

P-791R версия 2

Маршрутизатор G.SHDSL.bis

Руководство пользователя

Версия 3,40

5/2007

Вторая редакция

ВХОД В СИСТЕМУ ПО УМОЛЧАНИЮ

IP Address	http://192.168.1.1
Пароль администратора	1234
Пароль пользователя	user

ZyXEL
www.zyxel.ru

ZyXEL
www.zyxel.ru

О Руководстве пользователя

Целевая аудитория

Это руководство предназначено для пользователей, выполняющих настройку устройства ZyXEL посредством веб-конфигуратора. Предполагается знание основ TCP/IP и принципов построения сетей.

Другие документы

- Краткое руководство пользователя
Краткое руководство пользователя поможет немедленно начать работу. Оно содержит информацию о настройке сети и доступа в Интернет.
- Контекстная справка в веб-конфигураторе
Встроенная гипертекстовая справка с описаниями отдельных экранов и вспомогательными сведениями.



Для настройки устройство ZyXEL рекомендуется использовать веб-конфигуратор.

- Диск с сопроводительными материалами
На прилагаемом компакт-диске содержится вспомогательная документация.
- Веб-сайт ZyXEL
Дополнительную справочную документацию и сведения о сертификации изделий можно найти на сайте www.zyxel.ru.

Отзывы о руководстве пользователя

Ваши замечания помогут нам лучше учесть интересы пользователей. Любые комментарии по этому руководству, вопросы и пожелания вы можете направлять нам через «Интерактивную систему консультаций» на сайте www.zyxel.ru

Обозначения, принятые в документации

Предупреждения и примечания

Для предупреждений и примечаний в настоящем руководстве используются следующие обозначения.



Предупреждения обращают внимание на моменты, представляющие опасность для вас или оборудования.




Примечания отмечают другие важные сведения (например, параметры, которые необходимо настроить дополнительно), полезные советы и рекомендации.

Условные обозначения и синтаксис

- Маршрутизатор P-791R v2 может обозначаться в тексте как “устройство ZyXEL”, “устройство”, “система” или “изделие”.
- Названия изделий, экранов, заголовки полей и выбираемые значения приведены **жирным** шрифтом.
- Названия клавиш набраны заглавными буквами и заключены в квадратные скобки, например, [ENTER] означает нажатие клавиши “Enter” или “Return”.
- “Введите” означает, что следует набрать на клавиатуре один или несколько знаков и нажать клавишу [ENTER]. “Выберите” или “Отметьте” означает, что следует выбрать один из predetermined вариантов.
- Знак (>) обозначает переход между экранами. Например, последовательность **Maintenance > Log > Log Setting** означает, что сначала необходимо щелкнуть в панели навигации на пункте **Maintenance**, затем перейти в подменю **Log** и щелкнуть на вкладке **Log Setting** для перехода на соответствующий экран.
- В зависимости от контекста могут использоваться десятичные или двоичные единицы измерения. В частности, суффикс “к” (кило-) может обозначать 1000 или 1024, суффикс “М” (мега-) – 1 000 000 или 1 048 576 и т.д.

Значки, используемые на рисунках

На рисунках в Руководстве пользователя могут встречаться следующие универсальные обозначения. Значок устройство ZyXEL не является точным изображением вашего устройства.

устройство ZyXEL 	Компьютер 	Ноутбук 
Сервер 	DSLAM 	Сетевой экран 
Телефон 	Коммутатор 	Маршрутизатор 

Техника безопасности



В целях вашей безопасности примите к сведению и придерживайтесь следующих предупреждений и указаний по технике безопасности.

- НЕ устанавливайте устройство вблизи от воды, например, в сыром подвале или рядом с бассейном.
- НЕ подвергайте устройство воздействию влаги, пыли или агрессивных жидкостей.
- НЕ складывайте на устройство никаких предметов.
- НЕ устанавливайте, не эксплуатируйте и не ремонтируйте устройство во время грозы. Грозовые разряды создают риск поражения электрическим током.
- Подключайте к устройству ТОЛЬКО годное к применению вспомогательное оборудование.
- Ремонтировать или разбирать устройство должен ТОЛЬКО квалифицированный специалист.
- Убедитесь, что кабели правильно подключены к клеммам.
- Размещайте соединительные кабели так, чтобы не наступать на них и не задевать их.
- Перед обслуживанием или разборкой в обязательном порядке необходимо отсоединить от устройства все кабели.
- Эксплуатируйте устройство ТОЛЬКО с пригодным для него источником питания или шнуром. Сетевой шнур должен подключаться к сети переменного тока с соответствующим напряжением (110 вольт в Северной Америке и 230 вольт в Европе).
- НЕ ставьте какие-либо предметы на сетевой шнур или блок питания, НЕ размещайте устройство там, где на шнур или блок питания может кто-нибудь наступить.
- НЕ пользуйтесь устройством, если блок питания или шнур поврежден, иначе может произойти поражение электрическим током.
- В случае повреждения необходимо отсоединить шнур или блок питания от устройства и отключить его от электросети.
- НЕ пытайтесь починить шнур или блок питания. Обратитесь к местному поставщику и закажите новый шнур или блок питания.
- Не используйте устройство вне помещений. Убедитесь, что все соединения выполнены внутри помещений. Грозовые разряды создают риск поражения электрическим током.
- НЕ загораживайте вентиляционные проёмы устройства. Недостаточная вентиляция может повредить устройство.
- Монтируя устройство на стене, следите за тем, чтобы не повредить электропроводку, газо- или водопроводные трубы.

Изделие допускает возможность переработки. Соблюдайте правила утилизации.



Обзор содержания

Краткое введение и настройка с помощью мастеров	31
Краткое знакомство с P-791R v2	33
Знакомство с веб-конфигуратором	37
Мастер настройки доступа к Интернету.....	49
Прямые соединения	57
Настройка сети	61
Настройка WAN	63
Настройка LAN	87
Экраны настройки NAT	99
Безопасность	111
Фильтр	113
Расширенная настройка	115
Статическая маршрутизация	117
Настройка DNS для динамических адресов	121
Настройка удаленного управления	125
Универсальная технология “включи и работай” (UPnP)	135
Сопровождение	147
Экран System	149
Журналы	155
Системные инструменты	159
Диагностика	165
Использование SMT и устранение неполадок	167
Введение в SMT	169
Общая настройка	175
Настройка WAN	179
Настройка LAN	185
Настройка доступа к Интернету	191
Настройка удаленного узла	195
Настройка статического маршрута	207
Настройка NAT	211
Настройка фильтра	227
Настройка SNMP	241

Системный пароль	243
Информация о системе и диагностика	245
Работа с файлами микропрограмм и настроек	255
Разделы меню с 24.8 по 24.11	269
Настройка политик маршрутизации IP	277
Настройка расписания	285
Поиск и устранение неполадок	289
Приложения и предметный указатель	295

Содержание

О Руководстве пользователя.....	3
Обозначения, принятые в документации.....	4
Техника безопасности.....	6
Обзор содержания.....	9
Содержание.....	11
Список рисунков.....	21
Список таблиц.....	27

Часть I: Краткое введение и настройка с помощью мастеров 31

Глава 1

Краткое знакомство с P-791R v2.....	33
1.1 Общие сведения.....	33
1.1.1 Высокоскоростной доступ в Интернет.....	33
1.1.2 Высокоскоростные соединения по схеме “точка-точка”.....	34
1.2 Способы управления P-791R v2.....	34
1.3 Рекомендации по управлению P-791R v2.....	35
1.4 Светодиоды.....	35

Глава 2

Знакомство с веб-конфигуратором.....	37
2.1 Обзор веб-конфигуратора.....	37
2.2 Вызов веб-конфигуратора.....	37
2.3 Навигация в веб-конфигураторе.....	39
2.4 Экран состояния (Status).....	42
2.4.1 Раздел Status: Packet Statistics.....	45
2.5 Сброс P-791R v2.....	46
2.5.1 Использование кнопки сброса.....	47

Глава 3

Мастер настройки доступа к Интернету.....	49
3.1 Введение.....	49
3.2 Мастер настройки доступа к Интернету.....	49

