timeout <seconds>`	Установить время, в течение которого UDP-соединение может быть неактивным, прежде чем интернет-центр его закроет.
	`Config edit firewall set <set #> connection-timeout <seconds>`	Время ожидания установления сессии TCP до сброса.
	`Config edit firewall set <set #> fin-wait-timeout <seconds>`	Время, в течение которого соединение TCP остается открытым после получения межсетевым экраном ответа FIN (означающего конец сеанса TCP).
	`Config edit firewall set <set #> tcp-idle-timeout <seconds>`	Время, в течение которого неактивное соединение TCP остается открытым.
	`Config edit firewall set <set #> log <yes | no>`	Создавать или не создавать записи в журнале для пакетов, удовлетворяющих заданному по умолчанию набору правил.
Правила	`Config edit firewall set <set #> rule <rule #> permit <forward | block>`	Сбрасывать или разрешать пакеты, соответствующие данному правилу.
	`Config edit firewall set <set #> rule <rule #> active <yes | no>`	Включить или отключить данное правило.
	`Config edit firewall set <set #> rule <rule #> protocol <integer protocol value >`	Указать номер спецификации протокола в данном правиле для ICMP.
	`Config edit firewall set <set #> rule <rule #> log <none | match | not-match | both>`	Регистрировать или не регистрировать трафик, удовлетворяющий указанному правилу, не удовлетворяющий или частично удовлетворяющий указанному правилу.
	`Config edit firewall set <set #> rule <rule #> alert <yes | no>`	Посылать или не посылать по электронной почте уведомление при распознавании атаки DOS или при нарушении указанного правила.
	`config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>`	Проверять трафик с определенным адресом источника на совпадение с указанным правилом.
	`config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>`	Проверять трафик с определенным адресом подсети источника (определяется на основании IP-адреса и маски подсети) на совпадение с указанным правилом.

Табл. 138 Команды управления межсетевым экраном (продолжение)

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
Правила	`config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>`	Проверять трафик с адресом источника из данного диапазона на совпадение с указанным правилом.
	`config edit firewall set <set #> rule <rule #> destaddr-single <ip address>`	Проверять трафик с определенным адресом назначения на совпадение с указанным правилом.
	`config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask>`	Проверять трафик с определенным адресом подсети назначения (определяется на основании IP-адреса и маски подсети) на совпадение с указанным правилом.
	`config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address>`	Проверять трафик с адресом назначения из данного диапазона на совпадение с указанным правилом.
	`config edit firewall set <set #> rule <rule #> TCP destport-single <port #>`	Проверять TCP-трафик с данным адресом назначения на совпадение с указанным правилом. Эту команду можно повторить с различными (неповторяющимися) номерами портов.
	`config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #>`	Проверять TCP-трафик с портом назначения из данного диапазона на совпадение с указанным правилом.
	`config edit firewall set <set #> rule <rule #> UDP destport-single <port #>`	Проверять UDP-трафик с данным адресом назначения на совпадение с указанным правилом. Эту команду можно повторить с различными (неповторяющимися) номерами портов.
	`config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #>`	Проверять UDP-трафик с портом назначения из данного диапазона на совпадение с указанным правилом.
Удалить	`config delete firewall e-mail`	Удалить все настройки предупреждений, отсылаемых по электронной почте.
	`config delete firewall attack`	Вернуться к настройкам ответов на атаки по умолчанию.
	`config delete firewall set <set #>`	Удалить указанный набор из конфигурации межсетевого экрана.
	`config delete firewall set <set #> rule<rule #>`	Удалить указанное правило из конфигурации межсетевого экрана.

Приложение H
Команды фильтра NetBIOS

Ниже приводится описание команд пакетного фильтра NetBIOS.

Введение

Пакеты NetBIOS (Network Basic Input/Output System — Сетевая базовая система ввода-вывода) — 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 инициируют нежелательные вызовы.

Вы можете настроить фильтры NetBIOS, чтобы:

- Разрешить/запретить отправку пакетов NetBIOS из локальной сети (LAN) в глобальную (WAN) и наоборот.
- Разрешить/запретить отправку пакетов NetBIOS из локальной сети (LAN) в DMZ и наоборот.
- Разрешить/запретить отправку пакетов NetBIOS из глобальной сети (WAN) в DMZ и наоборот.
- Разрешить/запретить отправку пакетов NetBIOS через VPN-подключения.
- Разрешить/запретить отправку пакетов NetBIOS для инициирования звонков.

Вывод настроек фильтра NetBIOS

Синтаксис: `sys filter netbios disp`

Эта команда выводит доступный только для чтения список текущих параметров фильтров NetBIOS интернет-центра.

Пример команды вывода на экран настроек фильтра NetBIOS

```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
        Between LAN and DMZ: Block
        Between WAN and DMZ: Block
        IPSec Packets: Forward
        Trigger Dial: Disabled
```

Ниже перечислены типы фильтров и их установки по умолчанию.

Табл. 139 Настройки фильтров NetBIOS по умолчанию

ИМЯ	ОПИСАНИЕ	ПРИМЕР
Between LAN and WAN (из LAN в WAN)	Это поле показывает, будут ли пересылаться или блокироваться пакеты NetBIOS, исходящие из локальной сети в глобальную.	Block (Блокировать)
Between LAN and DMZ (из LAN в DMZ)	Это поле показывает, будут ли пересылаться или блокироваться пакеты NetBIOS, исходящие из локальной сети в DMZ.	Block (Блокировать)
Between WAN and DMZ (из WAN в DMZ)	Это поле показывает, будут ли пересылаться или блокироваться пакеты NetBIOS, исходящие из глобальной сети в DMZ.	Block (Блокировать)
IPSec Packets (Пакеты IPSec)	Это поле показывает, будут ли пересылаться или блокироваться пакеты NetBIOS по VPN-соединениям.	Forward (Пересылать)
Trigger dial (Инициировать вызов)	Это поле показывает, разрешено ли пакетам NetBIOS инициировать вызовы. Disabled (Отключено) означает, что пакеты NetBIOS не могут инициировать вызовы.	Disabled (Отключено)

Настройка фильтров NetBIOS

```
Синтаксис:sys filter netbios config <type> <on|off>
```

где

`<type>` = Указывает номер фильтра NetBIOS (от 0 до 3), который необходимо настроить.

0 = из LAN в WAN

1 = из LAN в DMZ

2 = из WAN в DMZ

3 = проход пакета IPSec

4 = инициирование вызова

`<on|off>` = Чтобы включить фильтр и блокировать пакеты NetBIOS, следует установить параметр "on" для фильтров 0 и 1. Установка параметра "off" отключает фильтр и разрешает пересылку пакетов NetBIOS.

Чтобы блокировать пересылку пакетов по соединениям VPN, следует установить параметр "on" для фильтра 3. Установка параметра "off" разрешает пересылку пакетов NetBIOS по соединениям VPN.

Чтобы разрешить пакетам NetBIOS инициировать вызовы, следует установить параметр "on" для фильтра 4. Установка параметра "off" не позволяет пакетам NetBIOS инициировать вызовы.

Примеры команд:

`sys filter netbios config 0 on`	Эта команда блокирует пакеты NetBIOS "LAN–WAN" и "WAN–LAN".
`sys filter netbios config 1 off`	Эта команда пересылает пакеты NetBIOS "LAN–DMZ" и "DMZ–LAN".
`sys filter netbios config 3 on`	Эта команда блокирует пакеты IPSec NetBIOS.
`sys filter netbios config 4 off`	Эта команда запрещает командам NetBIOS инициировать вызовы.

Приложение I
Сплиттеры и микрофильтры

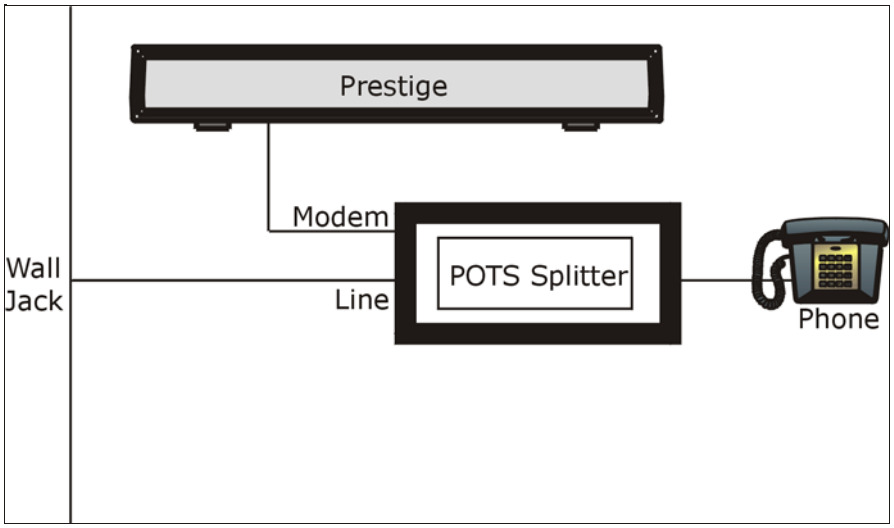
В этом приложении описывается установка сплиттера для подключения телефонного аппарата и телефонного микрофильтра.

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. 260 Подключение телефонного сплиттера



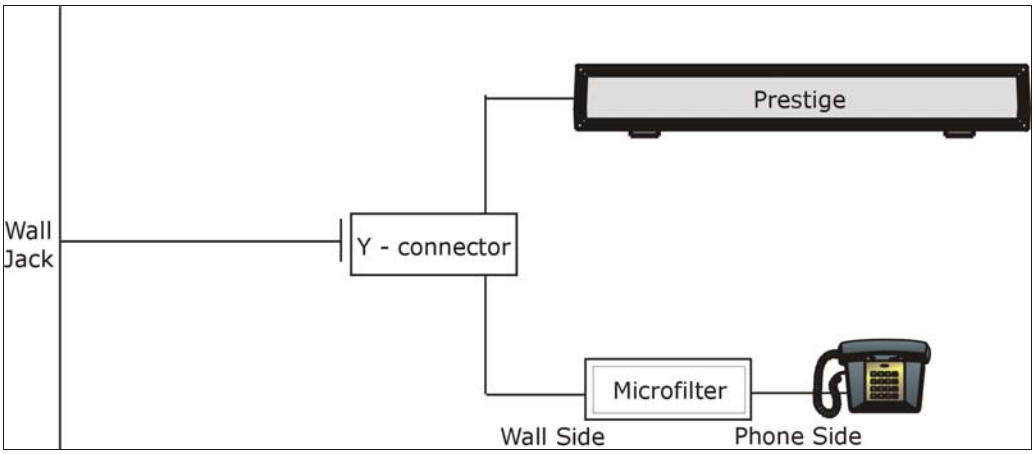
1. Подключите разъем с маркировкой "Phone" к телефону.
2. Подключите разъем с маркировкой "Modem" к интернет-центру.
3. Подключите разъем с маркировкой "Line" к настенной телефонной розетке.

Телефонные микрофильтры

Передача речи по телефонной линии осуществляется в нижнем диапазоне частот от 0 до 4 кГц, а сигналы ADSL передаются в более высоком диапазоне частот, выше 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. Подключите телефонный кабель от настенной розетки к Y-образному разъему со стороны с одним выводом.
2. Подключите один кабель от Y-образного разъема со стороны с двумя выводами к разъему "LINE" микрофильтра.
3. Подключите другой кабель от Y-образного разъема со стороны с двумя выводами к интернет-центру.
4. Подключите разъем "PHONE" микрофильтра к телефону, как показано на следующем рисунке.

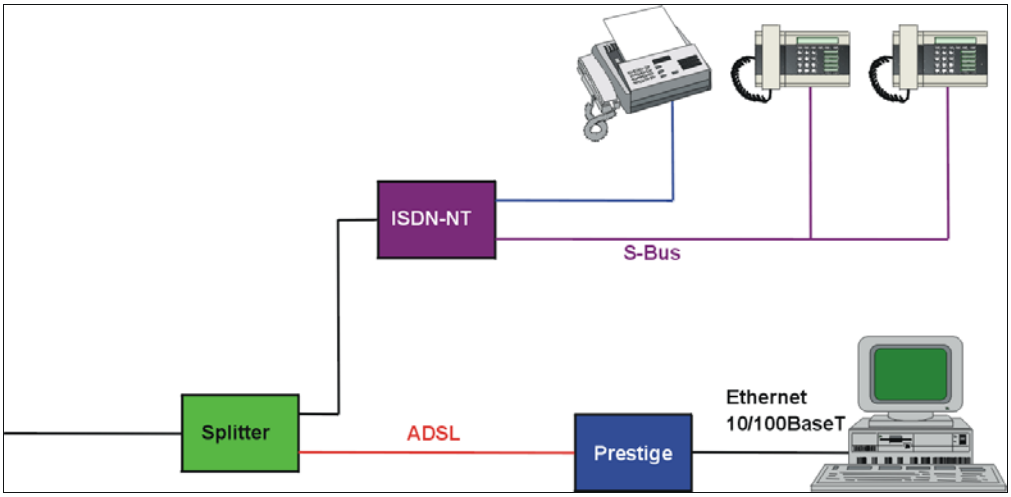
Рис. 261 Подключение микрофильтра



Использование интернет-центра с ISDN

Этот раздел предназначен только для тех, кто использует интернет-центр с ADSL в сети ISDN (Integrated Services Digital Network — Цифровая сеть с предоставлением комплексных услуг). Далее приводится пример установки интернет-центра для использования в сети ISDN.

Рис. 262 Использование интернет-центра с ISDN



Приложение J PPPoE (Протокол "точка-точка" поверх Ethernet)

PPPoE в действии

Модем ADSL создает мост для сеанса связи PPP по Ethernet (PPP поверх Ethernet, RFC 2516) от вашего компьютера до постоянного виртуального канала ATM (Permanent Virtual Circuit — PVC), который подключается к концентратору доступа ADSL, где сеанс связи PPP завершается (см. Рис. 263 на с. 451). Один постоянный виртуальный канал (PVC) может поддерживать любое количество сеансов PPP из локальной сети. Протокол PPPoE обеспечивает функции учета и управления доступом аналогично услуге доступа по коммутируемой линии с использованием протокола PPP.

Преимущества PPPoE

PPPoE обладает следующими преимуществами:

Имеет пользовательский интерфейс, знакомый по доступу в сеть по коммутируемой линии (Dial-Up Networking — DUN).

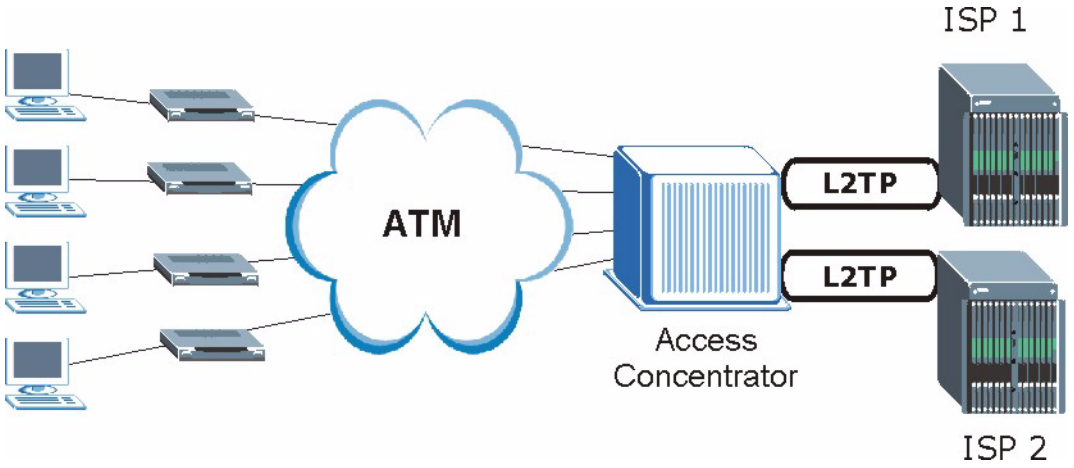
Уменьшает затраты операторов связи по обеспечению виртуальных каналов к многочисленным коммутаторам для тысяч пользователей на всем пути до Интернет-провайдера. Для GSTN (PSTN и ISDN) инфраструктура коммутации уже существует.

Позволяет Интернет-провайдеру использовать существующую модель доступа по коммутируемой линии для аутентификации и предоставлять (дополнительно) дифференцированные услуги.

Традиционный сценарий доступа по коммутируемой линии

На следующей схеме представлена типичная конфигурация оборудования, при которой компьютеры используют традиционный доступ в сеть по коммутируемой линии.

Рис. 263 Конфигурация оборудования "один маршрутизатор для одного компьютера"



Как работает PPPoE

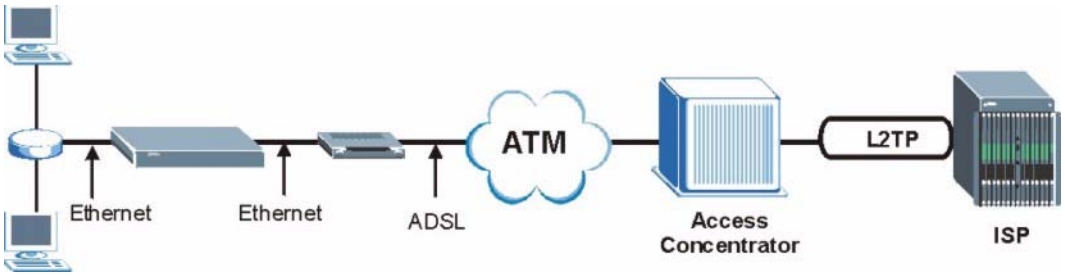
Драйвер PPPoE представляет Ethernet как последовательный канал связи с компьютером, по которому компьютер использует протокол PPP, в то время как модем передает по образованному мосту кадры Ethernet к DSL-коммутатору, который также называют концентратором доступа (Access Concentrator). DSL-коммутатор и Интернет-провайдер взаимодействуют следующим образом: DSL-коммутатор выступает в качестве L2TP (Layer 2 Tunneling Protocol — Протокол туннелирования 2 уровня) LAC (L2TP Access Concentrator — концентратор доступа L2TP) и туннеллирует PPP кадры к Интернет-провайдеру. L2TP туннель поддерживает одновременное сквозное пропускание нескольких сеансов PPP.

При использовании PPPoE виртуальный канал (VC — Virtual Circuit) является аналогом коммутируемого соединения и проходит между модемом и DSL-коммутатором на всем пути к Интернет-провайдеру. Однако сеанс PPP устанавливается между компьютером и Интернет-провайдером.

Интернет-центр в качестве клиента PPPoE

При использовании интернет-центра в качестве клиента PPPoE, компьютеры локальной сети видят только Ethernet и не знают о PPPoE. Это облегчает работу администратора, избавляя его от необходимости настройки клиентов PPPoE на отдельных компьютерах.

Рис. 264 Интернет-центр в качестве клиента PPPoE



Приложение K
Беспроводные локальные сети

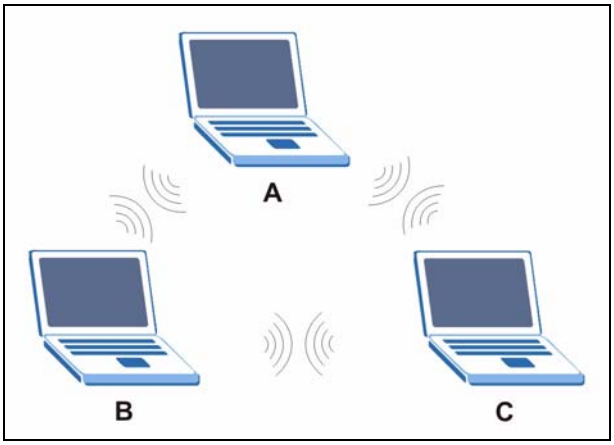
Топологии беспроводных локальных сетей

В этом разделе описаны временные (Ad-hoc) и фиксированные топологические схемы беспроводных локальных сетей.

Конфигурация временной (Ad-hoc) беспроводной локальной сети

Простейшей конфигурацией беспроводной локальной вычислительной сети (WLAN) является независимая (временная) WLAN, объединяющая группу компьютеров с беспроводными устройствами (A, B, C). Когда два или более беспроводных адаптеров попадают в зону действия друг друга, они могут образовать независимую сеть, обычно называемую "временной сетью" (Ad-hoc network) или "независимым базовым набором служб" (Independent Basic Service Set, IBSS). На приведенной диаграмме показан пример, где несколько ноутбуков используют беспроводные адаптеры для образования временной (Ad-hoc) беспроводной локальной сети.