Глава 4	
Прямые соединения	57
4.1 Общие сведения	57
4.2 Настройка соединения по схеме "точка-точка"	58
4.2.1 Настройка сервера	58
4.2.2 Настройка клиента	59
4.2.3 Соединение двух устройств P-791R v2	59
Часть II: Настройка сети	61
Глава 5	
Настройка WAN	63
5.1 Обзор параметров WAN	63
5.1.1 Encapsulation	63
5.1.2 Мультиплексирование	64
5.1.3 VPI и VCI	65
5.1.4 Присвоение IP-адресов	65
5.1.5 Закрепленное соединение (в режиме PPP)	65
5.1.6 NAT	66
5.2 Метрика	66
5.3 Ограничение трафика	66
5.3.1 Классы трафика в ATM	67
5.4 Настройка подключения к Интернету	68
5.4.1 Расширенная настройка соединения с Интернетом	71
5.5 Настройка дополнительных соединений	73
5.5.1 Редактирование дополнительных соединений	74
5.5.2 Расширенная настройка дополнительных соединений	77
5.6 Переадресация трафика	78
5.7 Интерфейс резервирования через коммутируемый доступ	79
5.8 Порт резервирования CON/AUX	80
5.9 Настройка резервирования WAN	80
5.9.1 Расширенная настройка резервирования	82
5.9.2 Расширенные настройки модема для резервирования через коммутируемый доступ	85
Глава 6	
Настройка LAN	87
6.1 Обзор локальной сети	87
6.1.1 Сети LAN, WAN и P-791R v2	87
6.1.2 Настройка DHCP	88
6.1.3 Адрес DNS-сервера	88

6.1.4 Присвоение адресов DNS-серверов	89
6.2 Параметры TCP/IP для локальной сети	89
6.2.1 IP-адрес и маска подсети	89
6.2.2 Настройка RIP	90
6.2.3 Multicast	91
6.3 Настройка параметров IP для локальной сети	91
6.3.1 Настройка дополнительных параметров локальной сети	92
6.4 Настройка DHCP	93
6.5 Список клиентов в локальной сети	95
6.6 Совмещение IP-адресов в локальной сети	96
Глава 7	
Экраны настройки NAT	99
7.1 Краткий обзор NAT	99
7.1.1 Определения, относящиеся к NAT	99
7.1.2 Назначение NAT	100
7.1.3 Принцип работы NAT	100
7.1.4 Применение NAT	101
7.1.5 Типы привязки NAT	101
7.2 Сравнение SUA и NAT	102
7.2.1 SIP ALG	102
7.3 Общая настройка NAT	103
7.4 Port Forwarding	104
7.4.1 IP-адрес сервера по умолчанию	104
7.4.2 Переадресация портов: сетевые службы и номера портов	104
7.4.3 Настройка серверов с переадресацией портов (пример)	105
7.5 Настройка переадресации портов	105
7.5.1 Редактирование правил переадресации портов	107
7.6 Address Mapping	107
7.6.1 Редактирование правила привязки адресов	109
Часть III: Безопасность	111
Глава 8	
Фильтр.....	113
8.1 Настройка фильтра	113

Часть IV: Расширенная настройка.....	115
Глава 9	
Статическая маршрутизация	117
9.1 Статический маршрут	117
9.2 Настройка статических маршрутов	117
9.2.1 Редактирование статического маршрута	118
Глава 10	
Настройка DNS для динамических адресов	121
10.1 Обзор поддержки DNS для динамических адресов	121
10.1.1 Шаблон DYNDNS	121
10.2 Настройка динамической DNS	121
Глава 11	
Настройка удаленного управления	125
11.1 Обзор удаленного управления	125
11.1.1 Ограничения удаленного управления	125
11.1.2 Удаленное управление и NAT	126
11.1.3 Системный таймер неактивности	126
11.2 WWW	126
11.3 Telnet	127
11.4 Настройка Telnet	127
11.5 Настройка FTP	128
11.6 SNMP	129
11.6.1 Поддерживаемые базы MIB	130
11.6.2 Прерывания SNMP	130
11.6.3 Настройка SNMP	131
11.7 Настройка DNS	132
11.8 Настройка ICMP	133
Глава 12	
Универсальная технология “включи и работай” (UPnP)	135
12.1 Обзор технологии UPnP	135
12.1.1 Как определить, используется ли UPnP?	135
12.1.2 Прослеживание NAT	135
12.1.3 Предостережения по отношению к UPnP	136
12.2 UPnP и ZyXEL	136
12.2.1 Настройка UPnP	136
12.3 Пример установки UPnP в Windows	137
12.4 Пример использования UPnP в Windows XP	140

Часть V: Сопровождение 147**Глава 13
Экран System 149**

- 13.1 Общая настройка 149
 - 13.1.1 Разделы General Setup и System Name 149
 - 13.1.2 Общая настройка 149
- 13.2 Установка часов 151

**Глава 14
Журналы 155**

- 14.1 Обзор средств ведения журналов 155
 - 14.1.1 Журналы и предупреждения 155
- 14.2 Просмотр журналов 155
- 14.3 Настройка параметров ведения журналов 156

**Глава 15
Системные инструменты 159**

- 15.1 Обновление микропрограммы 159
- 15.2 Экран Configuration 161
- 15.3 Restart 163

**Глава 16
Диагностика 165**

- 16.1 Общая диагностика 165
- 16.2 Экран DSL Line Diagnostic 165

Часть VI: Использование SMT и устранение неполадок 167**Глава 17
Введение в SMT 169**

- 17.1 Получение доступа к SMT через порт консоли 169
- 17.2 Получение доступа к SMT через Telnet 169
- 17.3 Структура меню SMT 170
- 17.4 Использование интерфейса SMT 174

**Глава 18
Общая настройка 175**

- 18.1 Задание общих настроек 175
 - 18.1.1 Настройка динамической DNS 176

Глава 19	
Настройка WAN.....	179
19.1 Настройка WAN	179
19.2 Настройка перенаправления трафика	181
19.3 Интерфейс резервирования через коммутируемый доступ	182
19.4 Настройка резервирования через коммутируемый доступ в меню 2	182
19.5 Расширенная настройка резервирования через коммутируемый доступ	183
Глава 20	
Настройка LAN.....	185
20.1 Вход в меню LAN	185
20.2 Меню LAN Port Filter Setup	185
20.3 Меню TCP/IP and DHCP Setup	186
20.4 Совмещение IP-адресов в локальной сети	188
Глава 21	
Настройка доступа к Интернету	191
21.1 Настройка доступа к Интернету	191
Глава 22	
Настройка удаленного узла.....	195
22.1 Введение в настройку удаленного узла	195
22.2 Настройка удаленного узла	195
22.3 Профиль удаленного узла	195
22.4 Опции сетевого уровня удаленного узла	199
22.5 Фильтр удаленного узла.	202
22.6 Параметры уровня ATM для удаленного узла	203
22.7 Специальные параметры настройки	204
Глава 23	
Настройка статического маршрута	207
23.1 Настройка статического IP-маршрута	207
23.2 Настройка статического маршрута в режиме моста	208
Глава 24	
Настройка NAT	211
24.1 Использование NAT	211
24.1.1 Сравнение SUA и других режимов NAT	211
24.1.2 Применение NAT	211
24.2 Настройка NAT	213
24.2.1 Наборы привязки адресов	213
24.3 Настройка сервера, находящегося за NAT	217
24.4 Общие примеры NAT	218

24.4.1 Пример 1: только доступ к Интернету	218
24.4.2 Пример 2: доступ к Интернету с использованием внутреннего сервера по умолчанию	220
24.4.3 Пример 3: несколько общедоступных IP-адресов с использованием внутренних серверов	220
24.4.4 Пример 4: программы, несовместимые с NAT	224
Глава 25	
Настройка фильтра.....	227
25.1 Основы применения фильтров	227
25.1.1 Структура фильтров устройства P-791R v2	228
25.2 Настройка набора фильтров	230
25.2.1 Настройка правила фильтра	231
25.2.2 Настройка правила фильтра TCP/IP	232
25.2.3 Настройка универсального правила фильтра	234
25.3 Пример фильтра	236
25.4 Типы фильтров и NAT	238
25.5 Применение фильтра	239
25.5.1 Применение фильтров LAN	239
25.5.2 Применение фильтров удаленного узла	239
Глава 26	
Настройка SNMP.....	241
26.1 Настройка SNMP	241
Глава 27	
Системный пароль	243
Глава 28	
Информация о системе и диагностика	245
28.1 Обзор средств наблюдения за состоянием системы	245
28.2 Меню System Status	245
28.3 System Information and Console Port Speed	247
28.3.1 Информация о системе	248
28.3.2 Настройка скорости консольного порта	248
28.4 Регистрация и трассировка	249
28.4.1 Просмотр журнала ошибок	249
28.4.2 Ведение журнала на SYSLOG-сервере	250
28.5 Диагностика	252
Глава 29	
Работа с файлами микропрограмм и настроек.....	255
29.1 Введение	255
29.2 Принятая схема именования файлов	255

29.3 Backup Configuration	256
29.3.1 Резервное копирование настроек	257
29.3.2 Выполнение команды FTP из командной строки	257
29.3.3 Пример выполнения команд FTP из командной строки	257
29.3.4 Клиенты FTP на основе графического интерфейса пользователя	258
29.3.5 Управление файлами через WAN	258
29.3.6 Резервное копирование настроек посредством TFTP	258
29.3.7 Пример команды TFTP	259
29.3.8 Клиенты TFTP на основе графического интерфейса пользователя	259
29.3.9 Резервное копирование через консольный порт	260
29.4 Восстановление настроек	261
29.4.1 Восстановление с использованием FTP	261
29.4.2 Пример восстановления с использованием сеанса FTP	262
29.4.3 Восстановление через консольный порт	262
29.5 Загрузка микропрограммы и файлов настроек в устройство	263
29.5.1 Загрузка файла микропрограммы в устройство	263
29.5.2 Загрузка файла настроек в устройство	264
29.5.3 Пример команды загрузки файла по FTP из приглашения DOS	264
29.5.4 Пример сессии FTP для загрузки файла микропрограммы	265
29.5.5 Загрузка файла по протоколу TFTP	265
29.5.6 Пример команды загрузки по TFTP	266
29.5.7 Загрузка файлов в устройство через консольный порт	266
29.5.8 Загрузка файлов микропрограммы через консольный порт	266
29.5.9 Пример загрузки файла микропрограммы по протоколу Xmodem с помощью программы HyperTerminal	267
29.5.10 Загрузка файлов настроек через консольный порт	267
29.5.11 Пример загрузки файла настроек по протоколу Xmodem с помощью программы HyperTerminal	268
Глава 30	
Разделы меню с 24.8 по 24.11	269
30.1 Режим интерпретатора команд	269
30.1.1 Синтаксис команд	269
30.1.2 Использование команд	270
30.2 Поддержка управления вызовами	270
30.2.1 Управление бюджетом	271
30.3 Установка даты и времени	272
30.4 Удаленное управление	274
30.4.1 Ограничения удаленного управления	275
Глава 31	
Настройка политик маршрутизации IP	277
31.1 Назначение политик маршрутизации	277

31.2 Преимущества	277
31.3 Политики маршрутизации	278
31.4 IP Routing Policy Setup	278
31.5 IP Routing Policy Setup	279
31.6 Меню IP Routing Policy	280
31.7 Пример IP-маршрутизации с использованием политик	282
Глава 32	
Настройка расписания	285
32.1 Краткие сведения о наборах расписаний	285
32.2 Настройка расписания	285
32.3 Настройка набора расписаний	286
Глава 33	
Поиск и устранение неполадок	289
33.1 Питание, подключение оборудования, светодиоды	289
33.2 Доступ к на P-791R v2 и вход в систему	290
33.3 Доступ к Интернету	292
33.4 Сброс на P-791R v2 к заводским настройкам	293
Часть VII: Приложения	
и предметный указатель	295
Приложение А Технические характеристики	297
Приложение В Настройка IP-адреса компьютера	303
Приложение С Разрешение всплывающих окон, сценариев JavaScript и апплетов Java319	
Приложение D IP-адреса и деление на подсети	327
Приложение E Конфликты в присвоении IP-адресов.....	337
Приложение F Распространенные сетевые службы.....	341
Приложение G Интерпретатор команд.....	345
Приложение H Формат журналов	351
Приложение I Команды фильтрации NetBIOS	363
Приложение J Авторское право	365
Приложение К Важная информация	367
Приложение L Юридический адрес изготовителя	369

Приложение М Гарантийное обслуживание ZyXEL.....	371
Приложение N О компании ZyXEL.....	373
Указатель	375

Список рисунков

Рис. 1	Высокоскоростной доступ в Интернет с P-791R v2	33
Рис. 2	Соединение по схеме "точка-точка" с помощью P-791R v2	34
Рис. 3	Светодиоды	35
Рис. 4	Экран входа	38
Рис. 5	Смена пароля при входе в систему	38
Рис. 6	Выбор режима	39
Рис. 7	Веб-конфигуратор: основной экран	40
Рис. 8	Status	43
Рис. 9	Экран Status > Packet Statistics	45
Рис. 10	Выбор режима	50
Рис. 11	Мастер: экран приветствия	50
Рис. 12	Мастер настройки доступа к Интернету: параметры поставщика услуг Интернета	51
Рис. 13	Настройка доступа в Интернет посредством PPPoE	52
Рис. 14	Настройка доступа в Интернет посредством RFC 1483	52
Рис. 15	Подключение к Интернету с использованием инкапсуляции ENET ENCAP	53
Рис. 16	Настройка доступа в Интернет посредством PPPoA	54
Рис. 17	Ошибка при проверке подключения – 1	55
Рис. 18	Ошибка при проверке подключения – 2	55
Рис. 19	Мастер настройки доступа в Интернет	55
Рис. 20	Пример: обзор соединений по схеме "точка-точка"	57
Рис. 21	Экран WAN > Internet Connection > Service Type	58
Рис. 22	Пример ограничения трафика	67
Рис. 23	Экран WAN > Internet Connection	69
Рис. 24	Экран WAN > Internet Connection > Advanced Setup	72
Рис. 25	Экран WAN > More Connections	74
Рис. 26	Экран WAN > More Connections > Edit	75
Рис. 27	Экран WAN > More Connections > Advanced Setup	77
Рис. 28	Пример переадресации трафика	79
Рис. 29	Настройка LAN для переадресации трафика	79
Рис. 30	Экран WAN > WAN Backup Setup	80
Рис. 31	Экран WAN > WAN Backup Setup > Advanced Setup	83
Рис. 32	Экран WAN > WAN Backup Setup > Advanced Setup > Edit	85
Рис. 33	IP-адреса в сетях LAN и WAN	87
Рис. 34	Экран LAN > IP	92
Рис. 35	Экран LAN > IP > Advanced Setup	92
Рис. 36	Экран LAN > DHCP Setup	94
Рис. 37	Экран LAN > Client List	95
Рис. 38	Физическая сеть и отдельные логические сети	96

Рис. 39 Экран LAN > IP Alias	97
Рис. 40 Принцип работы NAT	100
Рис. 41 Применение NAT с IP-псевдонимом	101
Рис. 42 Экран NAT > General	103
Рис. 43 Пример нескольких серверов, закрытых функцией NAT	105
Рис. 44 Экран NAT > Port Forwarding	106
Рис. 45 Экран NAT > Port Forwarding > Edit	107
Рис. 46 Экран NAT > Address Mapping	108
Рис. 47 Экран NAT > Address Mapping > Edit	109
Рис. 48 Security > Filter (Фильтр безопасности)	113
Рис. 49 Пример топологии статической маршрутизации	117
Рис. 50 Экран Static Route > Static Route	118
Рис. 51 Экран Static Route > Static Route > Edit	119
Рис. 52 Экран Dynamic DNS > Dynamic DNS	122
Рис. 53 Экран Remote MGMT > WWW	126
Рис. 54 Настройка Telnet в сети TCP/IP	127
Рис. 55 Экран Remote MGMT > Telnet	127
Рис. 56 Экран Remote MGMT > FTP	128
Рис. 57 Модель управления по протоколу SNMP	129
Рис. 58 Экран Remote MGMT > SNMP	131
Рис. 59 Экран Remote MGMT > DNS	132
Рис. 60 Экран Remote MGMT > ICMP	133
Рис. 61 Экран UPnP > General	136
Рис. 62 Установка и удаление программ: установка Windows: Связь	138
Рис. 63 Установка и удаление программ: установка Windows: Связь: Компоненты	138
Рис. 64 Сетевые подключения	139
Рис. 65 Мастер дополнительных сетевых компонентов Windows	139
Рис. 66 Сетевые службы	140
Рис. 67 Сетевые подключения	141
Рис. 68 Свойства подключения к Интернету	141
Рис. 69 Свойства подключения к Интернету: дополнительные параметры	142
Рис. 70 Свойства подключения к Интернету: расширенные параметры: добавление	142
Рис. 71 Значок в области уведомлений	142
Рис. 72 Состояние подключения к Интернету	143
Рис. 73 Сетевые подключения	144
Рис. 74 Сетевые подключения: сетевое окружение	145
Рис. 75 Сетевые подключения: сетевое окружение: свойства: пример	145
Рис. 76 Экран System > General	150
Рис. 77 Экран System > Time Setting	151
Рис. 78 Экран Logs > View Log	156
Рис. 79 Экран Logs > Log Settings	157
Рис. 80 Экран Tools > Firmware	159
Рис. 81 Выполнение загрузки микропрограммы	160