Рис. 265 Одноранговая связь во временной (Ad-hoc) беспроводной сети

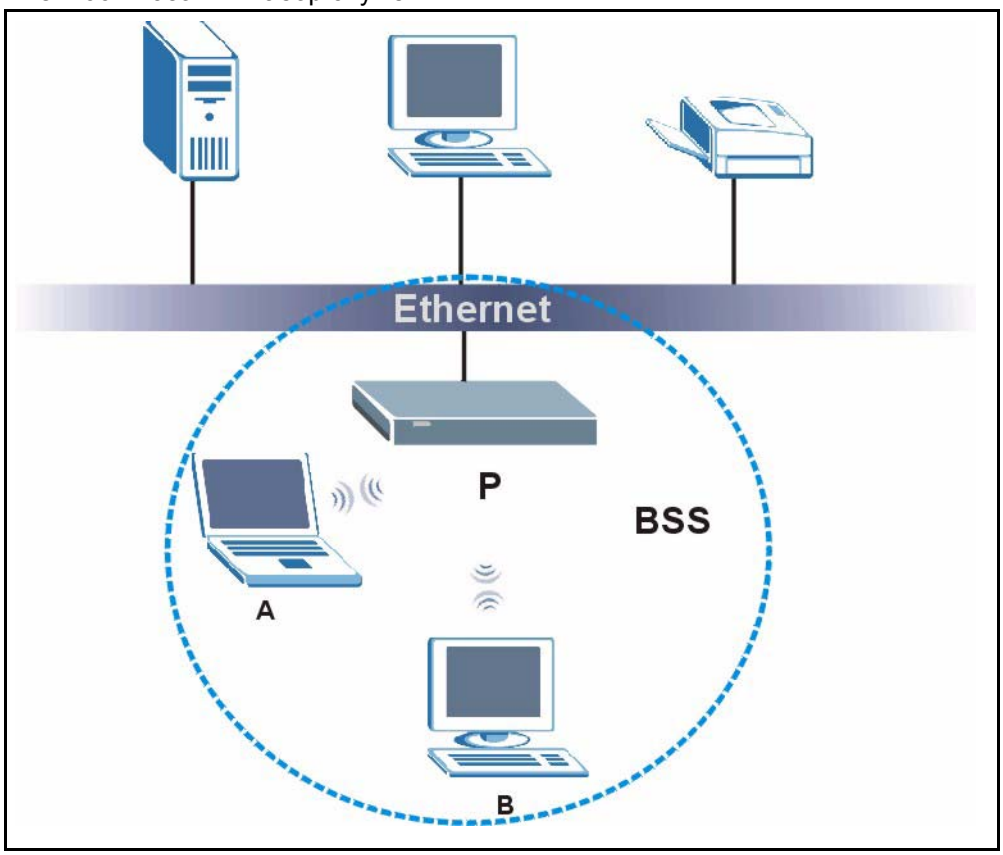


BSS (Базовый набор служб)

Базовый набор служб (BSS) существует тогда, когда весь трафик между беспроводными устройствами или между беспроводным устройством и клиентом проводной сети идет через одну точку доступа (AP).

Intra-BSS трафик — это трафик между беспроводными устройствами в пределах одного базового набора служб. При активации Intra-BSS трафика беспроводные устройства A и B могут получить доступ к проводной сети и обмениваться информацией между собой. При отключении Intra-BSS трафика беспроводные устройства A и B все равно могут получить доступ к проводной сети, однако не могут обмениваться информацией между собой.

Рис. 266 Базовый набор служб



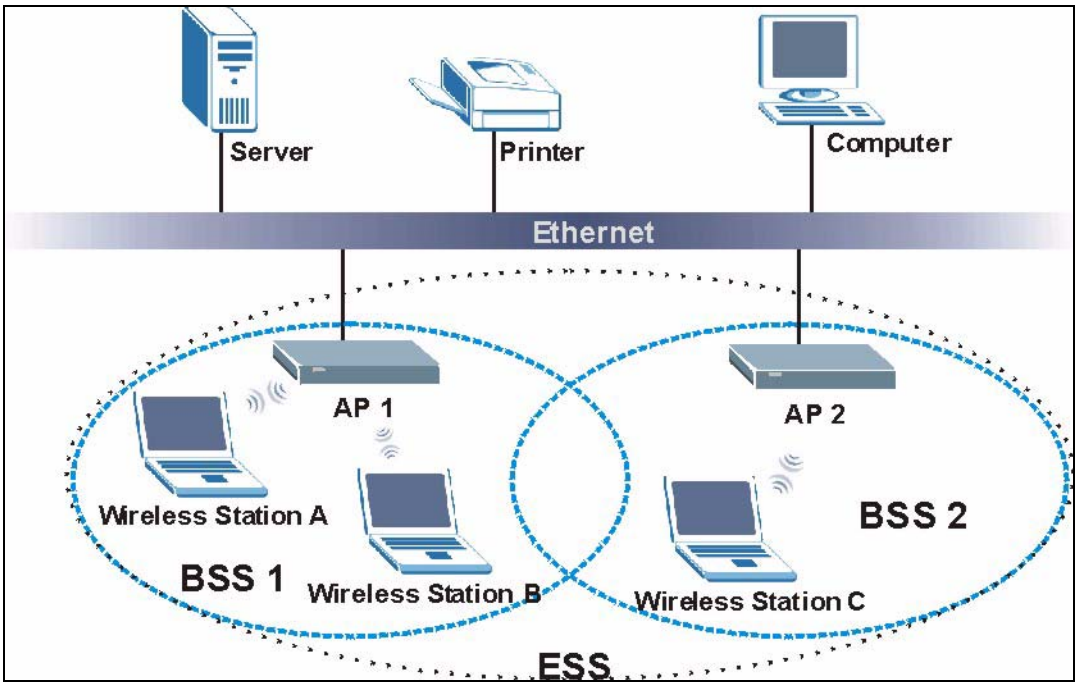
ESS

Расширенный набор служб (ESS) состоит из нескольких перекрывающихся базовых наборов служб (BSS), каждый из которых имеет точку доступа, а точки доступа связаны проводной сетью. Это проводное соединение точек доступа называется системой распределения (Distribution System, DS).

Этот тип беспроводной топологической организации локальной сети называется фиксированной беспроводной локальной сетью (Infrastructure WLAN). Точки доступа не только обеспечивают связь с проводной сетью, но и служат связующим звеном для трафика беспроводной локальной сети в непосредственном окружении.

Каждый ESS идентифицируется уникальным идентификатором (ESSID). Все точки доступа и связанные с ними беспроводные устройства в одном ESS должны иметь одинаковый идентификатор ESS.

Рис. 267 Фиксированная беспроводная сеть



Канал

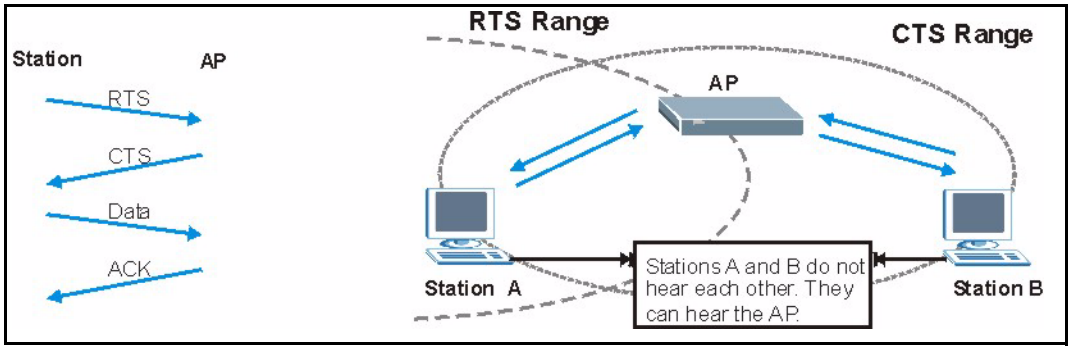
Канал представляет собой радиочастоту(ы), используемую(ые) беспроводными устройствами IEEE 802.11b/g. Доступность каналов зависит от географического положения. В некоторых регионах каналов может быть несколько, поэтому для снижения уровня помех следует использовать канал, отличающийся от канала ближайшей точки доступа. Помехи появляются при перекрывании радиосигналов от разных точек доступа, при этом ухудшается качество сигнала.

Однако смежные каналы частично перекрываются. Во избежание помех из-за перекрывания, канал точки доступа (AP) должен отстоять по крайней мере на пять каналов от частот, которые используют смежные точки доступа. Например, если в регионе действуют 11 каналов и смежная точка доступа использует канал 1, то Вам необходимо выбрать канал 6 или 11.

RTS/CTS (Запрос на передачу/Подтверждение готовности к приему)

"Скрытый" узел — это ситуация, когда два устройства находятся в рабочей зоне одной и той же точки доступа, но вне рабочих зон друг друга. Следующий рисунок иллюстрирует ситуацию “скрытого“ узла. Оба устройства (STA) находятся в рабочей зоне точки доступа (AP) или беспроводного шлюза, но вне рабочих зон друг друга, поэтому они не могут "слышать" друг друга, т. е. они не знают, используется ли в данный момент канал. Поэтому они считаются скрытыми друг от друга.

Рис. 268 RTS/CTS



Когда устройство A посылает данные в точку доступа, она может не знать, что устройство B уже использует канал. Если эти два устройства послали данные одновременно, может произойти конфликт, при котором обе партии данных достигают AP одновременно, результатом чего является потеря сообщений от обоих устройств.

RTS/CTS предназначен для предотвращения конфликтов из-за невидимых узлов. **RTS/CTS** определяет максимальный размер кадра данных, который можно отправить без квитирования (отправки запроса на передачу (RTS) и последующего получения подтверждения готовности к приему (CTS)).

Если кадр данных превышает значение **RTS/CTS**, установленное в диапазоне от 0 до 2432 байт, устройство, которое хочет передать этот кадр, должно вначале послать сообщение RTS (Request To Send/Запрос на передачу) точке доступа (AP) для получения разрешения на пересылку. Затем AP отвечает сообщением CTS (Clear to Send/ Готовность к приему) всем другим устройствам в рабочей зоне, извещая их о необходимости задержки передачи данных. Для устройства, отправлявщего запрос, это сообщение одновременно подтверждает временные рамки, отведенные на передачу данных.

Кадры, меньше указанных в **RTS/CTS**, устройства могут посылать непосредственно в AP, без запроса на передачу.

Настройка **RTS/CTS** необходима только в случае, если существует вероятность наличия "скрытых“ узлов в сети, а расходы на повторную отправку больших фрагментов оказывается больше, чем дополнительные сетевые издержки в связи с запросом разрешения на сеанс связи RTS/CTS.

Если значение **RTS/CTS** превышает значение **Порога фрагментации** (см. далее), квитирование RTS/CTS не будет иметь места, так как кадры данных будут фрагментированы до того как достигнут размера **RTS/CTS**.

ПРИМЕЧАНИЕ: Включение порога RTS влечет за собой лишние сетевые издержки, которые зачастую негативно сказываются на пропускной способности, а не меняют ситауцию к лучшему.

Порог фрагментации

Порог фрагментации — это максимальный размер фрагмента данных (в диапазоне от 256 до 2432 байт), который может быть послан в беспроводную сеть и при превышении которого точка доступа разделит пакет на меньшие кадры данных.

Большой **порог фрагментации** рекомендован для сетей, не склонных к помехам, тогда как для загруженных или склонных к помехам сетей необходимо установить меньший порог.

Если значение **порога фрагментации** меньше установленного значения **RTS/CTS** (см. ранее), квитирование RTS/CTS не будет иметь места, так как кадры данных будут фрагментированы до того как достигнут размера **RTS/CTS**.

Тип заголовка (Preamble Type)

Заголовок (вводная часть) используется для синхронизации времени передачи в беспроводной сети. Существует два режима заголовков: **Длинный (Long)** и **Короткий (Short)**.

Короткий заголовок требует меньше времени на обработку и минимизирует издержки, поэтому его следует использовать в хорошей беспроводной сети, если он поддерживается всеми беспроводными устройствами.

Режим **Long (Длинный заголовок)** следует выбрать в случае, если в сети высок уровень "шума" либо нет уверености относительно того, какой режим заголовков поддерживают используемые беспроводные устройства (все беспроводные адаптеры стандарта IEEE 802.11b должны поддерживать длинные заголовки). Однако не все беспроводные адаптеры поддерживают короткие заголовки. Используйте длинный заголовок, если Вы не уверены, какой режим заголовков поддерживают беспроводные адаптеры. В этом случае будет гарантировано взаимопонимание между точкой доступа и беспроводными устройствами, и связь в сетях с высоким уровнем "шума" станет более надежной.

Выберите **Dynamic**, чтобы точка доступа автоматически использовала короткий заголовок, если он поддерживается всеми беспроводными устройствами, и длинный заголовок в остальных случаях.

ПРИМЕЧАНИЕ: Точка доступа и беспроводные устройства *ДОЛЖНЫ* использовать один и тот же режим заголовков.

Беспроводные локальные сети стандарта IEEE 802.11g

Стандарт IEEE 802.11g полностью совместим со стандартом IEEE 802.11b. Это означает, что адаптер IEEE 802.11b может непосредственно связываться с точкой доступа IEEE 802.11g (и наоборот) на скорости 11 Мбит/с или ниже, в зависимости от режима. IEEE 802.11g имеет несколько промежуточных вариантов скорости передачи между максимальной и минимальной скоростью передачи данных. Скорость передачи данных IEEE 802.11g и режим модуляции выглядят следующим образом:

Табл. 140 IEEE 802.11g

СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ (МБИТ/С)	МОДУЛЯЦИЯ
1	DBPSK (Differential Binary Phase Shift Keyed/Кодирование дифференциальным двоичным сдвигом фазы)
2	DQPSK (Differential Quadrature Phase Shift Keying/Кодирование дифференциальным квадратурным сдвигом фазы)
5.5 / 11	CCK (Complementary Code Keying/Кодирование дополнительным кодом)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing/Ортогональное мультиплексирование с разделением частот)

IEEE 802.1x

В июне 2001 года был создан стандарт IEEE 802.1x, расширивший возможности стандарта IEEE 802.11, а именно поддерживающий расширенную аутентификацию и имеющий дополнительные функции учета и контроля. Он поддерживается Windows XP и рядом сетевых устройств. Вот некоторые из преимуществ IEEE 802.1x:

- Идентификация на уровне пользователей, обеспечивающая возможность роуминга.
- Поддержка системы RADIUS (Аутентификация удаленных пользователей по коммутируемым каналам связи, RFC 2138, 2139) для централизованного управления пользовательскими профилями и учетом на сетевом сервере RADIUS.
- Поддержка EAP (Расширяемого протокола аутентификации, RFC 2486), позволяющая использовать дополнительные методы аутентификации, не меняя настроек точки доступа и беспроводных устройств.

RADIUS

Система RADIUS основывается на модели "клиент-сервер", поддерживающей аутентификацию, авторизацию и учет. Клиент — это точка доступа, а сервер — это сервер RADIUS. Сервер RADIUS выполняет следующие задачи:

- Аутентификация

  Устанавливает подлинность пользователей.

- Авторизация

  Определяет сетевые службы, доступные для аутентифицированных пользователей после подключения к сети.

- Учет

  Отслеживает активность сети клиента.

RADIUS использует простой обмен пакетами, в котором точка доступа выступает в качестве ретранслятора сообщений между беспроводным устройством и сетевым сервером RADIUS.

Типы сообщений RADIUS

Следующие типы сообщений RADIUS пересылаются между точкой доступа и сервером RADIUS в целях аутентификации пользователей:

- Access-Request (Доступ-Запрос)

  Посылается точкой доступа при запросе аутентификации.

- Access-Reject (Доступ-Отказ)

  Посылается сервером RADIUS при отказе в доступе.

- Access-Accept (Доступ-Разрешение)

  Посылается сервером RADIUS при разрешении доступа.

- Access-Challenge (Доступ-Приглашение)

  Посылается сервером RADIUS при запросе дополнительной информации для получения доступа. Точка доступа получает от пользователя надлежащий ответ, а затем посылает еще одно сообщение Access-Request.

Следующие типы сообщений RADIUS пересылаются между точкой доступа и сервером RADIUS в целях учета пользователей:

- Accounting-Request (Учет-Запрос)

  Посылается точкой доступа при запросе учета.

- Accounting-Response (Учет-Ответ)

  Посылается сервером RADIUS и указывает, что учет начался или закончился.

Для обеспечения сетевой безопасности точка доступа и сервер RADIUS используют общий секретный ключ, который является паролем, известным им обоим. Этот ключ не передается по сети. Помимо общего секретного ключа, обмен информацией о пароле также кодируется для защиты сети от несанкционированного доступа.

Методы аутентификации

В этом приложении описаны некоторые популярные методы аутентификации: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** и **LEAP**.

Непосредственно используемый тип аутентификации зависит от сервера RADIUS и точки доступа. Подробную информацию можно получить у сетевого администратора.

EAP-MD5 (Алгоритм представления сообщения в краткой форме 5)

Аутентификация по методу MD5 — это простейший способ односторонней аутентификации. Сервер аутентификации отправляет беспроводному устройству запрос. Беспроводное устройство подтверждает знание пароля, для чего оно шифрует его и отправляет серверу в качестве ответа на запрос. Пароль не отправляется в виде обычного текста.

Однако метод MD5 имеет слабые стороны. Дело в том, что поскольку серверу аутентификации пароль нужен в виде обычного текста, его необходимо где-то сохранять. Следовательно, доступ к файлу с паролями может получить не только сервер аутентификации. Кроме того, сервер аутентификации можно сымитировать, т. е. выдать себя за него (поскольку метод MD5 не выполняет двусторонней аутентификации). И, наконец, метод MD5 не поддерживает шифрование данных с помощью динамического сеансового ключа. Чтобы зашифровать данные, необходимо настроить ключи шифрования WEP.

EAP-TLS (Безопасность на транспортном уровне)

При использовании метода EAP-TLS серверу и беспроводным устройствам для двусторонней аутентификации необходимы цифровые удостоверения. Сервер предоставляет клиентскому устройству свое удостоверение. После идентификации сервера клиентское устройство отправляет серверу свое удостоверение. До создания защищенного туннеля обмен удостоверениями производится в открытую. Это делает пользователя уязвимым для пассивных атак. Цифровое удостоверение — это электронная ID-карта, идентифицирующая отправителя. Однако для использования метода EAP-TLS необходимо иметь дело с Бюро сертификации (CA), которое занимается обработкой удостоверений, что повлечет за собой административные издержки.

EAP-TTLS (Защита туннелированного транспортного уровня)

Метод EAP-TTLS представляет собой расширенную версию метода EAP-TLS. Для установления безопасного соединения удостоверения используются для аутентификации только со стороны сервера. Аутентификация клиента производится путем отправки имени пользователя и пароля через безопасное соединение, таким образом обеспечивается защита клиента. Метод EAP-TTLS поддерживает методы аутентификации клиента EAP и традиционные методы аутентификации, такие как PAP, CHAP, MS-CHAP и MS-CHAP v2.

PEAP (Защищенный EAP)

Как и в методе EAP-TTLS, для создания безопасного соединения здесь используется аутентификация удостоверений на стороне сервера, затем для аутентификации клиентов используются обычные методы проверки имени пользователя и пароля через созданное безопасное соединение. Таким образом защищаются персональные данные клиентов. Однако метод PEAP поддерживает лишь методы аутенификации клиента EAP, такие как EAP-MD5, EAP-MSCHAPv2 и EAP-GTC. Метод EAP-GTC реализует только корпорация Cisco.

LEAP (Упрощенный расширяемый протокол аутентификации)

LEAP (Упрощенный расширяемый протокол аутентификации) представляет собой протокол стандарта IEEE 802.1x, реализованный корпорацией Cisco.

Dynamic WEP Key Exchange (Динамический обмен ключами WEP)

Точка доступа копирует уникальный ключ, генерируемый сервером RADIUS. Этот ключ действителен до тех пор, пока беспроводное соединение не будет разорвано, не будет превышен лимит времени простоя, либо пока не истечет время простоя при повторной аутентификации. При каждой повторной аутентификации генерируется новый ключ WEP.

Если включить эту функцию, то настраивать ключ шифрования по умолчанию в окне "Wireless" (Беспроводная сеть) не обязательно. Вы можете создавать и сохранять ключи в этом окне, но они не будут использоваться при включенном режиме динамического шифрования WEP.

ПРИМЕЧАНИЕ: EAP-MD5 нельзя использовать для динамического обмена ключами WEP

Для дополнительной безопасности методы аутентификации на основе цифровых удостоверений (EAP-TLS, EAP-TTLS и PEAP) используют динамические ключи для шифрования данных. Они часто используются в корпоративной среде, однако для применения в обычной среде более практичным оказывается традиционная пара "имя пользователя+пароль". В приведенной ниже таблице сравниваются функции различных методов аутентификации.

Табл. 141 Сравнительный анализ методов аутентификации EAP

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Двусторонняя аутентификация	Нет	Да	Да	Да	Да
Удостоверение — Клиент	Нет	Да	По выбору	По выбору	Нет
Удостоверение — Сервер	Нет	Да	Да	Да	Нет
Динамический обмен ключами	Нет	Да	Да	Да	Да
Credential Integrity (Целостность мандата)	Нет	Сильная	Сильная	Сильная	Средняя
Сложность применения	Простое	Сложное	Среднее	Среднее	Среднее
Client Identity Protection (Защита персональных данных клиентского устройства)	Нет	Нет	Да	Да	Нет

WPA

Аутентификация пользователя

В WPA применяется стандарт IEEE 802.1x и протокол EAP (Extensible Authentication Protocol — Расширяемый протокол аутентификации) для аутентификации беспроводных устройств с использованием внешней базы данных RADIUS.

Шифрование

В WPA шифрование данных оптимизируется с помощью протокола временной целостности ключа (TKIP) или расширенного стандарта шифрования (AES), проверки целостности пакетов (MIC) и IEEE 802.1x.

В протоколе TKIP используются 128-разрядные ключи, динамически генерируемые и распределяемые сервером аутентификации. Протокол поддерживает попакетное смешение ключей, проверку целостности пакетов (MIC), расширенный вектор инициализации (IV) с правилами упорядочения, а также механизм повторного генерирования ключей.

Протокол TKIP регулярно меняет и чередует ключи шифрования, так чтобы один и тот же ключ шифрования никогда не использовался дважды.

Сервер RADIUS выдает парный главный ключ (PMK) точке доступа, которая затем создает систему управления и иерархии ключей с использованием парного ключа для динамического генерирования уникальных ключей шифрования данных для шифрования каждого пакета, передаваемого беспроводным методом между точкой доступа и беспроводными устройствами. Все это происходит автоматически в фоновом режиме.

AES (Расширенный стандарт шифрования) также использует секретный ключ. В этой версии AES к 128-разрядным блокам данных применяются 128-разрядные ключи.

Проверка целостности пакетов (MIC) предназначена для предотвращения перехвата, изменения и повторной отправки пакетов данных злоумышленниками. MIC имеет строгую математическую функцию, где принимающая и отправляющая стороны вычисляют каждая свой MIC, которые затем сравниваются. Если они не совпадают, то предполагается, что данные испорчены, и пакет удаляется.

При помощи генерирования уникальных ключей шифрования данных для каждого пакета данных и создания алгоритма проверки на целостность (MIC) протокол TKIP гораздо больше осложняет дешифрование данных в сети Wi-Fi по сравнению с WEP, затрудняя злоумышленнику проникновение в сеть.

Механизмы шифрования, используемые для WPA и WPA-PSK, одинаковы. Разница между WPA и WPA-PSK состоит в том, что WPA-PSK использует единственный предварительно согласованный ключ (пароль) для аутентификации всех пользователей, в то время как WPA предполагает наличие индивидуального пароля у каждого пользователя. Использование обычного пароля делает механизм WPA-PSK восприимчивым к атакам "грубой силы" с подбором пароля, но по сравнению с WEP он является более прогрессивным, поскольку здесь применяется более простой в использовании, постоянный буквенно-цифровой пароль.

Обзор параметров безопасности

В этой таблице приведены прочие параметры безопасности, которые нужно настроить для каждого метода аутентификации/протокола управления ключами. MAC-адрес фильтров не зависит от конфигурации этих характеристик безопасности.

Табл. 142 Сравнительная таблица беспроводной безопасности

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	РУЧНОЙ ВВОД КЛЮЧА	ВКЛЮЧЕНИЕ IEEE 802.1X
Открытый	Отсутствует	Нет	Нет
Открытый	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен с динамическим ключом WEP
		Да	Отключен

Табл. 142 Сравнительная таблица беспроводной безопасности (продолжение)

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	РУЧНОЙ ВВОД КЛЮЧА	ВКЛЮЧЕНИЕ IEEE 802.1X
Коллективный	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен с динамическим ключом WEP
		Да	Отключен
WPA	WEP	Нет	Да
WPA	TKIP	Нет	Да
WPA-PSK	WEP	Да	Да
WPA-PSK	TKIP	Да	Да

Приложение L
Описание сообщений журнала

Настоящее приложение содержит примеры и описания сообщений в регистрационном журнале.

Табл. 143 Журнальные сообщения, связанные с обслуживанием системы

СООБЩЕНИЕ	ОПИСАНИЕ
`Time calibration is successful`	Маршрутизатор синхронизировал свое время на базе информации, полученной от сервера времени.
`Time calibration failed`	При синхронизации времени маршрутизатора с сервером времени произошел сбой.
`WAN interface gets IP:%s`	Порту WAN назначен новый IP-адрес от сервера DHCP, PPPoE, PPTP или удаленного сервера.
`DHCP client IP expired`	Время аренды IP-адреса клиента DHCP истекло.
`DHCP server assigns%s`	Сервер DHCP назначил клиенту IP-адрес.
`Successful SMT login`	Успешный вход в систему через интерфейс SMT.
`SMT login failed`	Произошел сбой при входе в систему через интерфейс SMT маршрутизатора.
`Successful WEB login`	Успешный вход в систему через интерфейс Web-конфигуратора.
`WEB login failed`	Произошел сбой при входе в систему через интерфейс Web-конфигуратора.
`Successful TELNET login`	Успешный вход в систему по telnet.
`TELNET login failed`	Произошел сбой при входе в систему по telnet.
`Successful FTP login`	Успешный вход в систему по ftp.
`FTP login failed`	Произошел сбой при регистрации сеанса ftp.
`NAT Session Table is Full!`	Достигнуто максимальное число записей в таблице NAT и таблица заполнена.
`Starting Connectivity Monitor`	Запуск Диспетчера соединений.
`Time initialized by Daytime Server`	Маршрутизатор получил время и дату от сервера даты и времени.
`Time initialized by Time server`	Маршрутизатор получил время и дату от сервера времени.
`Time initialized by NTP server`	Маршрутизатор получил время и дату от сервера NTP.
`Connect to Daytime server fail`	Произошел сбой при подключении маршрутизатора к серверу даты и времени.
`Connect to Time server fail`	Произошел сбой при подключении маршрутизатора к серверу времени.
`Connect to NTP server fail`	Произошел сбой при подключении маршрутизатора к серверу NTP.
`Too large ICMP packet has been dropped`	Маршрутизатор сбросил пакет ICMP, размер которого превышал допустимый.

Табл. 143 Журнальные сообщения, связанные с обслуживанием системы

СООБЩЕНИЕ	ОПИСАНИЕ
`SMT Session Begin`	Начался сеанс управления SMT.
`SMT Session End`	Закончился сеанс управления SMT.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	Маршрутизатор сохраняет изменения конфигурации.
`Successful SSH login`	Успешный вход в систему через сервер SSH.
`SSH login failed`	Произошел сбой при входе в систему через сервер SSH маршрутизатора.
`Successful HTTPS login`	Успешный вход в систему через интерфейс Web-конфигуратора по протоколу HTTPS.
`HTTPS login failed`	Произошел сбой при входе в систему через интерфейс Web-конфигуратора по протоколу HTTPS.

Табл. 144 Журнальные сообщения о системных ошибках

СООБЩЕНИЕ	ОПИСАНИЕ
`%s exceeds the max. number of session per host!`	Попытка создания сеанса NAT привела к превышению максимального количества записей в таблице сеансов NAT, допустимого для одного узла.
`setNetBIOSFilter: calloc error`	Произошел сбой при выделении памяти маршрутизатора для параметров фильтра NetBIOS.
`readNetBIOSFilter: calloc error`	Произошел сбой при выделении памяти маршрутизатора для параметров фильтра NetBIOS.
`WAN connection is down.`	Подключение к глобальной сети не работает. Доступ в сеть через этот порт невозможен.

Табл. 145 Журнальные сообщения, связанные с управлением доступом

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>`	Попытка доступа через протокол TCP/UDP/IGMP/ESP/GRE/OSPF, подпадающая под действие политики межсетевого экрана, заданной по умолчанию, и заблокированная либо переадресованная согласно установкам этой политики.
`Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>`	Попытка доступа через протокол TCP/UDP/IGMP/ESP/GRE/OSPF, подпадающая (или не подпадающая) под действие заданного правила межсетевого экрана (обозначается номером) и заблокированная или переадресованная согласно этому правилу.
`Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран разрешил проход сеанса с треугольным маршрутом.

Табл. 145 Журнальные сообщения, связанные с управлением доступом (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Маршрутизатор заблокировал пакет, для которого нет соответствующей записи в таблице NAT.
`Router sent blocked web site message: TCP`	Маршрутизатор отправил сообщение, уведомляющее пользователя о блокировке доступа к запрошенному Web-сайту.

Табл. 146 Журнальные сообщения о сбросе сеансов TCP

СООБЩЕНИЕ	ОПИСАНИЕ
`Under SYN flood attack, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP при обнаружении синхронной атаки на узел (подсчет незавершенных сеансов TCP ведется по целевому хосту.)
`Exceed TCP MAX incomplete, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP, когда количество незавершенных подключений через TCP превысило заданное пользователем пороговое значение. (Подсчет незавершенных сеансов TCP ведется по целевому хосту.) ПРИМЕЧАНИЕ: См. **TCP Maximum Incomplete (Максимальное кол-во незавершенных сеансов TCP)** в экранной форме **Firewall Attack Alerts (Сообщения об атаках на межсетевой экран)**.
`Peer TCP state out of order, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP при обнаружении сбоя в подключении через TCP. Примечание: Для проверки состояния подключения через TCP межсетевой экран обращается к RFC793 (рис. 6).
`Firewall session time out, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP по истечении времени простоя динамического сеанса связи через межсетевой экран. Время простоя сеансов связи по умолчанию: ICMP: 3 минуты UDP: 3 минуты TCP (трехсторонние сигналы согласования установления связи): 270 секунд Время ожидания TCP FIN: 2 x MSL (Maximum Segment Lifetime, максимальное время существования сегмента, задается в заголовке TCP). Простой соединения через TCP (установленного): 150 минут Время ожидания сброса TCP: 10 секунд

Табл. 146 Журнальные сообщения о сбросе сеансов TCP (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Exceed MAX incomplete, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP, когда количество незавершенных подключений (через TCP и UDP) превысило заданное пользователем пороговое значение. (Подсчет незавершенных подключений производится для всех подключений по TCP и UDP через межсетевой экран.) Примечание: когда количество незавершенных подключений (TCP + UDP) превышает верхний порог (“Maximum Incomplete High”), маршрутизатор отправляет пакеты сброса (TCP RST) подключений через TCP и начинает удаление динамических сеансов связи через межсетевой экран (TOS); операция прекращается, когда количество незавершенных подключений становится меньше нижнего порога (“Maximum Incomplete Low”).
`Access block, sent TCP RST`	Маршрутизатор отправит пакет TCP RST и создаст эту запись в журнале, если Вы включите механизм сброса TCP межсетевого экрана (с помощью команды интерепретатора "sys firewall tcprst").

Табл. 147 Журнальные сообщения о фильтре пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set:%d, rule:%d)`	Произведена попытка доступа, соответствущая настроенному правилу фильтра (указывается номер набора и номер правила), и выполнена блокировка или пересылка пакета в соответствии с правилом.

Табл. 148 Журнальные сообщения ICMP (протокол межсетевых управляющих сообщений)

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	Доступ через протокол межсетевых управляющих сообщений (ICMP), подпадающий под действие политики по умолчанию и заблокированный или переадресованный согласно настройкам пользователя. Подробное описание типов и кодов приведено в Табл. 160 на с. 481.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	Доступ через ICMP, подпадающий (либо не подпадающий) под действие правила для межсетевых экранов (идентифицированное своим номером) и блокированный или переадресованный в соответствии с правилом. Подробное описание типов и кодов приведено в Табл. 160 на с. 481.
`Triangle route packet forwarded: ICMP`	Межсетевой экран разрешил проход сеанса с треугольным маршрутом.
`Packet without a NAT table entry blocked: ICMP`	Маршрутизатор заблокировал пакет, для которого нет соответствующей записи в таблице NAT.

Табл. 148 Журнальные сообщения ICMP (протокол межсетевых управляющих сообщений) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Unsupported/out-of-order ICMP: ICMP`	Межсетевой экран не поддерживает такие пакеты ICMP либо произошел сбой в пакетах ICMP.
`Router reply ICMP packet: ICMP`	Маршрутизатор послал ответный пакет ICMP отправителю.

Табл. 149 Журнальные сообщения CDR (журнала регистрации вызовов)

СООБЩЕНИЕ	ОПИСАНИЕ
`board%d line%d channel%d, call%d,%s C01 Outgoing Call dev=%x ch=%x%s`	Маршрутизатор получил запрос на установление соединения для выполнения вызова. “call” — номер вызова. “dev” — тип устройства (3 — коммутируемое соединение, 6 — PPPoE, 10 — PPTP). "channel" или “ch” — идентификатор канала вызова. Например,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" означает, что маршрутизатор выполнял вызов сервера PPPoE 3 раза.
`board%d line%d channel%d, call%d,%s C02 OutCall Connected%d%s`	Установлено PPPoE, PPTP или коммутируемое соединение.
`board%d line%d channel%d, call%d,%s C02 Call Terminated`	Прервано PPPoE, PPTP или коммутируемое соединение.

Табл. 150 Журнальные сообщения PPP (протокола "точка-точка")

СООБЩЕНИЕ	ОПИСАНИЕ
`ppp:LCP Starting`	Запущена стадия протокола управления каналом связи для PPP соединения.
`ppp:LCP Opening`	Открывается стадия протокола управления каналом связи для PPP соединения.
`ppp:CHAP Opening`	Открывается стадия протокола аутентификации по методу "вызов-рукопожатие" (Challenge Handshake Authentication) для PPP соединения.
`ppp:IPCP Starting`	Начинается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.
`ppp:IPCP Opening`	Открывается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.
`ppp:LCP Closing`	Закрывается стадия протокола управления каналом связи (Link Control Protocol) для PPP соединения.
`ppp:IPCP Closing`	Закрывается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.

Табл. 151 Журнальные сообщения UPnP

СООБЩЕНИЕ	ОПИСАНИЕ
`UPnP pass through Firewall`	Пакеты UPnP могут проходить через межсетевой экран.

Табл. 152 Журнальные сообщения о фильтрации содержания

СООБЩЕНИЕ	ОПИСАНИЕ
`%s: Keyword blocking`	На запрошенной веб-странице имеется заданное пользователем ключевое слово.
`%s: Not in trusted web list`	Данный web-сайт находится на домене, не гарантирующем высокой степени защиты, и маршрутизатор блокирует весь трафик, оставляя доступ только к сайтам, размещенным на надежных доменах.
`%s: Forbidden Web site`	Данный web-сайт входит в список запрещенных.
`%s: Contains ActiveX`	Данный web-сайт содержит элементы ActiveX.
`%s: Contains Java applet`	Данный web-сайт содержит апплеты языка Java.
`%s: Contains cookie`	Данный web-сайт содержит файлы cookie.
`%s: Proxy mode detected`	Маршрутизатор обнаружил режим proxy в данном пакете .
`%s`	Сервер фильтрации содержания ответил, что данный web-сайт входит в список заблокированных, но не указал категорию блокировки.
`%s:%s`	Сервер фильтрации содержания ответил, что данный web-сайт входит в список заблокированных, и указал категорию блокировки.
`%s(cache hit)`	Система обнаружила, что данный web-сайт входит в список заблокированных из локального кэша, но не указала категорию блокировки.
`%s:%s(cache hit)`	Система обнаружила, что данный web-сайт входит в список заблокированных из локального кэша, и известна категория блокировки.
`%s: Trusted Web site`	Данный web-сайт находится на доверенном домене с высокой степенью защиты.
`%s`	Если фильтр содержания отключен согласно расписанию или Вы не поставили метку напротив Block Matched Web Site ("Блокируемый сайт"), то система переадресует содержание.
`Waiting content filter server timeout`	Сервер фильтрации внешнего содержания не ответил в течение заданного времени ожидания.
`DNS resolving failed`	Интернет-центр не может получить IP-адрес сервера фильтрации внешнего содержания через запрос DNS.
`Creating socket failed`	Интернет-центр не может выдать запрос из-за сбоя при создании канала TCP/IP, порт:номер порта.

Табл. 152 Журнальные сообщения о фильтрации содержания (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Connecting to content filter server fail`	Сбой при подключении к серверу фильтрации внешнего содержания.
`License key is invalid`	Недействительный лицензионный ключ внешнего сервера фильтрации содержания.

Табл. 153 Журнальные сообщения об атаках

СООБЩЕНИЕ	ОПИСАНИЕ
`attack [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран обнаружил атаку TCP/UDP/IGMP/ESP/GRE/OSPF.
`attack ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку ICMP. Подробное описание типов и кодов приведено в Табл. 160 на с. 481.
`land [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран обнаружил атаку по TCP/UDP/IGMP/ESP/GRE/OSPF на каталог локальной сети (LAND).
`land ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку ICMP на каталог локальной сети (LAND). Подробное описание типов и кодов приведено в Табл. 160 на с. 481.
`ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран обнаружил атаку с подменой IP-адреса на порт WAN.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку с подменой IP-адреса ICMP на порт WAN. Подробное описание типов и кодов приведено в Табл. 160 на с. 481.
`icmp echo: ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку с использованием отклика ICMP. Подробное описание типов и кодов приведено в Табл. 160 на с. 481.
`syn flood TCP`	Межсетевой экран обнаружил синхронную атаку TCP.
`ports scan TCP`	Межсетевой экран обнаружил атаку TCP со сканированием портов.
`teardrop TCP`	Межсетевой экран обнаружил Teardrop-атаку TCP.
`teardrop UDP`	Межсетевой экран обнаружил Teardrop-атаку UDP.
`teardrop ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил Teardrop-атаку ICMP. Подробное описание типов и кодов приведено в Табл. 160 на с. 481.
`illegal command TCP`	Межсетевой экран обнаружил атаку TCP с недопустимой командой.
`NetBIOS TCP`	Межсетевой экран обнаружил атаку TCP NetBIOS.
`ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран классифицировал пакет без записи о маршрутизации от источника как атаку с подменой IP-адреса.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	Межсетевой экран классифицировал пакет ICMP без указания источника как атаку с подстановкой IP (IP spoofing).

Табл. 153 Журнальные сообщения об атаках (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`vulnerability ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку ICMP на уязвимость. Подробное описание типов и кодов приведено в Табл. 160 на с. 481.
`traceroute ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку ICMP с отслеживанием маршрута. Подробное описание типов и кодов приведено в Табл. 160 на с. 481.

Табл. 154 Журнальные сообщения IPSec

СООБЩЕНИЕ	ОПИСАНИЕ
`Discard REPLAY packet`	Маршрутизатор получил и отклонил пакет с некорректным порядковым номером.
`Inbound packet authentication failed`	Маршрутизатор получил пакет, который был изменен. Пакет мог быть изменен или умышленно испорчен третьей стороной.
`Receive IPSec packet, but no corresponding tunnel exists`	Маршрутизатор удалил входящий пакет, для которого протокол последовательного периферийного интерфейса (SPI) не смог найти соответствующего безопасного соединения в фазе 2 (Phase 2 SA).
`Rule <%d> idle time out, disconnect`	Маршрутизатор разорвал соединение, имевшее исходящий и не имевшее входящего трафика в течение определенного периода времени. Для установки периода времени можно использовать команду "ipsec timer chk_conn". Значение по умолчанию составляет 2 минуты.
`WAN IP changed to <IP>`	Маршрутизатор разорвал все соединения с “MyIP” = “0.0.0.0” при изменении IP-адреса в глобальной сети (WAN).

Табл. 155 Журнальные сообщения протокола обмена ключами (IKE)

СООБЩЕНИЕ	ОПИСАНИЕ
`Active connection allowed exceeded`	Сбой при обмене ключами для установки нового соединения из-за достижения предельного количества одновременных безопасных подключений в фазе 2 (Phase 2 SA).
`Start Phase 2: Quick Mode`	Запущен быстрый режим 2-й фазы.
`Verifying Remote ID failed:`	Соединение разорвано во время 2-й фазы обмена ключами (IKE) из-за несовпадения локальных/удаленных адресов маршрутизатора и клиентского устройства.
`Verifying Local ID failed:`	Соединение разорвано во время 2-й фазы обмена ключами (IKE) из-за несовпадения локальных/удаленных адресов маршрутизатора и клиентского устройства.
`IKE Packet Retransmit`	Маршрутизатор выполнил повторную передачу пакета, т.к. не был получен ответ от клиентского устройства.
`Failed to send IKE Packet`	Передача пакетов обмена ключами (IKE) маршрутизатором была прервана из-за ошибки Ethernet.