Рис. 82 Сеть временно недоступна	160
Рис. 83 Сообщение об ошибке	161
Рис. 84 Экран Tools > Configuration	161
Рис. 85 Загрузка настроек выполнена успешно	162
Рис. 86 Сеть временно недоступна	162
Рис. 87 Ошибка при загрузке настроек	163
Рис. 88 Экран Tools > Restart	163
Рис. 89 Экран Diagnostic > General	165
Рис. 90 Экран Diagnostic > DSL Line	166
Рис. 91 Экран входа	169
Рис. 92 Главное меню SMT	170
Рис. 93 Меню 1: общая настройка	175
Рис. 94 Меню 1.1: настройка DNS для динамических адресов	177
Рис. 95 Меню 2: настройка WAN	179
Рис. 96 Меню 2.1: настройка перенаправления трафика	181
Рис. 97 Меню 2.2: настройка резервирования через коммутируемый доступ	182
Рис. 98 Меню 2.2.1: расширенная настройка резервирования через коммутируемый доступ	183
Рис. 99 Меню 3: настройка LAN	185
Рис. 100 Меню 3.1: настройка фильтров для порта LAN	185
Рис. 101 Меню 3.2: настройка TCP/IP и DHCP для Ethernet	186
Рис. 102 Меню 3.2.1: настройка совмещения IP-адресов	188
Рис. 103 Меню 4: настройка доступа к Интернету	191
Рис. 104 Меню 11: Remote Node Setup	195
Рис. 105 Меню 11.1: профиль удаленного узла (узлы 1 – 7)	196
Рис. 106 Меню 11.1: профиль удаленного узла (узел 8)	198
Рис. 107 Меню 11.3: опции сетевого уровня удаленного узла	200
Рис. 108 Меню 11.5: фильтр удаленного узла.	202
Рис. 109 Меню 11.6: параметры уровня ATM для удаленного узла	203
Рис. 110 Меню 11.8: специальные параметры настройки	204
Рис. 111 Меню 12.1: настройка статического IP-маршрута	207
Рис. 112 Меню 12.1.1: редактирование статического IP-маршрута	208
Рис. 113 Меню 12.3: настройка статического маршрута в режиме моста	209
Рис. 114 Меню 12.3.1: редактирование статического маршрута моста	209
Рис. 115 Меню 4: применение NAT для доступа к Интернету	212
Рис. 116 Меню 11.3: применение NAT к удаленному узлу	212
Рис. 117 Меню 15: NAT Setup	213
Рис. 118 Меню 15.1: наборы привязки адресов	214
Рис. 119 Меню 15.1.1: правила привязки адресов	214
Рис. 120 Меню 15.1.1.1: правило привязки адресов	216
Рис. 121 Меню 15.2: наборы серверов NAT	217
Рис. 122 Меню 15.2: настройка NAT в режиме сервера	218
Рис. 123 NAT: пример 1	219
Рис. 124 Меню 4: пример применения NAT для доступа в Интернет	219

Рис. 125 NAT: пример 2	220
Рис. 126 Меню 15.2: указание внутреннего сервера	220
Рис. 127 NAT: пример 3	221
Рис. 128 Пример 3: меню 11.3	222
Рис. 129 Пример 3: меню 15.1.1.1	222
Рис. 130 Пример 3: заключительное меню 15.1.1	223
Рис. 131 Пример 3: меню 15.2	223
Рис. 132 NAT: пример 4	224
Рис. 133 Пример 4: меню 15.1.1.1: правило привязки адресов	224
Рис. 134 Пример 4: меню 15.1.1: правила привязки адресов	225
Рис. 135 Процесс фильтрации исходящих пакетов	227
Рис. 136 Процесс выполнения правил фильтра	229
Рис. 137 Меню 21: настройка набора фильтров	230
Рис. 138 Меню 21.1: сводка правил фильтра	230
Рис. 139 Меню 21.1.1: правила фильтров TCP/IP	232
Рис. 140 Выполнение фильтра IP	234
Рис. 141 Меню 21.1.1: универсальное правило фильтра	235
Рис. 142 Пример фильтра для Telnet	236
Рис. 143 Пример фильтра: меню 21.1.1	237
Рис. 144 Пример сводки правил фильтров: меню 21.1.	237
Рис. 145 Наборы фильтров протокола и устройства	238
Рис. 146 Фильтрация трафика LAN	239
Рис. 147 Фильтрация трафика удалённого узла	239
Рис. 148 Меню 22: SNMP Configuration	241
Рис. 149 Меню 23: системный пароль	243
Рис. 150 Меню 24: обслуживание системы	245
Рис. 151 Меню 24.1: состояние системы	246
Рис. 152 Меню 24.2: System Information and Console Port Speed	247
Рис. 153 Меню 24.2.1: обслуживание системы – информация	248
Рис. 154 Меню 24.2.2: обслуживание системы: изменение скорости консольного порта	249
Рис. 155 Меню 24.3: обслуживание системы – журналы и трассировка	249
Рис. 156 Примеры ошибок и информационных сообщений	250
Рис. 157 Меню 24.3.2: обслуживание системы – UNIX SYSLOG	250
Рис. 158 Меню 24.4: обслуживание системы - диагностика	253
Рис. 159 Меню 24.5: Backup Configuration	257
Рис. 160 Пример сеанса FTP	257
Рис. 161 Обслуживание системы: Backup Configuration	260
Рис. 162 Обслуживание системы: экран начала приема файла по Xmodem	260
Рис. 163 Пример резервного копирования настроек	260
Рис. 164 Экран подтверждения выполнения резервного копирования	260
Рис. 165 Меню 24.6: Restore Configuration	261
Рис. 166 Пример восстановления с использованием сеанса FTP	262
Рис. 167 Обслуживание системы: Restore Configuration	262

Рис. 168 Обслуживание системы: экран начала приема файла по Xmodem	262
Рис. 169 Пример восстановления настроек	263
Рис. 170 Экран подтверждения восстановления настроек	263
Рис. 171 Меню 24.7.1: обслуживание системы – загрузка микропрограммы	264
Рис. 172 Меню 24.7.2: обслуживание системы – загрузка файла настроек	264
Рис. 173 Пример сессии FTP для загрузки файла микропрограммы	265
Рис. 174 Меню 24.7.1 при доступе через консольный порт	267
Рис. 175 Пример загрузки Xmodem	267
Рис. 176 Меню 24.7.2 при доступе через консольный порт	268
Рис. 177 Пример загрузки по Xmodem	268
Рис. 178 Режим команд в меню 24	269
Рис. 179 Допустимые команды	270
Рис. 180 Меню 24.9: обслуживание системы – управление вызовами	270
Рис. 181 Меню 24.9.1 - Budget Management	271
Рис. 182 Меню 24: обслуживание системы	272
Рис. 183 Меню 24.10: управление системой – настройка времени и даты	272
Рис. 184 Меню 24.11 – настройка удаленного управления	274
Рис. 185 Меню 25: IP Routing Policy Setup	278
Рис. 186 Меню 25.1: IP Routing Policy Setup	279
Рис. 187 Меню 25.1.1: меню IP Routing Policy	280
Рис. 188 Пример IP-маршрутизации с использованием политик	282
Рис. 189 Политика маршрутизации IP. Пример 1.	283
Рис. 190 Политика маршрутизации IP. Пример 2.	283
Рис. 191 Меню 26: настройка расписания	285
Рис. 192 Меню 26.1: настройка набора расписаний	286
Рис. 193 Пример монтажа на стене	301
Рис. 194 Пробка и винт M4	301
Рис. 195 Windows 95/98/Me: Сеть: Configuration	304
Рис. 196 Windows 95/98/Me: Свойства TCP/IP: IP-адрес	305
Рис. 197 Windows 95/98/Me: Свойства TCP/IP: Конфигурация DNS	306
Рис. 198 Windows XP: меню Пуск	307
Рис. 199 Windows XP: Панель управления	307
Рис. 200 Windows XP: Панель управления: Сетевые подключения: Свойства	308
Рис. 201 Windows XP: Свойства подключения по локальной сети	308
Рис. 202 Windows XP: Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP)) 309	
Рис. 203 Windows XP: Дополнительные параметры TCP/IP	310
Рис. 204 Windows XP: Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP)) 311	
Рис. 205 Macintosh OS 8/9: меню Apple	312
Рис. 206 Macintosh OS 8/9: TCP/IP	312
Рис. 207 Macintosh OS X: меню Apple	313
Рис. 208 Macintosh OS X: Сеть	314