Табл. 155 Журнальные сообщения протокола обмена ключами (IKE) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Too many errors! Deleting SA`	Безопасное соединение (SA) было сброшено из-за слишком большого количества ошибок.
`Phase 1 IKE SA process done`	Завершена 1-я фаза обмена ключами (IKE) при установке безопасного соединения.
`Duplicate requests with the same cookie`	Маршрутизатор получил несколько запросов от одного клиентского устройства, но продолжает обрабатывать первый пакет IKE от данного устройства.
`IKE Negotiation is in process`	Маршрутизатор уже начал согласование по установке соединения с другой стороной, но процесс обмена ключами (IKE) не завершен.
`No proposal chosen`	Не совпадают параметры фазы 1 или фазы 2. Проверьте все протоколы / настройки. Пример: если одно устройство конфигурируется под 3DES, а другое — под DES, то установить соединение будет невозможно.
`Local / remote IPs of incoming request conflict with rule <%d>`	Задан адрес безопасного шлюза “0.0.0.0”, и маршрутизатор использовал "локальный адрес" клиентского устройства в качестве "удаленного адреса" маршрутизатора. Эта информация вошла в конфликт со статическим правилом #d, поэтому подключение не было разрешено.
`Cannot resolve Secure Gateway Addr for rule <%d>`	Маршрутизатор не смог выделить IP-адрес из имени домена, который использовался в качестве адреса безопасного шлюза.
`Peer ID: <peer id> <My remote type> -<My local type>`	Отображаемый ID не совпал на разных концах соединения.
`vs. My Remote <My remote> - <My remote>`	Отображаемый ID не совпал на разных концах соединения.
`vs. My Local <My local>-<My local>`	Отображаемый ID не совпал на разных концах соединения.
`Send <packet>`	Отправлен пакет.
`Recv <packet>`	Протокол обмена ключами использует пакет ISAKMP для передачи данных. В каждом пакете ISAKMP содержится много различных типов полезной информации. Все они отображаются в журнале. Список всех типов полезной информации в пакетах ISAKMP приведен в RFC2408 – ISAKMP.
`Recv <Main or Aggressive> Mode request from <IP>`	Маршрутизатор получил с указанного адреса клиентского устройства запрос на начало согласования по обмену ключами.
`Send <Main or Aggressive> Mode request to <IP>`	Маршрутизатор начал процесс согласования с клиентским устройством.
`Invalid IP <Peer local> / <Peer local>`	Недействительный локальный IP-адрес клиентского устройства.
`Remote IP <Remote IP> / <Remote IP> conflicts`	Задан адрес безопасного шлюза “0.0.0.0”, и маршрутизатор использовал "локальный адрес" клиентского устройства в качестве "удаленного адреса" маршрутизатора. Эта информация вошла в конфликт со статическим правилом #d, поэтому подключение не было разрешено.

Табл. 155 Журнальные сообщения протокола обмена ключами (IKE) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Phase 1 ID type mismatch	Тип клиентского идентификатора ("Peer ID Type") данного маршрутизатора отличается от типа локального идентификатора ("Local ID Type") маршрутизатора IPSec, обслуживающего клиентское устройство.
Phase 1 ID content mismatch	Содержание клиентского идентификатора ("Peer ID Content") данного маршрутизатора отличается от содержания локального идентификатора ("Local ID Content") маршрутизатора IPSec, обслуживающего клиентское устройство.
No known phase 1 ID type found	При попытке подключения маршрутизатор не смог найти известного идентификатора 1-й фазы.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	Не совпадают типы идентификаторов 1-й фазы.
ID content mismatch	Не совпадает содержание идентификаторов 1-й фазы.
Configured Peer ID Content: <Configured Peer ID Content>	Не совпадает содержание идентификаторов 1-й фазы и отображается настроенное содержание идентификатора клиентского устройства ("Peer ID Content").
Incoming ID Content: <Incoming Peer ID Content>	Не совпадает содержание идентификаторов 1-й фазы и отображается содержание идентификатора входящих пакетов.
Unsupported local ID Type: <%d>	Данный тип идентификатора 1-й фазы не поддерживается маршрутизатором.
Build Phase 1 ID	Маршрутизатор начал построение идентификатора 1-й фазы.
Adjust TCP MSS to%d	Маршрутизатор автоматически изменил максимальный размер сегментов TCP после создания туннельного соединения.
Rule <%d> input idle time out, disconnect	Туннельное соединение в рамках имеющегося правила было разорвано из-за отсутствия входящего трафика в течение времени простоя.
XAUTH succeed! Username: <Username>	Для аутентификации имеющегося имени пользователя маршрутизатор использовал расширенную аутентификацию.
XAUTH fail! Username: <Username>	Маршрутизатор не смог использовать расширенную аутентификацию для аутентификации имеющегося имени пользователя.
Rule[%d] Phase 1 negotiation mode mismatch	Режим согласования 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 1 encryption algorithm mismatch	Алгоритм шифрования 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 1 authentication algorithm mismatch	Алгоритм аутентификации 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 1 authentication method mismatch	Метод аутентификации 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.

Табл. 155 Журнальные сообщения протокола обмена ключами (IKE) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Rule [%d] Phase 1 key group mismatch`	Группа ключей 1-й фазы обмена ключами (IKE), заданная в правиле маршрутизатора, не совпадает с таковой у клиентского устройства.
`Rule [%d] Phase 2 protocol mismatch`	Протокол 2-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
`Rule [%d] Phase 2 encryption algorithm mismatch`	Алгоритм шифрования 2-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
`Rule [%d] Phase 2 authentication algorithm mismatch`	Алгоритм аутентификации 2-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
`Rule [%d] Phase 2 encapsulation mismatch`	Инкапсуляция 2-й фазы обмена ключами (IKE), заданная в правиле маршрутизатора, не совпадает с таковой у клиентского устройства.
`Rule [%d]> Phase 2 pfs mismatch`	Настройки абсолютной секретности пересылки (pfs) 2-й фазы обмена ключами (IKE), заданные в правиле маршрутизатора, не совпадают с таковыми у клиентского устройства.
`Rule [%d] Phase 1 ID mismatch`	Идентификатор 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
`Rule [%d] Phase 1 hash mismatch`	Хэш 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
`Rule [%d] Phase 1 preshared key mismatch`	Предварительно согласованный ключ 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
`Rule [%d] Tunnel built successfully`	Успешно установлено заданное в правиле туннельное соединение IPSec.
`Rule [%d] Peer's public key not found`	Не найден заданный в правиле открытый ключ клиентского устройства в рамках 1-й фазы обмена ключами (IKE).
`Rule [%d] Verify peer's signature failed`	Не удалось проверить заданную в правиле подпись клиентского устройства в рамках 1-й фазы обмена ключами (IKE).
`Rule [%d] Sending IKE request`	Протокол обмена ключами (IKE) отправил IKE-запрос для имеющегося правила.
`Rule [%d] Receiving IKE request`	Протокол обмена ключами (IKE) получил IKE-запрос для имеющегося правила.
`Swap rule to rule [%d]`	Маршрутизатор переключился на использование имеющегося правила.
`Rule [%d] Phase 1 key length mismatch`	Длина ключа 1-й фазы обмена ключами (с алгоритмом шифрования AES), заданная в правиле маршрутизатора, не совпадает с таковой у клиентского устройства.
`Rule [%d] phase 1 mismatch`	1-я фаза обмена ключами (IKE), заданная в правиле маршрутизатора, не соответствует таковой у клиентского устройства.

Табл. 155 Журнальные сообщения протокола обмена ключами (IKE) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Rule [%d] phase 2 mismatch`	2-я фаза обмена ключами (IKE), заданная в правиле маршрутизатора, не соответствует таковой у клиентского устройства.
`Rule [%d] Phase 2 key length mismatch`	Длина ключей 2-й фазы обмена ключами (с алгоритмом шифрования AES), заданная в правиле маршрутизатора, не совпадает с таковой у клиентского устройства.

Табл. 156 Журнальные сообщения PKI (инфраструктуры сертификации открытых ключей)

СООБЩЕНИЕ	ОПИСАНИЕ
`Enrollment successful`	Успешно выполнена регистрация сертификата SCEP в режиме реального времени. Поле "Адрес назначения" содержит IP-адрес и порт сервера бюро сертификации.
`Enrollment failed`	Не удалось выполнить регистрацию сертификата SCEP в режиме реального времени. Поле "Адрес назначения" содержит IP-адрес и порт сервера бюро сертификации.
`Failed to resolve <SCEP CA server url>`	Не удалось выполнить регистрацию сертификата SCEP в режиме реального времени из-за невозможности определения адреса сервера бюро сертификации.
`Enrollment successful`	Успешно выполнена регистрация сертификата CMP в режиме реального времени. Поле "Адрес назначения" содержит IP-адрес и порт сервера бюро сертификации.
`Enrollment failed`	Не удалось выполнить регистрацию сертификата CMP в режиме реального времени. Поле "Адрес назначения" содержит IP-адрес и порт сервера бюро сертификации.
`Failed to resolve <CMP CA server url>`	Не удалось выполнить регистрацию сертификата CMP в режиме реального времени из-за невозможности определения IP-адреса сервера бюро сертификации.
`Rcvd ca cert: <subject name>`	Маршрутизатор получил сертификат бюро сертификации с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле "Отправитель".
`Rcvd user cert: <subject name>`	Маршрутизатор получил сертификат пользователя с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле "Отправитель".
`Rcvd CRL <size>: <issuer name>`	Маршрутизатор получил список аннулирования сертификатов (CRL) с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле "Отправитель".
`Rcvd ARL <size>: <issuer name>`	Маршрутизатор получил список аннулирования полномочий (ARL) с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле "Отправитель".
`Failed to decode the received ca cert`	Маршрутизатор получил недействительный сертификат бюро сертификации от сервера LDAP, IP-адрес и порт которого указаны в поле "Отправитель".

Табл. 156 Журнальные сообщения PKI (инфраструктуры сертификации открытых ключей) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Failed to decode the received user cert`	Маршрутизатор получил недействительный сертификат пользователя от сервера LDAP, IP-адрес и порт которого указаны в поле "Отправитель".
`Failed to decode the received CRL`	Маршрутизатор получил недействительный список аннулирования сертификатов (CRL) от сервера LDAP, IP-адрес и порт которого указаны в поле "Отправитель".
`Failed to decode the received ARL`	Маршрутизатор получил недействительный список аннулирования полномочий (ARL) от сервера LDAP, IP-адрес и порт которого указаны в поле "Отправитель".
`Rcvd data <size> too large! Max size allowed: <max size>`	Маршрутизатор получил слишком большой объем данных справочника (с указанием размера) от сервера LDAP, IP-адрес и порт которого указаны в поле "Отправитель". Также указывается максимальный размер данных справочника, которые может пропустить маршрутизатор.
`Cert trusted: <subject name>`	Маршрутизатор сверил путь сертификата с указанной темой.
`Due to <reason codes>, cert not trusted: <subject name>`	В силу перечисленных причин сертификат с указанной темой не прошел сверку пути. Зарегистрированные коды отражают лишь примерные причины ненадежности сертификату. Соответствующие описания кодов приведены в Табл. 157 на с. 478.

Табл. 157 Коды причин непрохождения сверки путей сертификатов

КОД	ОПИСАНИЕ
1	Несоответствие алгоритмов в сертификате и критериях поиска.
2	Несоответствие при использовании ключей в сертификате и критериях поиска.
3	Сертификат был недействителен в данном интервале времени.
4	(Не используется)
5	Сертификат недействителен.
6	Подлинность подписи сертификата не была корректно проверена.
7	Сертификат входит в список аннулирования сертификатов (CRL).
8	Сертификат не был добавлен в кэш.
9	Не удалось декодировать сертификат.
10	Сертификат (нигде) не найден.
11	Замыкание цепи сертификатов (не найден доверенный корень).
12	Сертификат содержит критическое расширение, которое не было обработано.
13	Непроверенный издатель сертификата (отсутствуют сведения о бюро сертификации).
14	(Не используется)
15	Слишком старый список аннулирования сертификатов (CRL).
16	Недействительный CRL.

Табл. 157 Коды причин непрохождения сверки путей сертификатов (продолжение)

КОД	ОПИСАНИЕ
17	Подлинность подписи CRL не была корректно проверена.
18	CRL (нигде) не найден.
19	CRL не был добавлен в кэш.
20	Не удалось декодировать CRL.
21	CRL будет действителен только в будущем.
22	CRL содержит дублируемые серийные номера.
23	Временной интервал не является непрерывным.
24	Нет сведений о времени.
25	Из-за истечения времени ожидания не удалось проверить подлинность методом баз данных.
26	Не удалось проверить подлинность методом баз данных.
27	Путь не проверен.
28	Достигнута максимальная длина пути.

Табл. 158 Журнальные сообщения 802.1X

СООБЩЕНИЕ	ОПИСАНИЕ
`Local User Database accepts user.`	Подлинность пользователя была установлена встроенной базой данных пользователей.
`Local User Database reports user credential error.`	Подлинность пользователя не была установлена встроенной базой данных пользователей, так как был введен неверный пароль.
`Local User Database does not find user`s credential.`	Подлинность пользователя не была установлена встроенной базой данных пользователей, так как пользователь не числится во встроенной базе данных.
`RADIUS accepts user.`	Подлинность пользователя была установлена сервером RADIUS.
`RADIUS rejects user. Pls check RADIUS Server.`	Подлинность пользователя не была установлена сервером RADIUS. Проверьте сервер RADIUS.
`Local User Database does not support authentication method.`	Встроенная база данных пользователей поддерживает только метод EAP-MD5. Пользователь пытался использовать другой метод метод аутентификации и его подлинность не была установлена.
`User logout because of session timeout expired.`	Маршрутизатор вывел из системы пользователя с истекшим сроком действия сеанса связи.
`User logout because of user deassociation.`	Маршрутизатор вывел из системы пользователя, завершившего сеанс связи.
`User logout because of no authentication response from user.`	Маршрутизатор вывел из системы пользователя, от которого не поступил ответ на аутентификацию.

Табл. 158 Журнальные сообщения 802.1X (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`User logout because of idle timeout expired.`	Маршрутизатор вывел из системы пользователя, у которого превышен лимит времени простоя.
`User logout because of user request.`	Пользователь вышел из системы.
`Local User Database does not support authentication mothed.`	Пользователь попытался использовать метод аутентификации, не поддерживаемый встроенной базой данных пользователей (база поддерживает только EAP-MD5).
`No response from RADIUS. Pls check RADIUS Server.`	Нет ответа от сервера RADIUS, проверьте сервер RADIUS.
`Use Local User Database to authenticate user.`	Встроенная база данных пользователей работает в качестве аутентификационного сервера.
`Use RADIUS to authenticate user.`	Сервер RADIUS работает в качестве аутентификационного сервера.
`No Server to authenticate user.`	Отсутствует аутентификационный сервер, способный установить подлинность пользователя.
`Local User Database does not find user`s credential.`	Подлинность пользователя не была установлена встроенной базой данных пользователей, так как пользователь не числится во встроенной базе данных.

Табл. 159 Настройка списка управления доступом (ACL)

НАПРАВЛЕНИЕ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L to W)	LAN to WAN (лок. сеть — глоб. сеть)	Список управления доступом (ACL) для пакетов, пересылаемых из локальной сети (LAN) в глобальную (WAN).
(W to L)	WAN to LAN (глоб. сеть — лок. сеть)	Список управления доступом (ACL) для пакетов, пересылаемых из глобальной сети (WAN) в локальную (LAN).
(D to L)	DMZ to LAN (DMZ — лок. сеть)	Список управления доступом (ACL) для пакетов, пересылаемых из DMZ в локальную сеть (LAN).
(D to W)	DMZ to WAN (DMZ — глоб. сеть)	Список управления доступом (ACL) для пакетов, пересылаемых из DMZ в глобальную сеть (WAN).
(W to D)	WAN to DMZ (глоб. сеть — DMZ)	Список управления доступом (ACL) для пакетов, пересылаемых из глобальной сети (WAN) в DMZ.
(L to D)	LAN to DMZ (лок. сеть — DMZ)	Список управления доступом (ACL) для пакетов, пересылаемых из локальной сети (LAN) в DMZ.

Табл. 159 Настройка списка управления доступом (ACL) (продолжение)

НАПРАВЛЕНИЕ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L to L/ZW)	Соединение одной лок. сети с другой (LAN–LAN) или с интернет-центром	Список управления доступом (ACL) для пакетов, пересылаемых из одной локальной сети в другую или в интернет-центр.
(W to W/ZW)	Соединение одной глоб. сети с другой (WAN–WAN) или с интернет-центром	Список управления доступом (ACL) для пакетов, пересылаемых из одной глобальной сети в другую или в интернет-центр.
(D to D/ZW)	Соединение одной DMZ с другой DMZ или с интернет-центром	Список управления доступом (ACL) для пакетов, пересылаемых из одной DMZ в другую или в интернет-центр.

Табл. 160 Записи ICMP

ТИП	КОД	ОПИСАНИЕ
0		Эхо-ответ
	0	Сообщение с эхо-ответом
3		Адресат недоступен
	0	Сеть недоступна
	1	Узел недоступен
	2	Протокол недоступен
	3	Порт недоступен
	4	Пакет, который требует фрагментации, отброшен, так как имеет параметр DF (Don't Fragment — не фрагментировать)
	5	Ошибка в маршруте источника
4		Источник произвел сброс
	0	Шлюз может сбросить дейтаграммы Интернет, если он не имеет буферной памяти, достаточной для организации очереди дейтаграмм, чтобы передать их в следующую сеть по маршруту к сети получателя.
5		Перенаправление
	0	Перенаправление дейтаграмм для сети
	1	Перенаправление дейтаграмм для узла
	2	Перенаправление дейтаграмм для типа услуги (ToS) и сети
	3	Перенаправление дейтаграмм для типа услуги (ToS) и узла
8		Эхо
	0	Эхо-сообщение

Табл. 160 Записи ICMP (продолжение)

ТИП	КОД	ОПИСАНИЕ
11		Время истекло
	0	Время жизни пекета истекло в пути
	1	Время на повторную сборку фрагментов истекло
12		Неверный параметр
	0	Указатель показывает на ошибку
13		Временная метка
	0	Сообщение с запросом временной метки
14		Ответ с временной меткой
	0	Ответное сообщение с временной меткой
15		Запрос параметров
	0	Сообщение с запросом параметров
16		Ответ на запрос параметров
	0	Сообщение с ответом на запрос параметров

Табл. 161 Сообщения системного журнала

СООБЩЕНИЕ	ОПИСАНИЕ
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	"Это сообщение посылается системой ("RAS" отображается в качестве системного имени, если оно не было присвоено), когда маршрутизатор создает запись в системном журнале. Эта функция устанавливается на странице: ГЛАВНОЕ МЕНЮ Web-конфигуратора->ЖУРНАЛЫ РЕГИСТРАЦИИ->Настройки журналов. Серьезность ошибки — это класс записи в системном журнале. Описание сообщений и записей определяются различными схемами записей в этом приложении. “devID” — это последние три символа MAC-адреса порта LAN маршрутизатора. “cat” — то же, что категория в журналах маршрутизатора.

В следующей таблице приводятся типы полезной информации в сообщениях протокола ISAKMP (см. RFC-2408), и их обозначения в журнале. Более подробную информацию по каждому типу см. в RFC.

Табл. 162 Типы данных сообщений RFC-2408 ISAKMP

ОБОЗНАЧЕНИЕ В ЖУРНАЛЕ	ТИП ПОЛЕЗНОЙ ИНФОРМАЦИИ
SA	Безопасное соединение
PROP	Предложение
TRANS	Преобразование
KE	Обмен ключами

Табл. 162 Типы данных сообщений RFC-2408 ISAKMP (продолжение)

ОБОЗНАЧЕНИЕ В ЖУРНАЛЕ	ТИП ПОЛЕЗНОЙ ИНФОРМАЦИИ
ID	Идентификация
CER	Сертификат
CER_REQ	Запрос сертификата
HASH	Хеш
SIG	Подпись
NONCE	Сл. число
NOTFY	Уведомление
DEL	Удалить
VID	Идентификационный номер поставщика

Команды регистрационного журнала

Перейдите к интерфейсу интерпретатора команд.

Настройка регистрационного журнала интернет-центра

1. Для загрузки буфера журнальных настроек, позволяющего определить подлежащие регистрации журнальные записи, используйте команду "sys logs load".
2. Для просмотра списка категорий регистрационных записей используйте команду "sys logs category".

Рис. 269 Пример отображения категорий регистрационных записей

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras>?
Valid commands are:
sys             exit            ether           aux
ip              ipsec           bridge          bm
certificates    cnm             8021x           radius
ras>
```

3. Для отображения параметров, имеющихся для данной категории, используется команда "sys logs category", после которой указывается категория журнальной записи.

Рис. 270 Пример отображения параметров регистрационных записей

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/
1:show debug type]
```

4 Для определения записей, подлежащих регистрации в журнале, используется команда "sys logs category", после которой указывается категория журнальной записи и параметр.

Если записи данной категории не должны регистрироваться, введите "0", если должны регистрироваться только записи данной категории, введите "1", если должны регистрироваться только предупреждения данной категории, введите "2", если же должны регистрироваться и записи, и предупреждения данной категории, введите "3". Не все параметры доступны для каждой категории.