Рис. 209 Red Hat 9.0: KDE: настройка сети: устройства	315
Рис. 210 Red Hat 9.0: KDE: устройство Ethernet: общие настройки	316
Рис. 211 Red Hat 9.0: KDE: настройка сети: DNS	316
Рис. 212 Red Hat 9.0: KDE: настройка сети: активация	317
Рис. 213 Red Hat 9.0: задание динамического IP-адреса в файле ifconfig-eth0	317
Рис. 214 Red Hat 9.0: задание статического IP-адреса в файле ifconfig-eth0	317
Рис. 215 Red Hat 9.0: настройка DNS в файле resolv.conf	318
Рис. 216 Red Hat 9.0: повторная инициализация сетевой платы	318
Рис. 217 Red Hat 9.0: проверка параметров TCP/IP	318
Рис. 218 Блокирование всплывающих окон	320
Рис. 219 Свойства обозревателя: Конфиденциальность	320
Рис. 220 Свойства обозревателя: Конфиденциальность	321
Рис. 221 Параметры блокирования всплывающих окон	322
Рис. 222 Свойства обозревателя: Security	323
Рис. 223 Параметры безопасности – сценарии JavaScript	324
Рис. 224 Параметры безопасности – Java-апплеты	325
Рис. 225 Java (Sun)	325
Рис. 226 Номер сети и идентификатор хоста	328
Рис. 227 Пример деления на подсети: до деления	330
Рис. 228 Пример деления на подсети: после деления	331
Рис. 229 Конфликты IP-адресов: случай А	337
Рис. 230 Конфликты IP-адресов: случай В	338
Рис. 231 Конфликты IP-адресов: случай С	338
Рис. 232 Конфликты IP-адресов: случай D:	339
Рис. 233 Пример просмотра списка категорий журналов	346
Рис. 234 Пример просмотра параметров ведения журнала	346
Рис. 235 Пример вызова команды routing	347
Рис. 236 Резервный шлюз	349
Рис. 237 Пример просмотра списка категорий журналов	361
Рис. 238 Пример просмотра параметров ведения журнала	362

Список таблиц

Таблица 1 Светодиоды	35
Таблица 2 Сводка экранов веб-конфигуратора	40
Таблица 3 Экран Status	43
Таблица 4 Экран Status > Packet Statistics	45
Таблица 5 Мастер настройки доступа к Интернету: параметры поставщика услуг Интернета	51
Таблица 6 Настройка доступа в Интернет посредством PPPoE	52
Таблица 7 Настройка доступа в Интернет посредством RFC 1483	53
Таблица 8 Подключение к Интернету с использованием инкапсуляции ENET ENCAP	53
Таблица 9 Настройка доступа в Интернет посредством PPPoA	54
Таблица 10 Экран WAN > Internet Connection	69
Таблица 11 Экран WAN > Internet Connection > Advanced Setup	72
Таблица 12 Экран WAN > More Connections	74
Таблица 13 Экран WAN > More Connections > Edit	75
Таблица 14 Экран WAN > More Connections > Advanced Setup	77
Таблица 15 Экран WAN > WAN Backup Setup	81
Таблица 16 Экран WAN > WAN Backup Setup > Advanced Setup	83
Таблица 17 Экран WAN > WAN Backup Setup > Advanced Setup > Edit	86
Таблица 18 Экран LAN > IP	92
Таблица 19 Экран LAN > IP > Advanced Setup	93
Таблица 20 Экран LAN > DHCP Setup	94
Таблица 21 Экран LAN > Client List	95
Таблица 22 Экран LAN > IP Alias	97
Таблица 23 Определения, относящиеся к NAT	99
Таблица 24 Типы привязки NAT	102
Таблица 25 Общие настройки NAT	103
Таблица 26 Экран NAT > Port Forwarding	106
Таблица 27 Экран NAT > Port Forwarding > Edit	107
Таблица 28 Экран NAT > Address Mapping	108
Таблица 29 Экран NAT > Address Mapping > Edit	110
Таблица 30 Защищенная реализация IP	113
Таблица 31 Экран Static Route > Static Route	118
Таблица 32 Экран Static Route > Static Route > Edit	119
Таблица 33 Экран Dynamic DNS > Dynamic DNS	122
Таблица 34 Экран Remote MGMT > WWW	126
Таблица 35 Экран Remote MGMT > Telnet	127
Таблица 36 Экран Remote MGMT > FTP	128
Таблица 37 Прерывания SNMPv1	130
Таблица 38 Прерывания SNMPv2	131

Таблица 39 Экран Remote MGMT > SNMP	131
Таблица 40 Экран Remote MGMT > DNS	133
Таблица 41 Экран Remote MGMT > ICMP	134
Таблица 42 Экран UPnP > General	137
Таблица 43 Экран System > General	150
Таблица 44 Экран System > Time Setting	152
Таблица 45 Экран Logs > View Log	156
Таблица 46 Экран Logs > Log Settings	157
Таблица 47 Экран Tools > Firmware	159
Таблица 48 Экран Tools > Configuration	161
Таблица 49 Экран Diagnostic > General	165
Таблица 50 Экран Diagnostic > DSL Line	166
Таблица 51 Краткий обзор главного меню	170
Таблица 52 Общая структура меню SMT	171
Таблица 53 Команды главного меню	174
Таблица 54 Меню 1: экран General Setup	175
Таблица 55 Меню 1.1: настройка DNS для динамических адресов	177
Таблица 56 Меню 2: настройка WAN	179
Таблица 57 Меню 2.1: настройка перенаправления трафика	181
Таблица 58 Меню 2.2: настройка резервирования через коммутируемый доступ	182
Таблица 59 Меню 2.2.1: расширенная настройка резервирования через коммутируемый доступ	183
Таблица 60 Меню 3.2: настройка TCP/IP и DHCP для Ethernet	186
Таблица 61 Меню 3.2.1: настройка совмещения IP-адресов	188
Таблица 62 Меню 4: настройка доступа к Интернету	191
Таблица 63 Меню 11.1: профиль удаленного узла (узлы 1 – 7)	196
Таблица 64 Меню 11.1: профиль удаленного узла (узел 8)	198
Таблица 65 Меню 11.3: параметры сетевого уровня для удаленного узла	200
Таблица 66 Меню 11.5: фильтр удаленного узла	202
Таблица 67 Меню 11.6: параметры уровня ATM для удаленного узла	203
Таблица 68 Меню 11.8: специальные параметры настройки	205
Таблица 69 Меню 12.1.1: редактирование статического маршрута IP	208
Таблица 70 Меню 12.3.1: редактирование статического маршрута моста	209
Таблица 71 Применение NAT в меню 4 и 11.3.	213
Таблица 72 Меню 15.1.1: правила привязки адресов	215
Таблица 73 Меню 15.1.1.1: правило привязки адресов	216
Таблица 74 Меню 15.2: настройка NAT в режиме сервера	218
Таблица 75 Аббревиатуры, используемые в меню сводки правил фильтров	231
Таблица 76 Используемые аббревиатуры правил	231
Таблица 77 Меню 21.1.1: правила фильтров TCP/IP	232
Таблица 78 Меню 21.1.1: универсальное правило фильтра	235
Таблица 79 Меню 22: настройка SNMP	241
Таблица 80 Меню 23: системный пароль	243