5 Этап 5.Для сохранения настроек интернет-центра (это необходимо выполнить, чтобы началась запись сообщений в журнал) используйте команду "sys logs save".

Отображение журнальных записей

- Для отображения всех записей журнала интернет-центра используйте команду "sys logs display".
- Для отображения настроек всех категорий журналов модема используйте команду "sys logs category display".
- Для отображения записей отдельной категории журнала интернет-центра используйте команду "sys logs display [log category]".
- Для удаления всех записей журнала интернет-центра используйте команду "sys logs clear".

Пример команды управления журналом

В этом примере показано, как настроить интернет-центр для регистрации сообщений и предупреждений о входе в систему и просмотреть результаты.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#.time                  source                  destination            notes

    message
 0|06/08/2004 05:58:21 |172.21.4.154          |224.0.1.24            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 1|06/08/2004 05:58:20 |172.21.3.56           |239.255.255.250       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 2|06/08/2004 05:58:20 |172.21.0.2            |239.255.255.254       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 3|06/08/2004 05:58:20 |172.21.3.191          |224.0.1.22            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 4|06/08/2004 05:58:20 |172.21.0.254          |224.0.0.1             |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 5|06/08/2004 05:58:20 |172.21.4.187:137      |172.21.255.255:137    |ACCESS
BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

Приложение M

Внутренний генератор таблицы системных параметров (SPTGEN)

Внутренний SPTGEN — общая информация

Внутренний генератор таблицы системных параметров (SPTGEN) представляет собой текстовый файл конфигурации, используемый для эффективной настройки нескольких интернет-центров. Внутренний генератор таблицы системных параметров (SPTGEN) позволяет задавать конфигурацию, сохранять и загружать множество меню одновременно при помощи одного текстового файла конфигурации, что исключает необходимость навигации и последовательной настройки множества меню SMT для каждого интернет-центра.

Формат текстового файла конфигурации

Все текстовые файлы внутреннего генератора таблицы системных параметров имеют схожий формат, а именно:

```
<field identification number = field name = parameter values
allowed = input>,
```

где <input> (ввод)- это вводимые данные, отвечающие <parameter values allowed> (допустимым значениям параметра).

На рисунке ниже приводится пример текстового файла внутреннего генератора таблицы системных параметров.

Рис. 271 Формат текстового файла конфигурации: описания столбцов

```
/ Menu 1 General Setup
 10000000 = Configured                 <0(No)| 1(Yes)>       = 1
 10000001 = System Name                <Str>                 = Prestige
 10000002 = Location                   <Str>                 =
 10000003 = Contact Person's Name      <Str>                 =
 10000004 = Route IP                   <0(No)| 1(Yes)>       = 1
 10000005 = Route IPX                 <0(No)| 1(Yes)>       = 0
 10000006 = Bridge                    <0(No)| 1(Yes)>       = 0
```

ПРИМЕЧАНИЕ: НЕ редактируйте и не удаляйте никакие поля, за исключением параметров в столбце "Input" (Ввод).

Более подробно примеры текстовых файлов представлены в приложении "*Примеры экранных форм внутреннего генератора таблицы системных параметров (SPTGEN)*".

Изменение файла внутреннего генератора таблицы системных параметров — что необходимо запомнить

Каждому вводимому параметру должны предшествовать один знак равенства "=" и один пробел.

Некоторые параметры зависят от других. Например: если отключить поле **Configured (Настроено)** в меню 1 (см. Рис. 271 на с. 487), то необходимо отключить все поля в данном меню.

Если в столбце **Input (Ввод)** введен неверный параметр, то интернет-центр не сохранит параметры, а в командной строке отобразится **Идентификационный номер поля (Field Identification Number)**. На Рис. 272 на с. 487 показан пример сообщения интернет-центра в случае ввода значений, отличных от “0” и “1” в столбце **Input (Ввод)** для **Идентификационного номера поля** 1000000 (см. Рис. 271 на с. 487).

Рис. 272 Введен неверный параметр: пример сообщения в командной строке

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

При вводе *корректных* параметров, интернет-центр отобразит следующую информацию.

Рис. 273 Введен корректный параметр: пример сообщения в командной строке

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Пример скачивания файла внутреннего генератора таблицы системных параметров по протоколу FTP

1. Запустите приложение FTP.
2. Введите "bin". Команда “bin” переключает режим передачи на бинарный.
3. Получите файл "rom-t" (get "rom-t"). Команда “get” копирует файлы из интернет-центра в компьютер. “rom-t” — это имя файла конфигурации интернет-центра.
4. Внесите изменения в файл "rom-t" при помощи текстового редактора (не используйте текстовый процессор). Для того, чтобы отредактировать файл, необходимо выйти из экранной формы FTP.

Рис. 274 Пример скачивания файла внутреннего генератора таблицы системных параметров по протоколу FTP

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-t
ftp>bye
c:\edit rom-t
(edit the rom-t text file by a text editor and save it)
```

ПРИМЕЧАНИЕ: Вы можете переименовать файл “rom-t” при сохранении его на компьютер, но при загрузке в интернет-центр он должен именоваться “rom-t”.

Пример загрузки внутреннего генератора таблицы системных параметров по протоколу FTP

1. Запустите приложение FTP.
2. Введите "bin". Команда “bin” переключает режим передачи на бинарный.
3. При помощи команды “put” загрузите файл “rom-t” с компьютера в интернет-центр.

4 Закройте приложение FTP.

Рис. 275 Пример загрузки внутреннего генератора таблицы системных параметров по протоколу FTP

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye
```

Пример экранных форм внутреннего генератора таблицы системных параметров

В этом разделе описаны экранные формы внутреннего генератора таблицы системных параметров интернет-центра.

Табл. 163 Сокращения, использованные в экранных формах внутреннего генератора таблицы системных параметров

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
FIN	Идентификационный номер поля (не виден в экранных формах SMT)
FN	Имя поля
PVA	Допустимые значения параметров
INPUT	Пример вводимых значений
*	Применимо к модели P–660HT/HTW EE.

Ниже перечислены экранные формы внутреннего генератора таблицы системных параметров, связанные с экранными формами SMT интернет-центра P–660HT/HTW EE.

Табл. 164 Меню 1 Общая настройка (SMT-меню 1)

/ Меню 1 — General Setup (Общая настройка) (SMT-меню 1)			
FIN	FN	PVA	INPUT
10000000 =	Configured (Настроено)	<0(Нет) | 1(Да)>	= 0
10000001 =	System Name (Системное имя)	<строка>	= Prestige
10000002 =	Location (Местонахождение)	<строка>	=
10000003 =	Contact Person's Name (Имя ответственного лица)	<строка>	=

Табл. 164 Меню 1 Общая настройка (SMT-меню 1)

10000004 =	Route IP (Маршрутизация IP)	<0(Нет) | 1(Да)>	= 1
10000006 =	Bridge (Мост)	<0(Нет) | 1(Да)>	= 0

Табл. 165 Меню 3 (SMT-меню 3)

/ Меню 3.1 — General Ethernet Setup (Общая настройка Ethernet) (SMT-меню 3.1)			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1 (Набор входных фильтров протоколов 1)		= 2
30100002 =	Input Protocol filters Set 2 (Набор входных фильтров протоколов 2)		= 256
30100003 =	Input Protocol filters Set 3 (Набор входных фильтров протоколов 3)		= 256
30100004 =	Input Protocol filters Set 4 (Набор входных фильтров протоколов 4)		= 256
30100005 =	Input device filters Set 1 (Набор входных фильтров устройства 1)		= 256
30100006 =	Input device filters Set 2 (Набор входных фильтров устройства 2)		= 256
30100007 =	Input device filters Set 3 (Набор входных фильтров устройства 3)		= 256
30100008 =	Input device filters Set 4 (Набор входных фильтров устройства 4)		= 256
30100009 =	Output protocol filters Set 1 (Набор выходных фильтров протоколов 1)		= 256
30100010 =	Output protocol filters Set 2 (Набор выходных фильтров протоколов 2)		= 256
30100011 =	Output protocol filters Set 3 (Набор выходных фильтров протоколов 3)		= 256
30100012 =	Output protocol filters Set 4 (Набор выходных фильтров протоколов 4)		= 256
30100013 =	Output device filters Set 1 (Набор выходных фильтров устройства 1)		= 256
30100014 =	Output device filters Set 2 (Набор выходных фильтров устройства 2)		= 256
30100015 =	Output device filters Set 3 (Набор выходных фильтров устройства 3)		= 256
30100016 =	Output device filters Set 4 (Набор выходных фильтров устройства 4)		= 256
/ Меню 3.2 — TCP/IP and DHCP Ethernet Setup (Настройка TCP/IP и DHCP Ethernet) (SMT-меню 3.2)			
FIN	FN	PVA	INPUT

Табл. 165 Меню 3 (SMT-меню 3 (продолжение))

30200001 =	DHCP	<0(нет) | 1(сервер) | 2(ретранслятор)>	= 0
30200002 =	Client IP Pool Starting Address (Начальный IP-адрес клиентского диапазона)		= 192.168.1.33
30200003 =	Size of Client IP Pool (Размер диапазона IP-адресов клиентов)		= 32
30200004 =	Primary DNS Server (Основной сервер DNS)		= 0.0.0.0
30200005 =	Secondary DNS Server (Дополнительный сервер DNS)		= 0.0.0.0
30200006 =	Remote DHCP Server (Удаленный сервер DHCP)		= 0.0.0.0
30200008 =	IP Address (IP-адрес)		= 172.21.2.200
30200009 =	IP Subnet Mask (Маска IP подсети)		= 16
30200010 =	RIP Direction (Направление RIP)	<0(нет) | 1(оба) | 2(только вход) | 3(только выход)>	= 0
30200011 =	Version (Версия)	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30200012 =	Multicast (Многоадресная рассылка)	<0(IGMP-v2) | 1(IGMP-v1) | 2(нет)>	= 2
30200013 =	IP Policies Set 1 (Набор политик IP 1) (1~12)		= 256
30200014 =	IP Policies Set 2 (Набор политик IP 2) (1~12)		= 256
30200015 =	IP Policies Set 3 (Набор политик IP 3) (1~12)		= 256
30200016 =	IP Policies Set 4 (Набор политик IP 4) (1~12)		= 256
/ Меню 3.2.1 — IP Alias Setup (Настройка псевдонимов IP) (SMT-меню 3.2.1)			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1 (Псевдоним IP 1)	<0(Нет) | 1(Да)>	= 0
30201002 =	IP Address (IP-адрес)		= 0.0.0.0
30201003 =	IP Subnet Mask (Маска IP подсети)		= 0

Табл. 165 Меню 3 (SMT-меню 3 (продолжение))

30201004 =	RIP Direction (Направление RIP)	<0(нет) | 1(оба) | 2(только вход) | 3(только выход)>	= 0
30201005 =	Version (Версия)	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1 (Псевдоним IP #1 Набор фильтров входных протоколов 1)		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2 (Псевдоним IP #1 Набор фильтров входных протоколов 2)		= 256
30201008 =	IP Alias #1 Incoming protocol filters Set 3 (Псевдоним IP #1 Набор фильтров входных протоколов 3)		= 256
30201009 =	IP Alias #1 Incoming protocol filters Set 4 (Псевдоним IP #1 Набор фильтров входных протоколов 4)		= 256
30201010 =	IP Alias #1 Outgoing protocol filters Set 1 (Псевдоним IP #1 Набор фильтров выходных протоколов 1)		= 256
30201011 =	IP Alias #1 Outgoing protocol filters Set 2 (Псевдоним IP #1 Набор фильтров выходных протоколов 2)		= 256
30201012 =	IP Alias #1 Outgoing protocol filters Set 3 (Псевдоним IP #1 Набор фильтров выходных протоколов 3)		= 256
30201013 =	IP Alias #1 Outgoing protocol filters Set 4 (Псевдоним IP #1 Набор фильтров выходных протоколов 4)		= 256
30201014 =	IP Alias 2 (Псевдоним IP 2) <0(Нет) | 1(Да)>		= 0
30201015 =	IP Address (IP-адрес)		= 0.0.0.0
30201016 =	IP Subnet Mask (Маска IP подсети)		= 0
30201017 =	RIP Direction (Направление RIP)	<0(нет) | 1(оба) | 2(только вход) | 3(только выход)>	= 0
30201018 =	Version (Версия)	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201019 =	IP Alias #2 Incoming protocol filters Set 1 (Псевдоним IP #2 Набор фильтров входных протоколов 1)		= 256

Табл. 165 Меню 3 (SMT-меню 3 (продолжение))

30201020 =	IP Alias #2 Incoming protocol filters Set 2 (Псевдоним IP #2 Набор фильтров входных протоколов 2)		= 256
30201021 =	IP Alias #2 Incoming protocol filters Set 3 (Псевдоним IP #2 Набор фильтров входных протоколов 3)		= 256
30201022 =	IP Alias #2 Incoming protocol filters Set 4 (Псевдоним IP #2 Набор фильтров входных протоколов 4)		= 256
30201023 =	IP Alias #2 Outgoing protocol filters Set 1 (Псевдоним IP #2 Набор фильтров выходных протоколов 1)		= 256
30201024 =	IP Alias #2 Outgoing protocol filters Set 2 (Псевдоним IP #2 Набор фильтров выходных протоколов 2)		= 256
30201025 =	IP Alias #2 Outgoing protocol filters Set 3 (Псевдоним IP #2 Набор фильтров выходных протоколов 3)		= 256
30201026 =	IP Alias #2 Outgoing protocol filters Set 4 (Псевдоним IP #2 Набор фильтров выходных протоколов 4)		= 256
*/ Меню 3.5 — Wireless LAN Setup (Настройка беспроводной локальной сети) (SMT-меню 3.5)			
FIN	FN	PVA	INPUT
30500001 =	ESSID		Wireless (Беспроводная сеть)
30500002 =	Hide ESSID (Скрыть ESSID)	<0(Нет) | 1(Да)>	= 0
30500003 =	Channel ID (Идентификатор канала)	<1|2|3|4|5|6|7|8|9|10|11|12|13>	= 1
30500004 =	RTS Threshold (Порог RTS)	<0 ~ 2432>	= 2432
30500005 =	Frag. Threshold (Порог фрагментации)	<256 ~ 2432>	= 2432
30500006 =	WEP	<0(ОТКЛЮЧ.) | 1(64-разрядное шифрование WEP) | 2(128-разрядное шифрование WEP)>	= 0
30500007 =	Default Key (Ключ по умолчанию)	<1|2|3|4>	= 0
30500008 =	WEP Key1 (Ключ WEP 1)		=
30500009 =	WEP Key2 (Ключ WEP 2)		=
30500010 =	WEP Key3 (Ключ WEP 3)		=
30500011 =	WEP Key4 (Ключ WEP 4)		=
30500012 =	Wlan Active (Беспроводная ЛВС активна)	<0(Отключ.) | 1(Включ.)>	= 0

Табл. 165 Меню 3 (SMT-меню 3 (продолжение))

*/ МЕНЮ 3.5.1 — WLAN MAC ADDRESS FILTER (ФИЛЬТР MAC-АДРЕСОВ БЕСПРОВОДНОЙ ЛВС) (SMT-МЕНЮ 3.5.1)			
FIN	FN	PVA	INPUT
30501001 =	Mac Filter Active (Фильтрация MAC-адресов включена)	<0(Нет) | 1(Да)>	= 0
30501002 =	Filter Action (Действие фильтра)	<0(разрешить) | 1(запретить)>	= 0
30501003 =	Address 1 (Адрес 1)		= 00:00:00:00:00:00
30501004 =	Address 2 (Адрес 2)		= 00:00:00:00:00:00
30501005 =	Address 3 (Адрес 3)		= 00:00:00:00:00:00
Продолжение	…		…
30501034 =	Address 32 (Адрес 32)		= 00:00:00:00:00:00

Табл. 166 Меню 4 — Internet Access Setup (Настройка доступа в Интернет) (SMT-меню 4)

/ Меню 4 — Internet Access Setup (Настройка доступа в Интернет) (SMT-меню 4)			
FIN	FN	PVA	INPUT
40000000 =	Configured (Настроено)	<0(Нет) | 1(Да)>	= 1
40000001 =	ISP (Интернет-провайдер)	<0(Нет) | 1(Да)>	= 1
40000002 =	Active (Активно)	<0(Нет) | 1(Да)>	= 1
40000003 =	ISP's Name (Имя Интернет-провайдера)		= ChangeMe
40000004 =	Encapsulation (Инкапсуляция)	<2(PPPOE) | 3(RFC 1483)| 4(PPPoA)| 5(ENET ENCAP)>	= 2
40000005 =	Multiplexing (Мультиплексирование)	<1(на основе LLC) | 2(на основе VC)	= 1
40000006 =	VPI # (Номер VPI)		= 0
40000007 =	VCI # (Номер VCI)		= 35
40000008 =	Service Name (Имя службы)	<строка>	= любое

Табл. 166 Меню 4 — Internet Access Setup (Настройка доступа в Интернет) (SMT-меню 4)

40000009 =	My Login (Имя пользователя)	<строка>	= test@pqa
40000010 =	My Password (Пароль)	<строка>	= 1234
40000011 =	Single User Account (Режим одной учетной записи)	<0(Нет) | 1(Да)>	= 1
40000012 =	IP Address Assignment (Назначение IP-адреса)	<0(статический)|1(динамический)>	= 1
40000013 =	IP Address (IP-адрес)		= 0.0.0.0
40000014 =	Remote IP address (Удаленный IP-адрес)		= 0.0.0.0
40000015 =	Remote IP Subnet Mask (Маска IP подсети удаленного узла)		= 0
40000016 =	ISP incoming protocol filter set 1 (Набор фильтров входного протокола интернет-провайдера 1)		= 6
40000017 =	ISP incoming protocol filter set 2 (Набор фильтров входного протокола интернет-провайдера 2)		= 256
40000018 =	ISP incoming protocol filter set 3 (Набор фильтров входного протокола интернет-провайдера 3)		= 256
40000019 =	ISP incoming protocol filter set 4 (Набор фильтров входного протокола интернет-провайдера 4)		= 256
40000020 =	ISP outgoing protocol filter set 1 (Набор фильтров выходного протокола интернет-провайдера 1)		= 256
40000021 =	ISP outgoing protocol filter set 2 (Набор фильтров выходного протокола интернет-провайдера 2)		= 256
40000022 =	ISP outgoing protocol filter set 3 (Набор фильтров выходного протокола интернет-провайдера 3)		= 256
40000023 =	ISP outgoing protocol filter set 4 (Набор фильтров выходного протокола интернет-провайдера 4)		= 256
40000024 =	ISP PPPoE idle timeout (Максимальное время простоя при соединении с провайдером по протоколу PPPoE)		= 0
40000025 =	Route IP (Маршрутизация IP)	<0(Нет) | 1(Да)>	= 1
40000026 =	Bridge (Мост)	<0(Нет) | 1(Да)>	= 0
40000027 =	ATM QoS Type (Тип качества обслуживания ATM)	<0(CBR) | 1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR) (Пиковая скорость ячеек)		= 0

Табл. 166 Меню 4 — Internet Access Setup (Настройка доступа в Интернет) (SMT-меню 4)

40000029 =	Sustain Cell Rate (SCR) (Поддерживаемая скорость ячеек)		= 0
40000030 =	Maximum Burst Size(MBS) (Максимальный размер пакета)		= 0
40000031=	RIP Direction (Направление RIP)	<0(нет) | 1(оба) | 2(только вход) | 3(только выход)>	= 0
40000032=	RIP Version (Версия RIP)	<0(Rip-1) | 1(Rip-2B) | 2(Rip-2M)>	= 0
40000033=	Nailed-up Connection (Постоянное соединение)	<0(Нет) | 1(Да)>	= 0

Табл. 167 Меню 12 (SMT-меню 12)

/ Меню 12.1.1 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.1)			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name (Набор статических маршрутов IP #1, имя)	<строка>	=
120101002 =	IP Static Route set #1, Active (Набор статических маршрутов IP #1, активный)	<0(Нет) | 1(Да)>	= 0
120101003 =	IP Static Route set #1, Destination IP address (Набор статических маршрутов IP #1, IP-адрес получателя)		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask (Набор статических маршрутов IP #1, маска IP подсети получателя)		= 0
120101005 =	IP Static Route set #1, Gateway (Набор статических маршрутов IP #1, шлюз)		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric (Набор статических маршрутов IP #1, метрика)		= 0
120101007 =	IP Static Route set #1, Private (Набор статических маршрутов IP #1, частный)	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.2 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.2)			
FIN	FN	PVA	INPUT
120102001 =	IP Static Route set #2, Name (Набор статических маршрутов IP #2, имя)		=

Табл. 167 Меню 12 (SMT-меню 12) (продолжение)

120102002 =	IP Static Route set #2, Active (Набор статических маршрутов IP #2, активный)	<0(Нет) | 1(Да)>	= 0
120102003 =	IP Static Route set #2, Destination IP address (Набор статических маршрутов IP #2, IP-адрес получателя)		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask (Набор статических маршрутов IP #2, маска IP подсети получателя)		= 0
120102005 =	IP Static Route set #2, Gateway (Набор статических маршрутов IP #2, шлюз)		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric (Набор статических маршрутов IP #2, метрика)		= 0
120102007 =	IP Static Route set #2, Private (Набор статических маршрутов IP #2, частный)	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.3 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.3)			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name (Набор статических маршрутов IP #3, имя)	<строка>	=
120103002 =	IP Static Route set #3, Active (Набор статических маршрутов IP #3, активный)	<0(Нет) | 1(Да)>	= 0
120103003 =	IP Static Route set #3, Destination IP address (Набор статических маршрутов IP #3, IP-адрес получателя)		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask (Набор статических маршрутов IP #3, маска IP подсети получателя)		= 0
120103005 =	IP Static Route set #3, Gateway (Набор статических маршрутов IP #3, шлюз)		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric (Набор статических маршрутов IP #3, метрика)		= 0
120103007 =	IP Static Route set #3, Private (Набор статических маршрутов IP #3, частный)	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.4 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.4)			
FIN	FN	PVA	INPUT

Табл. 167 Меню 12 (SMT-меню 12) (продолжение)

120104001 =	IP Static Route set #4, Name (Набор статических маршрутов IP #4, имя)	<строка>	=
120104002 =	IP Static Route set #4, Active (Набор статических маршрутов IP #4, активный)	<0(Нет) | 1(Да)>	= 0
120104003 =	IP Static Route set #4, Destination IP address (Набор статических маршрутов IP #4, IP-адрес получателя)		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask (Набор статических маршрутов IP #4, маска IP подсети получателя)		= 0
120104005 =	IP Static Route set #4, Gateway (Набор статических маршрутов IP #4, шлюз)		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric (Набор статических маршрутов IP #4, метрика)		= 0
120104007 =	IP Static Route set #4, Private (Набор статических маршрутов IP #4, частный)	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.5 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.5)			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name (Набор статических маршрутов IP #5, имя)	<строка>	=
120105002 =	IP Static Route set #5, Active (Набор статических маршрутов IP #5, активный)	<0(Нет) | 1(Да)>	= 0
120105003 =	IP Static Route set #5, Destination IP address (Набор статических маршрутов IP #5, IP-адрес получателя)		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask (Набор статических маршрутов IP #5, маска IP подсети получателя)		= 0
120105005 =	IP Static Route set #5, Gateway (Набор статических маршрутов IP #5, шлюз)		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric (Набор статических маршрутов IP #5, метрика)		= 0
120105007 =	IP Static Route set #5, Private (Набор статических маршрутов IP #5, частный)	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.6 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.6)			

Табл. 167 Меню 12 (SMT-меню 12) (продолжение)

FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name (Набор статических маршрутов IP #6, имя)	<строка>	=
120106002 =	IP Static Route set #6, Active (Набор статических маршрутов IP #6, активный)	<0(Нет) | 1(Да)>	= 0
120106003 =	IP Static Route set #6, Destination IP address (Набор статических маршрутов IP #6, IP-адрес получателя)		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask (Набор статических маршрутов IP #6, маска IP подсети получателя)		= 0
120106005 =	IP Static Route set #6, Gateway (Набор статических маршрутов IP #6, шлюз)		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric (Набор статических маршрутов IP #6, метрика)		= 0
120106007 =	IP Static Route set #6, Private (Набор статических маршрутов IP #6, частный)	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.7 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.7)			
FIN	FN	PVA	INPUT
120107001 =	IP Static Route set #7, Name (Набор статических маршрутов IP #7, имя)	<строка>	=
120107002 =	IP Static Route set #7, Active (Набор статических маршрутов IP #7, активный)	<0(Нет) | 1(Да)>	= 0
120107003 =	IP Static Route set #7, Destination IP address (Набор статических маршрутов IP #7, IP-адрес получателя)		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask (Набор статических маршрутов IP #7, маска IP подсети получателя)		= 0
120107005 =	IP Static Route set #7, Gateway (Набор статических маршрутов IP #7, шлюз)		= 0.0.0.0
120107006 =	IP Static Route set #7, Metric (Набор статических маршрутов IP #7, метрика)		= 0
120107007 =	IP Static Route set #7, Private (Набор статических маршрутов IP #7, частный)	<0(Нет) | 1(Да)>	= 0

Табл. 167 Меню 12 (SMT-меню 12) (продолжение)

/ Меню 12.1.8 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.8)			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name (Набор статических маршрутов IP #8, имя)	<строка>	=
120108002 =	IP Static Route set #8, Active (Набор статических маршрутов IP #8, активный)	<0(Нет) | 1(Да)>	= 0
120108003 =	IP Static Route set #8, Destination IP address (Набор статических маршрутов IP #8, IP-адрес получателя)		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask (Набор статических маршрутов IP #8, маска IP подсети получателя)		= 0
120108005 =	IP Static Route set #8, Gateway (Набор статических маршрутов IP #8, шлюз)		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric (Набор статических маршрутов IP #8, метрика)		= 0
120108007 =	IP Static Route set #8, Private (Набор статических маршрутов IP #8, частный)	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.9 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.9)			
FIN	FN	PVA	INPUT
120109001 =	IP Static Route set #9, Name (Набор статических маршрутов IP #9, имя)	<строка>	=
120109002 =	IP Static Route set #9, Active (Набор статических маршрутов IP #9, активный)	<0(Нет) | 1(Да)>	= 0
120109003 =	IP Static Route set #9, Destination IP address (Набор статических маршрутов IP #9, IP-адрес получателя)		= 0.0.0.0
120109004 =	IP Static Route set #9, Destination IP subnetmask (Набор статических маршрутов IP #9, маска IP подсети получателя)		= 0
120109005 =	IP Static Route set #9, Gateway (Набор статических маршрутов IP #9, шлюз)		= 0.0.0.0
120109006 =	IP Static Route set #9, Metric (Набор статических маршрутов IP #9, метрика)		= 0

Табл. 167 Меню 12 (SMT-меню 12) (продолжение)

120109007 =	IP Static Route set #9, Private (Набор статических маршрутов IP #9, частный)	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.10 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.10)			
FIN	FN	PVA	INPUT
120110001 =	IP Static Route set #10, Name (Набор статических маршрутов IP #10, имя)		=
120110002 =	IP Static Route set #10, Active (Набор статических маршрутов IP #10, активный)	<0(Нет) | 1(Да)>	= 0
120110003 =	IP Static Route set #10, Destination IP address (Набор статических маршрутов IP #10, IP-адрес получателя)		= 0.0.0.0
120110004 =	IP Static Route set #10, Destination IP subnetmask (Набор статических маршрутов IP #10, маска IP подсети получателя)		= 0
120110005 =	IP Static Route set #10, Gateway (Набор статических маршрутов IP #10, шлюз)		= 0.0.0.0
120110006 =	IP Static Route set #10, Metric (Набор статических маршрутов IP #10, метрика)		= 0
120110007 =	IP Static Route set #10, Private (Набор статических маршрутов IP #10, частный)	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.11 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.11)			
FIN	FN	PVA	INPUT
120111001 =	IP Static Route set #11, Name (Набор статических маршрутов IP #11, имя)	<строка>	=
120111002 =	IP Static Route set #11, Active (Набор статических маршрутов IP #11, активный)	<0(Нет) | 1(Да)>	= 0
120111003 =	IP Static Route set #11, Destination IP address (Набор статических маршрутов IP #11, IP-адрес получателя)		= 0.0.0.0
120111004 =	IP Static Route set #11, Destination IP subnetmask (Набор статических маршрутов IP #11, маска IP подсети получателя)		= 0
120111005 =	IP Static Route set #11, Gateway (Набор статических маршрутов IP #11, шлюз)		= 0.0.0.0

Табл. 167 Меню 12 (SMT-меню 12) (продолжение)

120111006 =	IP Static Route set #11, Metric (Набор статических маршрутов IP #11, метрика)		= 0
120111007 =	IP Static Route set #11, Private (Набор статических маршрутов IP #11, частный)	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.12 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.12)			
FIN	FN	PVA	INPUT
120112001 =	IP Static Route set #12, Name (Набор статических маршрутов IP #12, имя)	<строка>	=
120112002 =	IP Static Route set #12, Active (Набор статических маршрутов IP #12, активный)	<0(Нет) | 1(Да)>	= 0
120112003 =	IP Static Route set #12, Destination IP address (Набор статических маршрутов IP #12, IP-адрес получателя)		= 0.0.0.0
120112004 =	IP Static Route set #12, Destination IP subnetmask (Набор статических маршрутов IP #12, маска IP подсети получателя)		= 0
120112005 =	IP Static Route set #12, Gateway (Набор статических маршрутов IP #12, шлюз)		= 0.0.0.0
120112006 =	IP Static Route set #12, Metric (Набор статических маршрутов IP #12, метрика)		= 0
120112007 =	IP Static Route set #12, Private (Набор статических маршрутов IP #12, частный)	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.13 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1.13)			
FIN	FN	PVA	INPUT
120113001 =	IP Static Route set #13, Name (Набор статических маршрутов IP #13, имя)	<строка>	=
120113002 =	IP Static Route set #13, Active (Набор статических маршрутов IP #13, активный)	<0(Нет) | 1(Да)>	= 0
120113003 =	IP Static Route set #13, Destination IP address (Набор статических маршрутов IP #13, IP-адрес получателя)		= 0.0.0.0
120113004 =	IP Static Route set #13, Destination IP subnetmask (Набор статических маршрутов IP #13, маска IP подсети получателя)		= 0

Табл. 167 Меню 12 (SMT-меню 12) (продолжение)

120113005 =	IP Static Route set #13, Gateway (Набор статических маршрутов IP #13, шлюз)		= 0.0.0.0
120113006 =	IP Static Route set #13, Metric (Набор статических маршрутов IP #13, метрика)		= 0
120113007 =	IP Static Route set #13, Private (Набор статических маршрутов IP #13, частный)	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.14 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1. 14)			
FIN	FN	PVA	INPUT
120114001 =	IP Static Route set #14, Name (Набор статических маршрутов IP #14, имя)	<строка>	=
120114002 =	IP Static Route set #14, Active (Набор статических маршрутов IP #14, активный)	<0(Нет) | 1(Да)>	= 0
120114003 =	IP Static Route set #14, Destination IP address (Набор статических маршрутов IP #14, IP-адрес получателя)		= 0.0.0.0
120114004 =	IP Static Route set #14, Destination IP subnetmask (Набор статических маршрутов IP #14, маска IP подсети получателя)		= 0
120114005 =	IP Static Route set #14, Gateway (Набор статических маршрутов IP #14, шлюз)		= 0.0.0.0
120114006 =	IP Static Route set #14, Metric (Набор статических маршрутов IP #14, метрика)		= 0
120114007 =	IP Static Route set #14, Private (Набор статических маршрутов IP #14, частный)	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.15 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1. 15)			
FIN	FN	PVA	INPUT
120115001 =	IP Static Route set #15, Name (Набор статических маршрутов IP #15, имя)	<строка>	=
120115002 =	IP Static Route set #15, Active (Набор статических маршрутов IP #15, активный)	<0(Нет) | 1(Да)>	= 0
120115003 =	IP Static Route set #15, Destination IP address (Набор статических маршрутов IP #15, IP-адрес получателя)		= 0.0.0.0

Табл. 167 Меню 12 (SMT-меню 12) (продолжение)

120115004 =	IP Static Route set #15, Destination IP subnetmask (Набор статических маршрутов IP #15, маска IP подсети получателя)		= 0
120115005 =	IP Static Route set #15, Gateway (Набор статических маршрутов IP #15, шлюз)		= 0.0.0.0
120115006 =	IP Static Route set #15, Metric (Набор статических маршрутов IP #15, метрика)		= 0
120115007 =	IP Static Route set #15, Private (Набор статических маршрутов IP #15, частный)	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.16 — IP Static Route Setup (Настройка статических маршрутов IP) (SMT-меню 12.1. 16)			
FIN	FN	PVA	INPUT
120116001 =	IP Static Route set #16, Name (Набор статических маршрутов IP #16, имя)	<строка>	=
120116002 =	IP Static Route set #16, Active (Набор статических маршрутов IP #16, активный)	<0(Нет) | 1(Да)>	= 0
120116003 =	IP Static Route set #16, Destination IP address (Набор статических маршрутов IP #16, IP-адрес получателя)		= 0.0.0.0
120116004 =	IP Static Route set #16, Destination IP subnetmask (Набор статических маршрутов IP #16, маска IP подсети получателя)		= 0
120116005 =	IP Static Route set #16, Gateway (Набор статических маршрутов IP #16, шлюз)		= 0.0.0.0
120116006 =	IP Static Route set #16, Metric (Набор статических маршрутов IP #16, метрика)		= 0
120116007 =	IP Static Route set #16, Private (Набор статических маршрутов IP #16, частный)	<0(Нет) | 1(Да)>	= 0

Табл. 168 Меню 15 — SUA Server Setup (Настройка сервера SUA) (SMT-меню 15)

/ Меню 15 — SUA Server Setup (Настройка сервера SUA) (SMT-меню 15)			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port (IP-адрес сервера SUA для порта по умолчанию)		= 0.0.0.0

Табл. 168 Меню 15 — SUA Server Setup (Настройка сервера SUA) (SMT-меню 15) (продолжение)

150000002 =	SUA Server #2 Active (Сервер SUA #2, активный)	<0(Нет) | 1(Да)>	= 0
150000003 =	SUA Server #2 Protocol (Сервер SUA #2, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000004 =	SUA Server #2 Port Start (Сервер SUA #2, начальный порт)		= 0
150000005 =	SUA Server #2 Port End (Сервер SUA #2, конечный порт)		= 0
150000006 =	SUA Server #2 Local IP address (Локальный IP-адрес сервера SUA #2)		= 0.0.0.0
150000007 =	SUA Server #3 Active (Сервер SUA #3, активный)	<0(Нет) | 1(Да)>	= 0
150000008 =	SUA Server #3 Protocol (Сервер SUA #3, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000009 =	SUA Server #3 Port Start (Сервер SUA #3, начальный порт)		= 0
150000010 =	SUA Server #3 Port End (Сервер SUA #3, конечный порт)		= 0
150000011 =	SUA Server #3 Local IP address (Локальный IP-адрес сервера SUA #3)		= 0.0.0.0
150000012 =	SUA Server #4 Active (Сервер SUA #4, активный)	<0(Нет) | 1(Да)>	= 0
150000013 =	SUA Server #4 Protocol (Сервер SUA #4, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000014 =	SUA Server #4 Port Start (Сервер SUA #4, начальный порт)		= 0
150000015 =	SUA Server #4 Port End (Сервер SUA #4, конечный порт)		= 0
150000016 =	SUA Server #4 Local IP address (Локальный IP-адрес сервера SUA #4)		= 0.0.0.0
150000017 =	SUA Server #5 Active (Сервер SUA #5, активный)	<0(Нет) | 1(Да)>	= 0
150000018 =	SUA Server #5 Protocol (Сервер SUA #5, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000019 =	SUA Server #5 Port Start (Сервер SUA #5, начальный порт)		= 0
150000020 =	SUA Server #5 Port End (Сервер SUA #5, конечный порт)		= 0
150000021 =	SUA Server #5 Local IP address (Локальный IP-адрес сервера SUA #5)		= 0.0.0.0
150000022 =	SUA Server #6 Active (Сервер SUA #6, активный)	<0(Нет) | 1(Да)> = 0	= 0
150000023 =	SUA Server #6 Protocol (Сервер SUA #6, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000024 =	SUA Server #6 Port Start (Сервер SUA #6, начальный порт)		= 0

Табл. 168 Меню 15 — SUA Server Setup (Настройка сервера SUA) (SMT-меню 15) (продолжение)

150000025 =	SUA Server #6 Port End (Сервер SUA #6, конечный порт)		= 0
150000026 =	SUA Server #6 Local IP address (Локальный IP-адрес сервера SUA #6)		= 0.0.0.0
150000027 =	SUA Server #7 Active (Сервер SUA #7, активный)	<0(Нет) | 1(Да)>	= 0
150000028 =	SUA Server #7 Protocol (Сервер SUA #7, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start (Сервер SUA #7, начальный порт)		= 0
150000030 =	SUA Server #7 Port End (Сервер SUA #7, конечный порт)		= 0
150000031 =	SUA Server #7 Local IP address (Локальный IP-адрес сервера SUA #7)		= 0.0.0.0
150000032 =	SUA Server #8 Active (Сервер SUA #8, активный)	<0(Нет) | 1(Да)>	= 0
150000033 =	SUA Server #8 Protocol (Сервер SUA #8, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000034 =	SUA Server #8 Port Start (Сервер SUA #8, начальный порт)		= 0
150000035 =	SUA Server #8 Port End (Сервер SUA #8, конечный порт)		= 0
150000036 =	SUA Server #8 Local IP address (Локальный IP-адрес сервера SUA #8)		= 0.0.0.0
150000037 =	SUA Server #9 Active (Сервер SUA #9, активный)	<0(Нет) | 1(Да)>	= 0
150000038 =	SUA Server #9 Protocol (Сервер SUA #9, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000039 =	SUA Server #9 Port Start (Сервер SUA #9, начальный порт)		= 0
150000040 =	SUA Server #9 Port End (Сервер SUA #9, конечный порт)		= 0
150000041 =	SUA Server #9 Local IP address (Локальный IP-адрес сервера SUA #9)		= 0.0.0.0
150000042	SUA Server #10 Active (Сервер SUA #10, активный)	<0(Нет) | 1(Да)>	= 0
150000043 =	SUA Server #10 Protocol (Сервер SUA #10, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000044 =	SUA Server #10 Port Start (Сервер SUA #10, начальный порт)		= 0
150000045 =	SUA Server #10 Port End (Сервер SUA #10, конечный порт)		= 0
150000046 =	SUA Server #10 Local IP address (Локальный IP-адрес сервера SUA #10)		= 0.0.0.0
150000047 =	SUA Server #11 Active (Сервер SUA #11, активный)	<0(Нет) | 1(Да)>	= 0

Табл. 168 Меню 15 — SUA Server Setup (Настройка сервера SUA) (SMT-меню 15) (продолжение)

150000048 =	SUA Server #11 Protocol (Сервер SUA #11, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000049 =	SUA Server #11 Port Start (Сервер SUA #11, начальный порт)		= 0
150000050 =	SUA Server #11 Port End (Сервер SUA #11, конечный порт)		= 0
150000051 =	SUA Server #11 Local IP address (Локальный IP-адрес сервера SUA #11)		= 0.0.0.0
150000052 =	SUA Server #12 Active (Сервер SUA #12, активный)	<0(Нет) | 1(Да)>	= 0
150000053 =	SUA Server #12 Protocol (Сервер SUA #12, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000054 =	SUA Server #12 Port Start (Сервер SUA #12, начальный порт)		= 0
150000055 =	SUA Server #12 Port End (Сервер SUA #12, конечный порт)		= 0
150000056 =	SUA Server #12 Local IP address (Локальный IP-адрес сервера SUA #12)		= 0.0.0.0

Табл. 169 Меню 21.1 — Filter set #1 (Набор фильтров #1) (SMT-меню 21.1)

/ Меню 21 — Filter set #1 (Набор фильтров #1) (SMT-меню 21)			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name (Набор фильтров 1, Имя)	<строка>	=
/ Меню 21.1.1.1 — Set #1, rule #1 (Набор #1, правило #1) (SMT-меню 21.1.1.1)			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1,Rule 1 Type (Набор фильтров IP 1, правило 1, тип)	<2(TCP/IP)>	= 2
210101002 =	IP Filter Set 1,Rule 1 Active (Набор фильтров IP 1, правило 1 активно)	<0(Нет) | 1(Да)>	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol (Набор фильтров IP 1, правило 1, протокол)		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address (Набор фильтров IP 1, правило 1, IP-адрес получателя)		= 0.0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask (Набор фильтров IP 1, правило 1, маска подсети получателя)		= 0
210101006 =	IP Filter Set 1,Rule 1 Dest Port (Набор фильтров IP 1, правило 1, порт получателя)		= 137

Табл. 169 Меню 21.1 — Filter set #1 (Набор фильтров #1) (SMT-меню 21.1) (продолжение)

210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp (Набор фильтров IP 1, правило 1, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address (Набор фильтров IP 1, правило 1, IP-адрес отправителя)		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask (Набор фильтров IP 1, правило 1, маска подсети отправителя)		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port (Набор фильтров IP 1, правило 1, порт отправителя)		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp (Набор фильтров IP 1, правило 1, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match (Набор фильтров IP 1, правило 1, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match (Набор фильтров IP 1, правило 1, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.1.2 — Set #1, rule #2 (Набор #1, правило #2) (SMT-меню 21.1.1.2)			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type (Набор фильтров IP 1, правило 2, тип)	<2(TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active (Набор фильтров IP 1, правило 2 активно)	<0(Нет) | 1(Да)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol (Набор фильтров IP 1, правило 2, протокол)		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address (Набор фильтров IP 1, правило 2, IP-адрес получателя)		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask (Набор фильтров IP 1, правило 2, маска подсети получателя)		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port (Набор фильтров IP 1, правило 2, порт получателя)		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp (Набор фильтров IP 1, правило 2, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1