Таблица 81 Меню 24.1: состояние системы	246
Таблица 82 Меню 24.2.1: обслуживание системы – информация	248
Таблица 83 Меню 24.3.2: обслуживание системы - UNIX Syslog	250
Таблица 84 Меню 24.4: обслуживание системы – диагностика	253
Таблица 85 Принятая схема именования файлов	256
Таблица 86 Общие команды для клиентов FTP на основе GUI.	258
Таблица 87 Общие команды для клиентов TFTP на основе GUI	259
Таблица 88 Меню 24.9.1 – управление бюджетом	271
Таблица 89 Меню 24.10: управление системой – настройка времени и даты	273
Таблица 90 Меню 24.11 – настройка удаленного управления	274
Таблица 91 Меню 25.1: настройка политик маршрутизации IP	279
Таблица 92 Меню 25: настройка политик маршрутизации IP, сокращения	279
Таблица 93 Меню 25.1.1: политика маршрутизации IP	280
Таблица 94 Меню 26: настройка расписания	286
Таблица 95 Меню 26.1: настройка набора расписаний	287
Таблица 96 Технические характеристики	297
Таблица 98 Функциональные возможности микропрограммы	298
Таблица 97 Микропрограмма	298
Таблица 99 Поддерживаемые стандарты	299
Таблица 100 Пример номера сети и идентификатора хоста в IP-адресе	328
Таблица 101 Маски подсетей	329
Таблица 102 Максимально возможное число хостов	329
Таблица 103 Альтернативный способ записи маски подсети	330
Таблица 104 Подсеть 1	332
Таблица 105 Подсеть 2	332
Таблица 106 Подсеть 3	332
Таблица 107 Подсеть 4	332
Таблица 108 Восемь подсетей	333
Таблица 109 Планирование подсетей в сети с 24-битным номером	333
Таблица 110 Планирование подсетей в сети с 16-битным номером	334
Таблица 111 Часто используемые сетевые службы	341
Таблица 112 Журналы обслуживания системы	351
Таблица 113 Системные журналы ошибок	352
Таблица 114 Журналы контроля доступа	352
Таблица 115 Журналы пакетов сброса TCP	352
Таблица 116 Журналы фильтрации пакетов	353
Таблица 117 Журналы ICMP	353
Таблица 118 Журналы вызовов (CDR)	353
Таблица 119 Журналы PPP	353
Таблица 120 Журналы IKE	354
Таблица 121 Журналы PKI	357
Таблица 122 Коды причин непрохождения проверки сертификата	358
Таблица 123 Замечания по заданию ACL	359

Таблица 124 Пояснения к кодам ICMP	359
Таблица 125 Журналы SYSLOG	360
Таблица 126 Типы полезной нагрузки ISAKMP по стандарту RFC-2408	361
Таблица 127 Настройки фильтра NetBIOS по умолчанию	364

ЧАСТЬ I

Краткое введение и настройка с помощью мастеров

Краткое знакомство с P-791R v2 (33)
Знакомство с веб-конфигуратором (37)
Мастер настройки доступа к Интернету (49)
Прямые соединения (57)

Краткое знакомство с P-791R v2

В этой главе описаны основные характеристики и функции P-791R v2.

1.1 Общие сведения

Устройство P-791R v2 — это маршрутизатор G.SHDSL (G.992.1, симметричный высокоскоростной абонентский цифровой канал).bis, предоставляющий высокоскоростную связь между локальными сетями и доступ к Интернету с помощью подключения G.SHDSL.bis по телефонной линии. В зависимости от настроек поставщика услуг Интернета (ISP) P-791R v2 можно использовать как для IP-маршрутизации, так и для установки мостов.

[Приложение А на стр. 297](#) содержит развернутый список функций, настраиваемых в вашем P-791R v2.

1.1.1 Высокоскоростной доступ в Интернет

P-791R v2 будет идеальным решением для высокоскоростного доступа в Интернет. Помимо других преимуществ, стандарт G.SHDSL.bis поддерживает одинаково высокую скорость передачи и приема, что отличает его от ADSL и VDSL.

Рис. 1 Высокоскоростной доступ в Интернет с P-791R v2



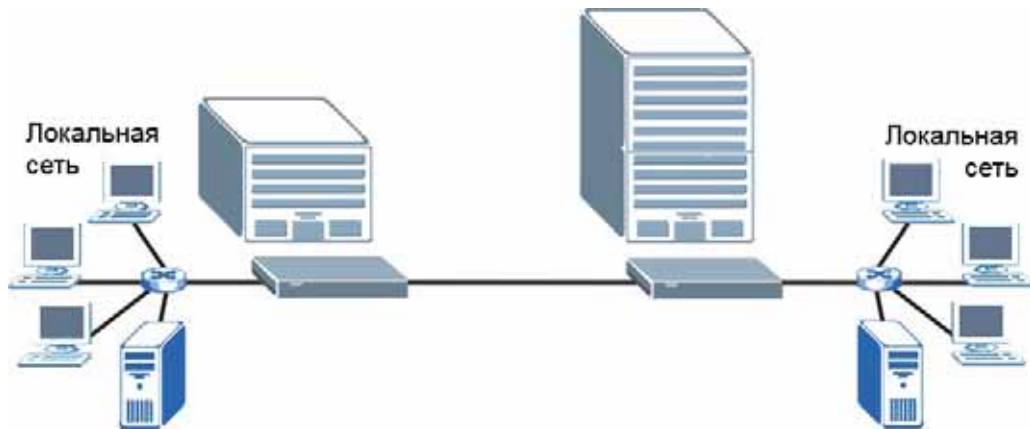
Для доступа в Интернет соедините порт DSL с телефонным портом. Затем подключите ваш компьютер или сервер к порту ETHERNET. (Подробные указания по подключению аппаратной части см. в Руководстве по быстрому запуску.) Далее настройте устройство P-791R v2 в режиме маршрутизатора или моста в зависимости от требуемой конфигурации. Поскольку устройство P-791R v2 является маршрутизатором, оно обеспечивает функции защиты и связи. Применение P-791R v2 в роли моста сводит к минимуму объем необходимых изменений в настройках существующей сети.

1.1.2 Высокоскоростные соединения по схеме “точка-точка”

С помощью двух устройств P-791R v2 можно построить недорогое высокоскоростное соединение для таких требовательных к полосе пропускания задач, как видеоконференции и дистанционное обучение. Устройства P-791R v2 позволяют создавать простые и высокоскоростные двухточечные соединения между двумя территориально разнесенными сетями.

В приведенном ниже примере два P-791R v2 соединяют штаб-квартиру корпорации с ее филиалом.

Рис. 2 Соединение по схеме “точка-точка” с помощью P-791R v2



См. [гл. 4 на стр. 57](#) для получения дополнительной информации о настройке соединений по схеме “точка-точка”.

1.2 Способы управления P-791R v2

Управлять устройством P-791R v2 можно одним из следующих способов.

- Веб-конфигуратор. Это рекомендуемый способ решения повседневных задач управления устройством P-791R v2. Необходим только поддерживаемый веб-браузер. См. [гл. 2 на стр. 37](#).
- Интерфейс командной строки. Командная строка используется для устранения неполадок инженерами сервисных служб. См. [Приложение G на стр. 345](#).
- SMT. SMT (терминал управления системой) представляет собой текстовый интерфейс на основе меню, позволяющий настраивать устройство. См. [гл. 17 на стр. 169](#).
- FTP. FTP (протокол передачи файлов) используется для обновления микропрограммы, а также резервного копирования и восстановления настроек. См. [гл. 11 на стр. 125](#).
- SNMP. Для контроля и управления устройством можно применять диспетчер SNMP. См. [гл. 11 на стр. 125](#).

1.3 Рекомендации по управлению P-791R v2

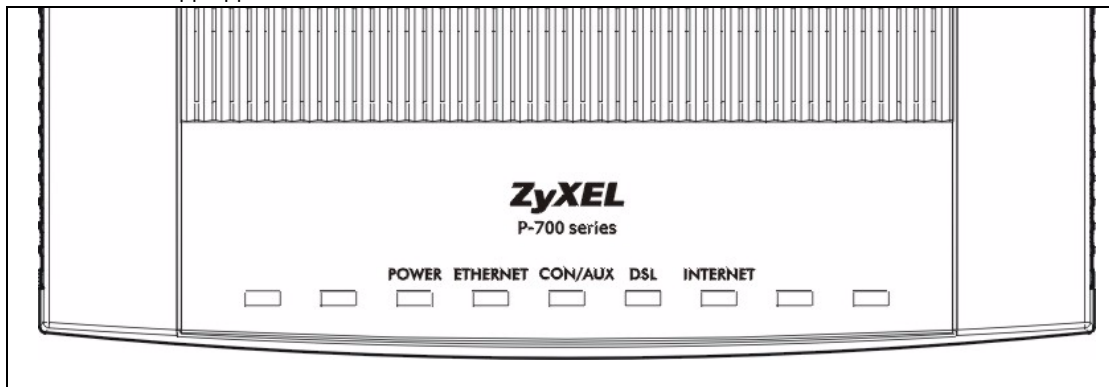
Чтобы максимально защитить P-791R v2 и сделать управление P-791R v2 более эффективным, регулярно выполняйте следующие профилактические операции.