Табл. 169 Меню 21.1 — Filter set #1 (Набор фильтров #1) (SMT-меню 21.1) (продолжение)

210102008 =	IP Filter Set 1,Rule 2 Src IP address (Набор фильтров IP 1, правило 2, IP-адрес отправителя)		= 0.0.0.0
210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask (Набор фильтров IP 1, правило 2, маска подсети отправителя)		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port (Набор фильтров IP 1, правило 2, порт отправителя)		= 0
210102011 =	IP Filter Set 1,Rule 2 Src Port Comp (Набор фильтров IP 1, правило 2, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match (Набор фильтров IP 1, правило 2, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match (Набор фильтров IP 1, правило 5, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.1.3 — Set #1, rule #3 (Набор #1, правило #3) (SMT-меню 21.1.1.3)			
FIN	FN	PVA	INPUT
210103001 =	IP Filter Set 1,Rule 3 Type (Набор фильтров IP 1, правило 3, тип)	<2(TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active (Набор фильтров IP 1, правило 3 активно)	<0(Нет) | 1(Да)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol (Набор фильтров IP 1, правило 3, протокол)		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address (Набор фильтров IP 1, правило 3, IP-адрес получателя)		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask (Набор фильтров IP 1, правило 3, маска подсети получателя)		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port (Набор фильтров IP 1, правило 3, порт получателя)		= 139
210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp (Набор фильтров IP 1, правило 3, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address (Набор фильтров IP 1, правило 3, IP-адрес отправителя)		= 0.0.0.0

Табл. 169 Меню 21.1 — Filter set #1 (Набор фильтров #1) (SMT-меню 21.1) (продолжение)

210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask (Набор фильтров IP 1, правило 3, маска подсети отправителя)		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port (Набор фильтров IP 1, правило 3, порт отправителя)		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp (Набор фильтров IP 1, правило 3, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210103013 =	IP Filter Set 1,Rule 3 Act Match (Набор фильтров IP 1, правило 3, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210103014 =	IP Filter Set 1,Rule 3 Act Not Match (Набор фильтров IP 1, правило 3, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.1.4 — Set #1, rule #4 (Набор #1, правило #4) (SMT-меню 21.1.1.4)			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type (Набор фильтров IP 1, правило 3, тип)	<2(TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active (Набор фильтров IP 1, правило 1 активно)	<0(Нет) | 1(Да)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol (Набор фильтров IP 1, правило 4, протокол)		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address (Набор фильтров IP 1, правило 4, IP-адрес получателя)		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask (Набор фильтров IP 1, правило 4, маска подсети получателя)		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port (Набор фильтров IP 1, правило 4, порт получателя)		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp (Набор фильтров IP 1, правило 4, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address (Набор фильтров IP 1, правило 4, IP-адрес отправителя)		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask (Набор фильтров IP 1, правило 4, маска подсети отправителя)		= 0

Табл. 169 Меню 21.1 — Filter set #1 (Набор фильтров #1) (SMT-меню 21.1) (продолжение)

210104010 =	IP Filter Set 1,Rule 4 Src Port (Набор фильтров IP 1, правило 4, порт отправителя)		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp (Набор фильтров IP 1, правило 4, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match (Набор фильтров IP 1, правило 4, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match (Набор фильтров IP 1, правило 4, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.1.5 — Set #1, rule #5 (Набор #1, правило #5) (SMT-меню 21.1.1.5)			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type (Набор фильтров IP 1, правило 5, тип)	<2(TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active (Набор фильтров IP 1, правило 5 активно)	<0(Нет) | 1(Да)>	= 1
210105003 =	IP Filter Set 1,Rule 5 Protocol (Набор фильтров IP 1, правило 5, протокол)		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address (Набор фильтров IP 1, правило 5, IP-адрес получателя)		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask (Набор фильтров IP 1, правило 5, маска подсети получателя)		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port (Набор фильтров IP 1, правило 5, порт получателя)		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp (Набор фильтров IP 1, правило 5, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP address (Набор фильтров IP 1, правило 5, IP-адрес отправителя)		= 0.0.0.0
210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask (Набор фильтров IP 1, правило 5, маска подсети отправителя)		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port (Набор фильтров IP 1, правило 5, порт отправителя)		= 0

Табл. 169 Меню 21.1 — Filter set #1 (Набор фильтров #1) (SMT-меню 21.1) (продолжение)

210105011 =	IP Filter Set 1,Rule 5 Src Port Comp (Набор фильтров IP 1, правило 5, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match (Набор фильтров IP 1, правило 5, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match (Набор фильтров IP 1, правило 5, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.1.6 — Set #1, rule #6 (Набор #1, правило #6) (SMT-меню 21.1.1.6)			
FIN	FN	PVA	INPUT
210106001 =	IP Filter Set 1,Rule 6 Type (Набор фильтров IP 1, правило 6, тип)	<2(TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active (Набор фильтров IP 1, правило 6 активно)	<0(Нет) | 1(Да)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol (Набор фильтров IP 1, правило 6, протокол)		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address (Набор фильтров IP 1, правило 6, IP-адрес получателя)		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask (Набор фильтров IP 1, правило 6, маска подсети получателя)		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port (Набор фильтров IP 1, правило 6, порт получателя)		= 139
210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp (Набор фильтров IP 1, правило 6, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address (Набор фильтров IP 1, правило 6, IP-адрес отправителя)		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask (Набор фильтров IP 1, правило 6, маска подсети отправителя)		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port (Набор фильтров IP 1, правило 6, порт отправителя)		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp (Набор фильтров IP 1, правило 6, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0

Табл. 169 Меню 21.1 — Filter set #1 (Набор фильтров #1) (SMT-меню 21.1) (продолжение)

210106013 =	IP Filter Set 1,Rule 6 Act Match (Набор фильтров IP 1, правило 6, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match (Набор фильтров IP 1, правило 6, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 2

Табл. 170 Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1)

/ Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1)			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam (Набор фильтров 2, Имя)	<строка>	= NetBIOS_WAN
/ Меню 21.1.2.1 — Filter set #2, rule #1 (Набор фильтров #2, правило #1) (SMT-меню 21.1.2.1)			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2,Rule 1 Type (Набор фильтров IP 2, правило 1, тип)	<0(нет) | 2(TCP/IP)>	= 2
210201002 =	IP Filter Set 2,Rule 1 Active (Набор фильтров IP 2, правило 1 активно)	<0(Нет) | 1(Да)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol (Набор фильтров IP 2, правило 1, протокол)		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address (Набор фильтров IP 2, правило 1, IP-адрес получателя)		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask (Набор фильтров IP 2, правило 1, маска подсети получателя)		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port (Набор фильтров IP 2, правило 1, порт получателя)		= 137
210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp (Набор фильтров IP 2, правило 1, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210201008 =	IP Filter Set 2,Rule 1 Src IP address (Набор фильтров IP 2, правило 1, IP-адрес отправителя)		= 0.0.0.0
210201009 =	IP Filter Set 2,Rule 1 Src Subnet Mask (Набор фильтров IP 2, правило 1, маска подсети отправителя)		= 0

Табл. 170 Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1) (продолжение)

210201010 =	IP Filter Set 2, Rule 1 Src Port (Набор фильтров IP 2, правило 1, порт отправителя)		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp (Набор фильтров IP 2, правило 1, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match (Набор фильтров IP 2, правило 1, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210201014 =	IP Filter Set 2, Rule 1 Act Not Match (Набор фильтров IP 2, правило 1, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.2.2 — Filter set #2, rule #2 (Набор фильтров #2, правило #2) (SMT-меню 21.1.2.2)			
FIN	FN	PVA	INPUT
210202001 =	IP Filter Set 2, Rule 2 Type (Набор фильтров IP 2, правило 2, тип)	<0(нет)| 2(TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active (Набор фильтров IP 2, правило 2 активно)	<0(Нет) | 1(Да)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol (Набор фильтров IP 2, правило 2, протокол)		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address (Набор фильтров IP 2, правило 2, IP-адрес получателя)		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask (Набор фильтров IP 2, правило 2, маска подсети получателя)		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port (Набор фильтров IP 2, правило 2, порт получателя)		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp (Набор фильтров IP 2, правило 2, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address (Набор фильтров IP 2, правило 2, IP-адрес отправителя)		= 0.0.0.0
210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask (Набор фильтров IP 2, правило 2, маска подсети отправителя)		= 0
210202010 =	IP Filter Set 2, Rule 2 Src Port (Набор фильтров IP 2, правило 2, порт отправителя)		= 0

Табл. 170 Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1) (продолжение)

210202011 =	IP Filter Set 2, Rule 2 Src Port Comp (Набор фильтров IP 2, правило 2, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match (Набор фильтров IP 2, правило 2, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210202014 =	IP Filter Set 2, Rule 2 Act Not Match (Набор фильтров IP 2, правило 2, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.2.3 — Filter set #2, rule #3 (Набор фильтров #2, правило #3) (SMT-меню 21.1.2.3)			
FIN	FN	PVA	INPUT
210203001 =	IP Filter Set 2, Rule 3 Type (Набор фильтров IP 2, правило 3, тип)	<0(нет) | 2(TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active (Набор фильтров IP 2, правило 3 активно)	<0(Нет) | 1(Да)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol (Набор фильтров IP 2, правило 3, протокол)		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address (Набор фильтров IP 2, правило 3, IP-адрес получателя)		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask (Набор фильтров IP 2, правило 3, маска подсети получателя)		= 0
210203006 =	IP Filter Set 2, Rule 3 Dest Port (Набор фильтров IP 2, правило 3, порт получателя)		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp (Набор фильтров IP 2, правило 3, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address (Набор фильтров IP 2, правило 3, IP-адрес отправителя)		= 0.0.0.0
210203009 =	IP Filter Set 2, Rule 3 Src Subnet Mask (Набор фильтров IP 2, правило 3, маска подсети отправителя)		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port (Набор фильтров IP 2, правило 3, порт отправителя)		= 0
210203011 =	IP Filter Set 2, Rule 3 Src Port Comp (Набор фильтров IP 2, правило 3, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0

Табл. 170 Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1) (продолжение)

210203013 =	IP Filter Set 2, Rule 3 Act Match (Набор фильтров IP 2, правило 3, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210203014 =	IP Filter Set 2, Rule 3 Act Not Match (Набор фильтров IP 2, правило 3, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.2.4 — Filter set #2, rule #4 (Набор фильтров #2, правило #4) (SMT-меню 21.1.2.4)			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type (Набор фильтров IP 2, правило 4, тип)	<0(нет) | 2(TCP/IP)>	= 2
210204002 =	IP Filter Set 2, Rule 4 Active (Набор фильтров IP 2, правило 4 активно)		<0(Нет) | 1(Да)> = 1
210204003 =	IP Filter Set 2, Rule 4 Protocol (Набор фильтров IP 2, правило 4, протокол)		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address (Набор фильтров IP 2, правило 4, IP-адрес получателя)		= 0.0.0.0
210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask (Набор фильтров IP 2, правило 4, маска подсети получателя)		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port (Набор фильтров IP 2, правило 4, порт получателя)		= 137
210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp (Набор фильтров IP 2, правило 4, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address (Набор фильтров IP 2, правило 4, IP-адрес отправителя)		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask (Набор фильтров IP 2, правило 4, маска подсети отправителя)		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port (Набор фильтров IP 2, правило 4, порт отправителя)		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp (Набор фильтров IP 2, правило 4, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210204013 =	IP Filter Set 2, Rule 4 Act Match (Набор фильтров IP 2, правило 4, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3

Табл. 170 Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1) (продолжение)

210204014 =	IP Filter Set 2, Rule 4 Act Not Match (Набор фильтров IP 2, правило 4, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.2.5 — Filter set #2, rule #5 (Набор фильтров #2, правило #5) (SMT-меню 21.1.2.5)			
FIN	FN	PVA	INPUT
210205001 =	IP Filter Set 2, Rule 5 Type (Набор фильтров IP 2, правило 5, тип)	<0(нет) | 2(TCP/IP)>	= 2
210205002 =	IP Filter Set 2, Rule 5 Active (Набор фильтров IP 2, правило 5 активно)	<0(Нет) | 1(Да)>	= 1
210205003 =	IP Filter Set 2, Rule 5 Protocol (Набор фильтров IP 2, правило 5, протокол)		= 17
210205004 =	IP Filter Set 2, Rule 5 Dest IP address (Набор фильтров IP 2, правило 5, IP-адрес получателя)		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask (Набор фильтров IP 2, правило 5, маска подсети получателя)		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port (Набор фильтров IP 2, правило 5, порт получателя)		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp (Набор фильтров IP 2, правило 5, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address (Набор фильтров IP 2, правило 5, IP-адрес отправителя)		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask (Набор фильтров IP 2, правило 5, маска подсети отправителя)		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port (Набор фильтров IP 2, правило 5, порт отправителя)		= 0
210205011 =	IP Filter Set 2, Rule 5 Src Port Comp (Набор фильтров IP 2, правило 5, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match (Набор фильтров IP 2, правило 5, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210205014 =	IP Filter Set 2, Rule 5 Act Not Match (Набор фильтров IP 2, правило 5, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1

Табл. 170 Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1) (продолжение)

/ Меню 21.1.2.6 — Filter set #2, rule #6 (Набор фильтров #2, правило #6) (SMT-меню 21.1.2.5)			
FIN	FN	PVA	INPUT
210206001 =	IP Filter Set 2, Rule 6 Type (Набор фильтров IP 2, правило 6, тип)	<0(нет) | 2(TCP/ IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active (Набор фильтров IP 2, правило 6 активно)	<0(Нет) | 1(Да)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol (Набор фильтров IP 2, правило 6, протокол)		= 17
210206004 =	IP Filter Set 2, Rule 6 Dest IP address (Набор фильтров IP 2, правило 6, IP-адрес получателя)		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask (Набор фильтров IP 2, правило 6, маска подсети получателя)		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port (Набор фильтров IP 2, правило 6, порт получателя)		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp (Набор фильтров IP 2, правило 6, сравнение порта получателя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address (Набор фильтров IP 2, правило 6, IP-адрес отправителя)		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask (Набор фильтров IP 2, правило 6, маска подсети отправителя)		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port (Набор фильтров IP 2, правило 6, порт отправителя)		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp (Набор фильтров IP 2, правило 6, сравнение порта отправителя)	<0(нет) | 1(равно) | 2(не равно) | 3(меньше) | 4(больше)>	= 0
210206013 =	IP Filter Set 2, Rule 6 Act Match (Набор фильтров IP 2, правило 6, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210206014 =	IP Filter Set 2, Rule 6 Act Not Match (Набор фильтров IP 1, правило 6, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 2
241100005 =	FTP Server Access (Доступ к серверу FTP)	<0(LAN+WAN) | 1(недоступен) | 2(LAN) | 3(WAN)>	= 0

Табл. 170 Меню 21.1 — Filer Set #2 (Набор фильтров #2) (SMT-меню 21.1) (продолжение)

241100006 =	FTP Server Secured IP address (Безопасный IP-адрес сервера FTP)		= 0.0.0.0
241100007 =	Web Server Port (Порт Web-сервера)		= 80
241100008 =	WEB Server Access (Доступ к Web-серверу)	<0(LAN+WAN) | 1(недоступен) | 2(LAN) | 3(WAN)>	= 0
241100009 =	WEB Server Secured IP address (Безопасный IP-адрес WEB-сервера)		= 0.0.0.0

Табл. 171 Меню 23 — System Menus (Системные меню) (SMT-меню 23)

*/ Меню 23.1 — System Password Setup (Настройка системного пароля) (SMT-меню 23.1)			
FIN	FN	PVA	INPUT
230000000 =	System Password (Системный пароль)		= 1234
*/ Меню 23.2. System security (Системные функции безопасности): radius server (сервер RADIUS) (SMT-меню 23.2)			
FIN	FN	PVA	INPUT
230200001 =	Authentication Server Configured (Сервер аутентификации настроен)	<0(Нет) | 1(Да)>	= 1
230200002 =	Authentication Server Active (Сервер аутентификации активен)	<0(Нет) | 1(Да)>	= 1
230200003 =	Authentication Server IP Address (IP-адрес сервера аутентификации)		= 192.168.1.32
230200004 =	Authentication Server Port (Порт сервера аутентификации)		= 1822
230200005 =	Authentication Server Shared Secret (Сервер аутентификации, общий секретный ключ)		= 1111111111111111 1111111111111111
230200006 =	Accounting Server Configured (Сервер учета настроен)	<0(Нет) | 1(Да)>	= 1
230200007 =	Accounting Server Active (Сервер учета активен)	<0(Нет) | 1(Да)>	= 1
230200008 =	Accounting Server IP Address (IP-адрес сервера учета)		= 192.168.1.44
230200009 =	Accounting Server Port (Порт сервера учета)		= 1823
230200010 =	Accounting Server Shared Secret (Сервер учета, общий секретный ключ)		= 1234
*/ Меню 23.4. System security (Системные функции безопасности): IEEE 802.1x (SMT-меню 23.4)			
FIN	FN	PVA	INPUT

Табл. 171 Меню 23 — System Menus (Системные меню) (SMT-меню 23) (продолжение)

230400001 =	Wireless Port Control (Управление беспроводной точкой доступа)	<0(требуется аутентификация) | 1(доступ запрещен) | 2(аутентификация не требуется)>	= 2
230400002 =	ReAuthentication Timer (in Seconds) (Таймер повторной аутентификации, сек.)		= 555
230400003 =	Idle Timeout (in second) (Макс. время простоя, сек.)		= 999
230400004 =	Authentication Databases (Базы данных аутентификации)	<0(только БД лок. польз.) | 1(только RADIUS) | 2(лок., RADIUS) | 3(RADIUS, лок.)>	= 1
230400005 =	Key Management Protocol (Протокол управления ключами)	<0(8021x) | 1(WPA) | 2(WPAPSK)>	= 0
230400006 =	Dynamic WEP Key Exchange (Динамический обмен ключами WEP)	<0(ОТКЛЮЧ.) | 1(64-разрядное шифрование WEP) | 2(128-разрядное шифрование WEP)>	= 0
230400007 =	PSK =		=
230400008 =	WPA Mixed Mode (Смешанный режим WPA)	<0(Отключ.) | 1(Включ.)>	= 0
230400009 =	Data Privacy for Broadcast/ Multicast packets (Конфиденциальность данных для пакетов широковещательной/ многоадресной рассылки)	<0(TKIP) | 1(WEP)>	= 0
230400010 =	WPA Broadcast/ Multicast Key Update Timer (Таймер обновления ключа WPA широковещательной/ многоадресной рассылки)		= 0

Табл. 172 Меню 24.11 — Remote Management Control (Удаленное управление) (SMT-меню 24.11)

/ Меню 24.11 — Remote Management Control (Удаленное управление) (SMT-меню 24.11)			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port (Порт сервера TELNET)		= 23
241100002 =	TELNET Server Access (Доступ к серверу TELNET)	<0(LAN+WAN) | 1(недоступен) | 2(LAN) | 3(WAN)>	= 0
241100003 =	TELNET Server Secured IP address (Безопасный IP-адрес сервера TELNET)		= 0.0.0.0

Табл. 172 Меню 24.11 — Remote Management Control (Удаленное управление) (SMT-меню 24.11)

241100004 =	FTP Server Port (Порт сервера FTP)		= 21
241100005 =	FTP Server Access (Доступ к серверу FTP)	<0(LAN+WAN) | 1(недоступен) | 2(LAN) | 3(WAN)>	= 0
241100006 =	FTP Server Secured IP address (Безопасный IP-адрес сервера FTP)		= 0.0.0.0
241100007 =	Web Server Port (Порт Web-сервера)		= 80
241100008 =	WEB Server Access (Доступ к Web-серверу)	<0(LAN+WAN) | 1(недоступен) | 2(LAN) | 3(WAN)>	= 0
241100009 =	WEB Server Secured IP address (Безопасный IP-адрес WEB-сервера)		= 0.0.0.0

Примеры команд

Ниже приведены примеры сообщений внутреннего генератора SPTGEN, выводимых в ответ на команды интерпретатора команд интернет-центра.

Табл. 173 Примеры команд

FIN	FN	PVA	INPUT
Команда /ci (для приложения A): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(glite)|1(t1.413)|2(gdmt)|3(multimode)>	= 3
Команда /ci (для приложения B): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(etsi)|1(normal)|2(gdmt)|3(multimode)>	= 3

Алфавитный указатель

Numerics

110 В, переменный ток 3
230 В, переменный ток 3

A

ADSL, что это такое? 41
Any IP (Любой IP) 43
  как работает 74
  примечание 73
AWG (Американская система калибровки проводов) 3

B

BSS (Базовый набор служб) 456

C

CA (Бюро сертификации) 463
CDR 347
CDR (Запись о деталях установления вызова) 346
CHAP (Протокол аутентификации по методу "вызов-рукопожатие") 273
CTS (Готовность к приему) 459

D

DHCP 45, 69, 70, 130, 230, 231, 258, 344
DNS (Система доменных имен) 259
DSL (Цифровая абонентская линия) 40
DSL, что это такое? 40
DSLAM (Мультиплексор цифровых абонентских линий) 47

E

EAP 78
ECHO 121
ESS 457
ESSID (Идентификатор набора дополнительных услуг) 82
Ethernet 403

F

Finger (Указатель) 121
FTP 120, 121, 185, 372
  Ограничения 372

H

HTTP 140
HTTP (Протокол передачи гипертекста) 121, 137, 139, 236

I

IANA (Агентство по назначению имен и уникальных параметров протоколов Интернет) 71, 162
IBSS (Независимый базовый набор служб) 456
ICMP (Протокол управляющих сообщений в сети Интернет) 142, 171
IEEE 802.11g 46, 461
IEEE 802.11i 46
IEEE802.1x 334
IGMP 72
Integrated Services Digital Network (Цифровая сеть с предоставлением комплексных услуг) 42
IP Static Route Setup 283
IP-адрес 70, 120, 231, 259, 284, 289, 319, 344, 350, 377
IP-адрес в локальной сети по умолчанию 50
IP-адрес сервера системных журналов 347

IP-маска 318
ISDN (Цифровая сеть с предоставлением комплексных услуг) 42

L

LAN (ЛВС) 342
LAN (ЛВС, см. Локальная сеть) 342
LAND 141

M

MAC (Управление доступом к среде) 231, 286
MAC-адрес 84, 288
Max-incomplete High 173
Max-incomplete Low 173
MBS (см. Максимальный размер пакета) 269
MSDU (Единица данных MAC) 261

N

NAT 120, 122
  правило отображения адресов 127
NAT (Трансляция сетевых адресов) 70, 116, 269, 322
  как работает 117
  назначение 117
  настройка 292
  определения 116
  порядок применения правил 295
  приложения, не поддерживающие NAT 305
  применение 118
  применение NAT в меню SMT 290
  примеры 299
  типы отображения 119
NAT Transversal 188
NNTP 121

O

One-Minute High 174

P

Packet triggered (Инициирующий пакет) 348
PAP (Протокол аутентификации пароля) 273
Ping of Death 140
POP3 121, 139, 140
PPP Log (Журнал регистрации PPP) 349
PPP поверх Ethernet (PPP over Ethernet, RFC 2516) 102
PPPoA 271
PPPoE 106
  преимущества 106
PPPoE (Протокол "точка-точка" поверх Ethernet) 44, 106, 452
PPTP 121
PSK (Предварительно согласованный ключ) 336
PVC 102

R

RADIUS 461
  настройка 100
  общий секретный ключ 462
RAS 344, 375
Restore Configuration 357
RFC 1483 103
RFC 1631 116
RFC-1483 271
RFC-2364 271, 272
RFC2516 44
RIP 259, 276
RIP, см. Routing Information Protocol (Протокол обмена информацией о маршрутизации) 71
romfile 352
Routing (Маршрутизация) 264
RTS (Запрос на передачу) 261, 459

S

SCR (см. Поддерживаемая скорость ячеек) 269
SMTP 121
Smurf 142
SUA 120, 121
SYN Flood 141
SYN-ACK 141

T

TCP/IP 139, 140, 186, 322, 350
Teardrop 140
Telnet 185, 240
TFTP
  Ограничения 372
ToS (Тип услуги) 374, 375, 377, 378, 379
Traceroute 143

U

UPnP 188

V

VC (Виртуальный канал) 103
VCI (Идентификатор виртуального канала) 104
VPI (Идентификатор виртуального пути) 104
VPI и VCI 104

W

WAN (Глобальная сеть) 102
Web-конфигуратор 50, 52, 53, 138, 147, 148, 154, 309
  интерфейс 52
WEP 83
WEP (Протокол шифрования WEP) 47, 261
  ключ по умолчанию 262
WEP-шифрование 81, 261
WPA 86, 337
  вспомогательное ПО 88
  предварительно согласованный ключ 86
  пример применения с RADIUS 87
WPA-PSK 86

Z

ZyXEL Communications Corporation 2

A

Авторское право 2
Агентство по назначению имен и уникальных параметров протоколов Интернет, см. IANA 71
Агрессивные жидкости 3
Адаптер питания 3
Адрес источника 154, 161
Адрес получателя 155
Адресация IP 426
Альтернативные варианты записи маски подсети 428
Американская система калибровки проводов 3
Атаки
  "Smurf" 142
  "грубой силой" 142
  DoS 140
  LAND 140
  SYN Flood 140
  Teardrop 140
Аутентификация 273, 274
  EAP 334
  пользователя 465
Аутентификация EAP 463

Б

База управляющей информации (MIB) 329
Базы данных аутентификации 93, 337
Бассейн 3
Безопасность TCP 146
Безопасность UDP/ICMP 147
Беспроводная локальная сеть (WLAN) 260
  настройка 81
  параметры безопасности 466
  помехи 458
Бюджет пропускной способности 211, 221
Бюро сертификации 463

B

Вектор инициализации (IV) 465
Вентиляционные отверстия 3
Версия микропрограммы ZyNOS 353
Влага 3
Владельцы торговых марок 2
Влажные подвалы 3
Внутренний генератор таблицы системных параметров (SPTGEN) 488

пример загрузки по протоколу FTP 490
текстовый файл 488
что необходимо помнить 489
Вода 3
Водопроводы 3
Воздействие 3
Воспроизведение 2
Время бездействия системы 185, 372
Время блокирования 174
Время ожидания 253
Время простоя 274
Вскрывать 3
Вспомогательное программное обеспечение для беспроводных клиентов WPA 88
Встроенная база данных пользователей 98, 338
Встроенная справка 53
Высокое напряжение 3

Г

Газопроводы 3
Генератор таблицы системных параметров 488
Главное меню 245
Гроза 3

Д

Действие фильтра MAC-адресов 85, 263
Диагностика 233
Динамическая система доменных имен (DYNDNS) 45, 130, 249, 250
Динамический обмен ключами WEP 93, 336, 464
Доступ в Интернет 43, 47, 58, 264, 267, 268
с использованием автоматической настройки модема (Zero Configuration) 43
Доступ в Интернет с использованием автоматической настройки модема (Zero Configuration) 107

Е

Европа 3

Ж

Жидкости, агрессивные 3
Журнал регистрации и трассировка 346
Журнал регистрации ошибок 345
Журнал регистрации сообщений 345

З

Загрузка микропрограммы 359
Загрузка ЦП 342
Заимствование пропускной способности 216
у исходного класса 221
занимает 46
Зарегистрированная 2
Зарегистрированная торговая марка 2
Защита беспроводной связи 78
Защищенный доступ Wi-Fi (Wi-Fi Protected Access, WPA) 86
Защищенный доступ Wi-Fi (WPA) 46
Значения допустимых порогов 173

И

Идентификатор канала (Channel ID) 261
Идентификатор хоста 426
Изменение пароля при входе 51
Имя домена 70, 121, 248
Имя класса 221
Имя компьютера 248
Имя пользователя 131
Инициализировать заново линию ADSL 235
Инкапсуляция 102, 268, 271
PPPoA 103
RFC 1483 103
инкапсуляция ENET ENCAP 102
протокол "точка-точка" поверх Ethernet 102
Инкапсуляция PPP 279
Инспекция пакетов с учетом состояния 44, 136, 137, 144
для модели P–660HT/HTW EE 146
процесс 145
Интерактивные приложения 375
Информация о системе 343
диагностика 340
Источник питания 3
ремонт 3

К

Кабели, соединительные 3
Кабель питания 3
Канал 458
  помехи 458
Качество услуги 374
Квалифицированный технический персонал 3
Класс пропускной способности 211
Классы IP 426
Клиент DHCP 45
Кнопка сброса настроек модема 52
Код страны 344
Команда AT 353
Команды NetBIOS 143
Комплектующие 3
Конфиденциальность данных 336
Конфликт 342
Корневой класс 219
Краткое руководство 39, 50
Крышка 3

Л

Линия DSL, инициализировать заново 235
Лицензия 2
Логические сети 264
Локальная сеть
  список правил 157
Любой IP 73

М

Максимальный размер пакета (MBS) 107, 110
Максимум неполных TCP (TCP Maximum Incomplete) 174
Маршрутизация на базе источника 374
Маршрутизация на базе политики 374
Маска подсети 70, 161, 259, 275, 284, 344, 427
Мастер установки доступа в Интернет 58
Межсетевой экран
  Anti-Probing (Блокирование эхо-тестирования) 171
  введение 138
  включение 156
  логика правил 153
  межсетевой экран и фильтры 149
  меню SMT 308
  назначение портов пользователем 162
  правила 152
  правила LAN–WAN 155
  правила с точки зрения безопасности 154
  предупреждения 155
  руководство по улучшению безопасности 148
  службы 168
  случаи использования 150
  создание/редактирование правил 159
  список вопросов для составления правил 153
  способы настройки 152, 308
  тип адреса 161
  типы 136
  удаленное управление 308
Межсетевой экран ZyXEL
  введение 138
Межсетевые экраны на уровне приложений 137
Межсетевые экраны с фильтрацией пакетов 137
Метрика 105, 276, 284
Микропрограмма 236, 352
  загрузка 236
  обновление 236
  ошибка загрузки 238
Многоадресная рассылка 72, 276
Многопротокольная инкапсуляция 103
Модель P–660HT/HTW EE 352
Молния 3
Мост 250, 273, 286
  Ethernet 286
  Ethernet-адрес 288
  время хранения адреса Ethernet 288
  настройка статических маршрутов 288
  удаленный узел 286
Мой адрес в глобальной сети 275
Мультиплексирование 103, 268, 271
  на базе LLC 103
  на базе VC 103
Мультиплексирование на базе LLC 279
Мультиплексирование на базе VC 271

Н

Набор серверов SUA/NAT 124
Набор фильтров
  класс 317
Наборы расписаний
  продолжительность 385
Назначение IP-адреса 104
  PPPoA или PPPoE 104
  RFC 1483 104
  инкапсуляция ENET ENCAP 104
Назначение адреса 70

Напряжение сети 3
Напряжение, высокое 3
Настенное крепление 3
Настройка 69, 230
Настройка Any IP 76
Настройка TCP/IP локальной сети 70
Настройка Telnet 186
Настройка беспроводной локальной сети 260
Настройка глобальной сети 253
Настройка диапазона IP 69
Настройка доступа в Интернет 290, 389
Настройка классов пропускной способности 219
Настройка локальной сети 68, 102
Настройка общих параметров 248
Настройка правила фильтра 317
Настройка статического маршрута IP 283
Настройка удаленного управления 370
Настройки пользователей 98, 338
Независимый базовый набор служб 456
Неисправность 3
Неопределенная скорость передачи (UBR) 110
Непризнание иска 2
Номер модели 236
Номера портов 121

О

Обзор меню SMT 241
Обслуживание 3
Общая безопасность 148
Общий секретный ключ 101, 333
Обязательные поля 244
Ограничение трафика 106
Ограничения на FTP 185, 355
Ограничения на TFTP 185, 355
Ограничения на удаленное управление 185, 372
Опасность 3
Организация подсетей 428
Основные поля для настройки правил 154
Ответ ICMP 142
Ответственность 2
Отказ в обслуживании (DoS) 44, 138, 139, 173, 174, 308
  основные сведения 139
Отображение адресов 125

П

Пакет
  ошибка 342
  передано 342
  принято 342
Пакет IP 320
Пакеты 341
Параметры безопасности 466
Параметры класса пропускной способности 220
Параметры системного журнала UNIX 347
Параметры уровня ATM 278
Парный главный ключ (PMK) 466
Пароль 240, 246, 272, 273, 329
Патент 2
Перевод 2
Передача голоса по IP-протоколу (VoIP) 210
Передача файлов с помощью FTP 359
Передача файлов с помощью TFTP 361
Переменная скорость передачи (VBR) 110
Переменный ток 3
Перенаправление трафика 44, 112, 113, 115
  настройка 254
Период простоя при управлении 51
Пиковая скорость ячеек (PCR) 107, 110
Письменное разрешение 2
Плавательный бассейн 3
Планировщик 213
Планировщик на основе приоритетов 213
Планировщик на основе равномерного распределения 213
Повреждения 3
Подвал 3
Поддерживаемая скорость ячеек (SCR) 107, 110
Поддержка IGMP 276
Подстановка IP-адреса (IP Spoofing) 140, 143
Политика IP 264
Политика маршрутизации 375
Политика маршрутизации IP (IPPR) 45, 264, 374
  критерии 375
  настройка 375
  политики IP для Ethernet 379
  преимущества 374
  применение политики IP 379
  сокращение расходов 374
  шлюз 379

  Политика маршрутизации IP (IPPR)
  распределение нагрузки 374
Политики IP 379
Полноскоростной 448

Полуоткрытые сеансы связи 173
Пользовательские порты
  создание/редактирование 163
Пользовательские службы 162, 163
Поражение электрическим током 3
Порог RTS 83, 261, 458, 459
Порог фрагментации 261, 460
Порядковый номер удаленного узла 341
Поставщик 3
Постоянная скорость передачи (CBR) 110
Постоянное соединение 105
Права 2
Правила 155
  LAN to WAN (ЛВС — глобальная сеть) 155
  контрольный список 153
  логика 153
  основные поля 154
  предварительно настроенные службы 168
  список 157
Правила LAN–WAN 155
Правила с точки зрения безопасности 154
Правила фильтра протоколов 322
Правила фильтра устройства 322
Правило устройства 322
Предварительно согласованный ключ 336
  формат 86
Предупреждения 3
Предупреждения об атаках 175
Приложение реального времени 210
Приложения
  доступ в Интернет 47
Применение WPA с RADIUS 87
Применение WPA-PSK 86
Пример IP-адресов 276
Приоритет 221, 375, 378
Приток воздуха 3
Проверка целостности пакетов (MIC) 465
Пропорциональное распределение пропускной способности 211
Пропускная способность 211
Протокол 318
Протокол "Точка-точка" по уровню 5 адаптации ATM (AAL5) 103
Протокол IP 375, 378
Протокол SNMP 121
  Get (Получить) 329
  GetNext (Получить следующее) 329
  Set (Установить) 329
  Trap (Прерывание) 329
  базы управляющей информации 329
  доверенный узел 330
  настройка 329
  пароль 330
  управляющая программа 329
Протокол Xmodem 353
Протокол аутентификации 274
Протокол временной целостности ключа (TKIP) 465
Протокол динамической настройки узла 45
Протокол маршрутизации канального уровня с инкапсуляцией MAC (ENET ENCAP) 102
Протокол обмена информацией о маршрутизации 71
  версия 72
  направление 71
Протокол разрешения адресов (ARP) 74
Протокол туннелирования "точка-точка" 121
Протокол управления ключами 336
Протоколы верхнего уровня 146, 147
Процесс реализации правил фильтра 312
Процесс фильтрации
  исходящие пакеты 311
Псевдоним IP 45, 264
Пыль 3

P

Рабочая частота 261
Радиочастота (RF) 46, 82
Размещение журнала 347
Разрешение 2
Расписание вызовов 384
  PPPoE 386
  макс. количество наборов расписаний 384
  пример приоритета 384
  приоритет 384
Расширенный набор служб 457
Регистрационное имя 272
Регистрационные журналы 202
Регистрация фильтров 348
Режим NAT 122
Режим заголовка 460
Режим интерпретатора команд 364
Резервирование глобальной сети 113
Резервное копирование 353
Результаты трассировки 345
Ремонт 3
Ретранслятор DHCP (DHCP relay) 45
Риск 3
Розетка электропитания 3

C

Сброс настроек интернет-центра 51
Сводная таблица окон Web-конфигуратора 53
Северная Америка 3
Сервер 119, 292, 294, 297, 298, 300, 301, 302, 368
Сервер DHCP 45, 231, 258
Сервер FTP 302
Сервер RADIUS 332
Сервер SUA 120, 123
  набор серверов по умолчанию 120
Сервер за NAT 297
Сервер системного журнала 346
Сетевая операционная система ZyXEL (ZyNOS) 2, 352, 353
Сеть электропитания 3
Система
  диагностика 349
  журнал регистрации и трассировка 345
  информация о системе 343
  системный журнал и учет ресурсов 346
  скорость консольного порта 345
  состояние системы 340
Система распределения (DS) 87
Системная консоль 243
Системные функции безопасности 332
Системный журнал 168, 346
Системный журнал UNIX 345, 347
Системный пароль 332
Скорость
  передача 342
  прием 342
Скорость передачи данных 43
Скрытые меню 244
Скрытый узел 458
Служба имен доменов 69
Службы 121, 154
Смешанный режим WPA 336
Снимать 3
Соединительные кабели 3
Создание псевдонимов IP 265
Создание расписания 385
Сообщения RADIUS 462
Сообщения об ошибках SMTP 207
Сопроводительная документация 39
Сопровождение 226
Сопровождение системы 340, 343, 353, 356, 362, 364, 365, 368
Состояние системы 341
Сохранение состояния 144
Список правил 157
Сплиттеры 448
Способы настройки 308
Справочный компакт-диск 39
Сравнение SUA и NAT 120
Средства диагностики 340
Стандарты ADSL 42
Статический маршрут 282
Статический маршрут IP 282
Стоимость передачи 276, 284
Структура имен файлов 352, 353
Счетчик переходов по сети 276, 284

T

Таблица Any IP (Любой IP) 231
Таблица DHCP 231
Телефонный провод 3
Техника безопасности 3
Технический персонал 3
Тип протокола IP 168
Тип резервирования 114
Тип службы 164
Тип соединения 341
Тип услуги 389
Типы атак 142
Типы атак DoS
  Типы 140
Типы сообщений RADIUS 462
Топология статической маршрутизации 282
Торговая марка 2
Точка доступа (AP) 458
Точки-точка 41
Транзит PPPoE-соединений 280
Трансляция сетевых адресов (NAT) 45, 290
Трехстороннее квитирование 141
Трубопроводы 3

У

Увеличение использования пропускной способности 213
Удаленное управление
  межсетевой экран 308
Удаленное управление и NAT 185
Удаленный сервер DHCP 259

Удаленный узел 270, 342
  настройка удаленного узла 270
  профиль удаленного узла 272
Удар электрическим током 3
Удар, электрический ток 3
Узел (Host) 56
Универсальная функция "Plug and Play" (UPnP) 44
Универсальная функция Plug and Play 188
  применение 188
  проблемы безопасности сети 189
Управление беспроводной точкой доступа 90, 335
Управление бюджетом 365, 366
Управление пропускной способностью 44, 210
  монитор 225
  общие настройки 218
  статистика 223
Управление с помощью Telnet 185
Управление сетью 121
Уровень 5 адаптации ATM (AAL5) 103
Уровни подклассов 219
Условия, препятствующие работе TFTP и FTP по глобальной сети 355
Условные обозначения 38
Установка UPnP 190
  Windows Me 190
  Windows XP 192
Установка времени и даты 367
Учетная запись одиночного пользователя (SUA) 120, 290

Ф

Файл конфигурации 352
Фильтр 256, 310
  SUA 322
  правила фильтрации 315
  правило фильтра TCP/IP 317
  правило фильтра общего типа 320
  применение фильтров 325
  пример 324
  структура фильтра 312
  трафик Ethernet 325, 326
  удаленный узел 277
  фильтры для удаленного узла 277, 326
Фильтр IP 320
  логическая схема 319
Фильтр MAC-адресов 79, 262
Фильтр общего типа 322
Фильтр пропускной способности 211
Фильтр протоколов 322
Фильтрация 310, 317
Фильтрация MAC-адресов 84, 262
  действие фильтра 263
  для беспроводной сети 46
Фильтрация вызовов 310
Фильтрация данных 310
Фильтрация на основе содержания (контентная фильтрация) 44, 178
  блокировка по ключевым словам в URL 179
  график 181
  категории 178
  надежные (правомочные) компьютеры 181
Фильтрация пакетов 149
  случаи использования 149
Фильтры вызовов
  встроенные фильтры 310
  определяемые пользователем 310
Формат текстового файла 488
Форум по универсальной функции Plug and Play 189
Фотокопирование 2
Функция журнальной регистрации 319, 322

Ч

Часовой пояс 369
Частный адрес 276, 284

Ш

Шаблоны DYNDNS 130
Шифрование 465
Шлюз 284
Шлюзовой узел 289

Э

Электронная почта
  пример журнала 207
Электропроводка 3
Эхо-тестирование 350