- Меняйте пароль. Используйте пароли, которые сложно подобрать. Составляйте пароль из различных символов, например, цифр и букв.
- Записывайте пароли и храните их в защищенном месте.
- Выполняйте резервное копирование настроек (убедитесь в том, что вам известен способ их восстановления). Восстановление ранее работавших настроек может понадобиться, если устройство начнет работать неустойчиво или откажется функционировать. Если вы забудете пароль, потребуется восстановить заводские настройки P-791R v2. Наличие ранее сохраненного файла настроек означает, что вам не потребуется перенастраивать P-791R v2 заново. Будет достаточно восстановить последние действовавшие настройки.

1.4 Светодиоды

На следующем рисунке изображено расположение светодиодов.

Рис. 3 Светодиоды



Назначение светодиодов описано в следующей таблице.

Таблица 1 Светодиоды

СВЕТО-ДИОДЫ	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
POWER	Зелёный	Вкл.	Устройство P-791R v2 включено и функционирует исправно.
		Мигание	P-791R v2 перезагружается или проходит диагностику.
	Красный	Вкл.	Для работы P-791R v2 недостаточно питания.
		Выкл.	Система не готова или находится в состоянии сбоя.
CON/AUX	Зелёный	Вкл.	Порт успешно подключен к консоли.
	Оранжевый	Вкл.	Порт успешно подключен к коммутируемому соединению.
		Выкл.	Соединение на порту отсутствует.

Таблица 1 Светодиоды (продолжение)

СВЕТО-ДИОДЫ	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
ETHERNET	Зелёный	Вкл.	Порт успешно подключен к Ethernet-сети.
		Мигание	Порт передает/принимает данные.
		Выкл.	Соединение на порту отсутствует.
DSL	Зелёный	Вкл.	DSL-соединение установлено.
		Мигание	P-791R v2 инициализирует DSL-линию.
		Выкл.	DSL-линия разъединена.
INTERNET	Зелёный	Вкл.	Соединение с Интернетом установлено, и устройство P-791R v2 получило IP-адрес. (Если P-791R v2 организует соединение RFC 1483 в режиме моста, этот светодиод не загорается, но он мигает в то время, когда P-791R v2 передает или принимает данные.)
		Мигание	P-791R v2 передает/принимает данные.
	Красный	Вкл.	Устройство P-791R v2 предприняло попытку получить IP-адрес, но возникла ошибка.
		Выкл.	Соединение с Интернетом не установлено.

Знакомство с веб-конфигуратором

В этой главе будет рассказано, как вызвать веб-конфигуратор и как перемещаться по его экранам.

2.1 Обзор веб-конфигуратора

Веб-конфигуратор имеет HTML-интерфейс, поэтому настраивать устройство P-791R v2 и управлять им можно с помощью веб-браузера. Следует использовать Internet Explorer 6,0, Netscape Navigator 7,0 или более новые версии браузеров. Рекомендуем установить разрешение экрана 1024 x 768 пикселей.

Чтобы пользоваться веб-конфигуратором, нужно разрешить веб-браузеру следующее.

- На компьютере в веб-браузере нужно разрешить всплывающие окна. В операционной системе Windows XP SP с пакетом обновления 2 (SP2) всплывающие окна по умолчанию блокируются.
- Сценарии JavaScript (их выполнение разрешено по умолчанию).
- Разрешения на выполнение Java-кода (включены по умолчанию).

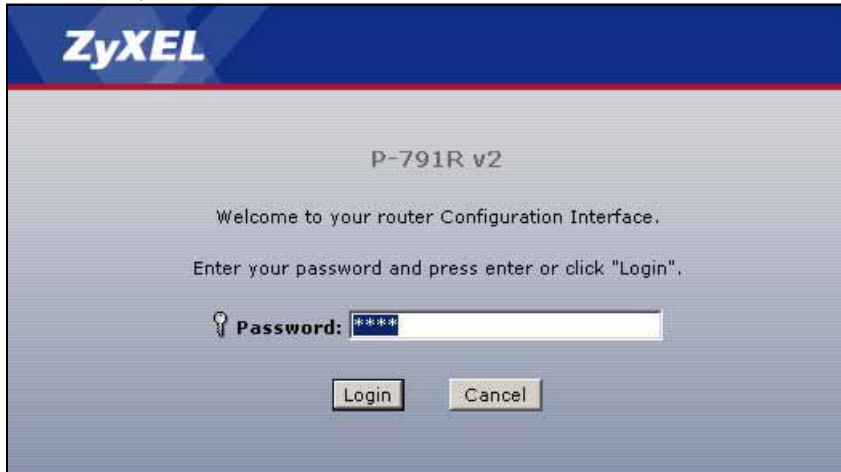
Проверка необходимых настроек Internet Explorer описана в главе, посвященной устранению проблем.

2.2 Вызов веб-конфигуратора

- 1 Убедитесь, что все аппаратные подключения P-791R v2 выполнены правильно (см. Руководство по быстрому запуску).
- 2 Подготовьте компьютер/сеть для соединения с P-791R v2 (см. Руководство по быстрому запуску).
- 3 Откройте веб-браузер.
- 4 Введите "192.168.1.1" в качестве URL.
- 5 Появляется экран, изображённый на следующем рисунке. Чтобы воспользоваться мастерами настройки или настроить дополнительные функции, введите пароль администратора по умолчанию: **1234**. Чтобы только просмотреть состояние устройства, введите пароль пользователя по умолчанию: **user**. Чтобы перейти на

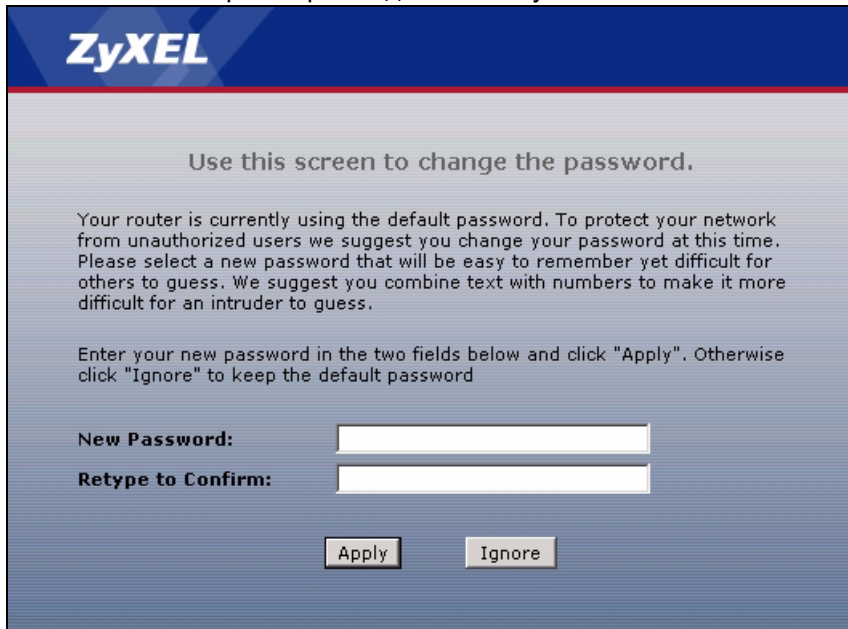
экран, на котором будет предложено изменить пароль, нажмите кнопку **Login**. Чтобы оставить устройство с паролем по умолчанию, выберите **Cancel**.

Рис. 4 Экран входа



6 Если был введен пароль пользователя, появится экран **Status**. См. [разд. 2.4 на стр. 42](#). Если введен пароль администратора, появится изображенный ниже экран.

Рис. 5 Смена пароля при входе в систему



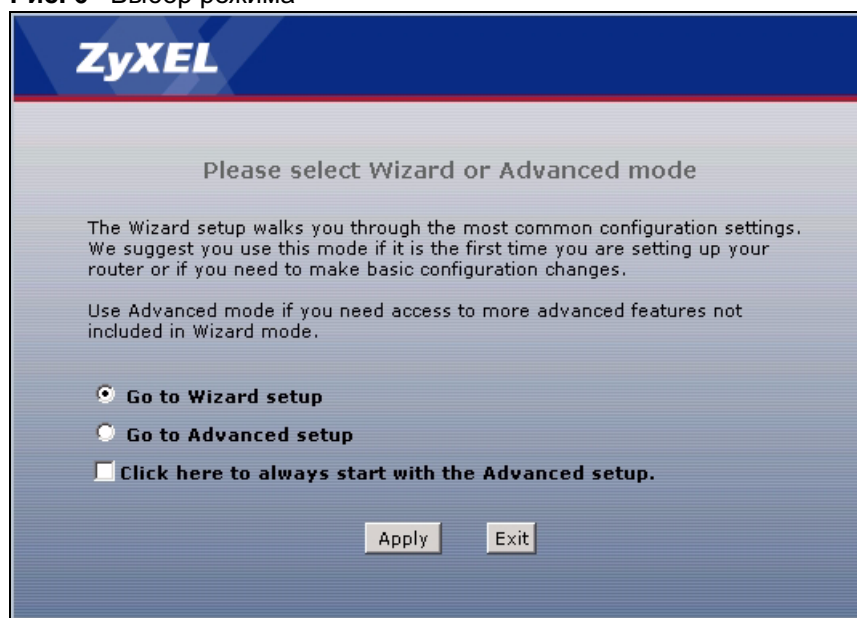
Настоятельно рекомендуется сменить пароль администратора по умолчанию. Введите новый пароль (от 1 до 30 знаков), повторно введите его для подтверждения и нажмите **Apply**. Если вы не хотите менять пароль, нажмите **Ignore**, чтобы перейти к главному меню.



Если пароль по умолчанию не будет сменен, этот экран продолжит появляться при каждом входе в систему с паролем администратора. Изменить пароль можно на экране [Экран System > General](#) или [Меню 23: системный пароль](#).

- 7 Чтобы открыть основной экран мастера, выберите **Go to Wizard setup** и нажмите кнопку **Apply**. Для перехода на экран **Status** выберите **Go to Advanced setup** и нажмите кнопку **Apply**. Отметьте флажок **Click here to always start with the Advanced setup**, чтобы отключить этот экран. После этого устройство P-791R v2 всегда будет открывать экран **Status**. См. [разд. 2.4 на стр. 42](#).

Рис. 6 Выбор режима

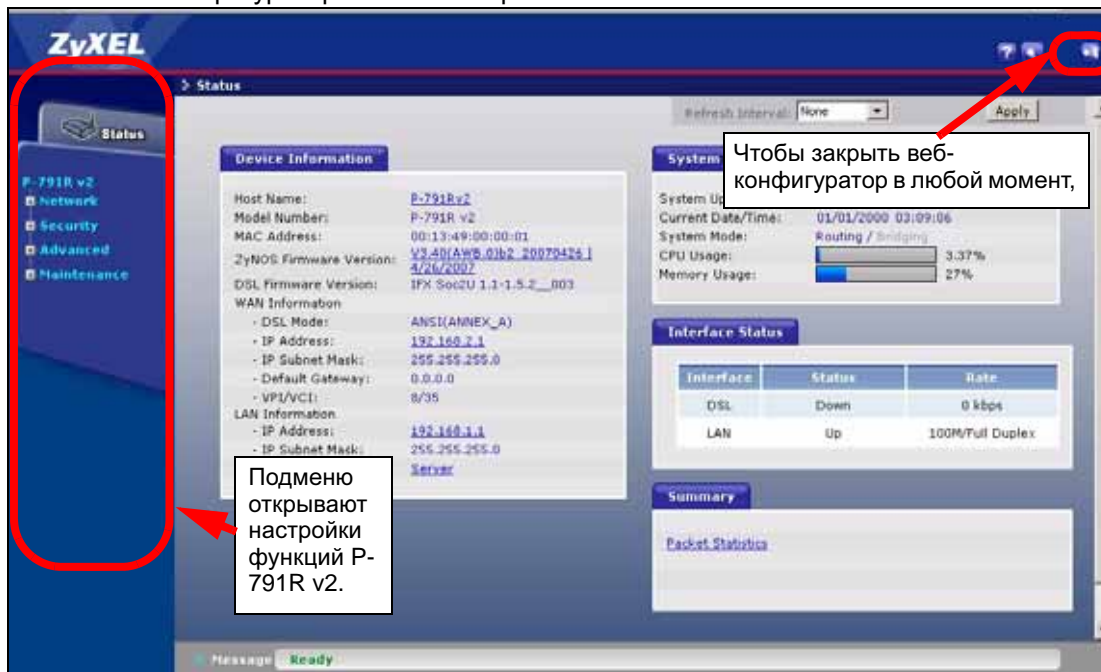


Сеанс управления автоматически прерывается по истечении периода неактивности, заданного в поле **Administrator Inactivity Timer** (по умолчанию – пять минут). В этом случае для возобновления сеанса достаточно повторно войти в управление P-791R v2.

2.3 Навигация в веб-конфигураторе

Введя пароль администратора, можно перейти к настройке функций P-791R v2 через подменю на навигационной панели. Эти подменю описаны в следующей таблице.

Рис. 7 Веб-конфигуратор: основной экран




Для просмотра встроенной справки щелкните на значке  (он расположен в правом верхнем углу на большинстве экранов).

Таблица 2 Сводка экранов веб-конфигуратора



ССЫЛКА/ ЗНАЧОК	ПОДРАЗДЕЛ	НАЗНАЧЕНИЕ
Мастер 	INTERNET SETUP	Эти экраны служат для запуска процесса начальной настройки, включающего общую настройку, установку параметров поставщика услуг Интернета и назначение IP-адреса в сети, DNS-сервера и MAC-адреса.
Logout 		Этот значок служит для выхода из веб-конфигуратора.
Status		Этот экран позволяет просмотреть общее состояние устройства P-791R v2, сведения о системе и интерфейсах. На нем также доступны сводные таблицы статистики.
Сеть		
WAN	Internet Connection	Этот экран служит для настройки параметров поставщика услуг Интернета, присвоения IP-адресов в сети WAN, задания параметров DSL-линий, а также настройки прямых соединений по схеме "точка – точка".
	More Connections	Этот экран служит для настройки и вызова удаленного межсетевых шлюза.
	WAN Backup Setup	Этот экран предназначен для настройки параметров переадресации трафика и резервирования WAN.

Таблица 2 Сводка экранов веб-конфигуратора (продолжение)

ССЫЛКА/ ЗНАЧОК	ПОДРАЗДЕЛ	НАЗНАЧЕНИЕ
LAN	IP	Этот экран служит для настройки параметров TCP/IP локальной сети и других дополнительных параметров.
	DHCP Setup	Этот экран служит для настройки параметров DHCP для локальной сети.
	Client List	Этот экран служит для просмотра текущих параметров DHCP-клиентов и привязки постоянных IP-адресов к определенным MAC-адресам (и именам хостов).
	IP Alias	Этот экран служит для разделения интерфейса LAN на подсети.
NAT	General	Этот экран служит для активации NAT.
	Port Forwarding	Этот экран служит для настройки серверов, находящихся во внутренней сети за P-791R v2.
Security		
Фильтр	General	Этот экран используется для настройки фильтров Интернет-безопасности и применения предварительно установленных правил фильтрации.
Advanced		
Static Route	Static Route	Этот экран служит для настройки статических IP-маршрутов.
Dynamic DNS	Dynamic DNS	Этот экран служит для настройки DNS для динамических адресов.
Remote MGMT	WWW	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается управлять устройством P-791R v2 по протоколам HTTPS и HTTP.
	Telnet	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается управлять устройством P-791R v2 по протоколу Telnet.
	FTP	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается управлять устройством P-791R v2 по протоколу FTP.
	SNMP	Этот экран служит для настройки параметров управления P-791R v2 по упрощенному протоколу управления сетью (SNMP).
	DNS	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается направлять DNS-запросы на P-791R v2.
	ICMP	Этот экран позволяет изменить настройки защиты от зондирования.
UPnP	General	Этот экран позволяет включить или отключить поддержку UPnP в P-791R v2.
Maintenance		
System	General	Этот экран содержит административную и относящуюся к системе информацию, а также позволяет изменить пароль.
	Time Setting	Это окно служит для настройки даты и времени в P-791R v2.

Таблица 2 Сводка экранов веб-конфигуратора (продолжение)

ССЫЛКА/ ЗНАЧОК	ПОДРАЗДЕЛ	НАЗНАЧЕНИЕ
Logs	View Log	Этот экран служит для просмотра журналов по выбранным категориям.
	Log Settings	Этот экран служит для настройки ведения журналов в P-791R v2.
Tools	Firmware	Этот экран служит для загрузки микропрограмм в P-791R v2.
	Configuration	Этот экран служит для резервного копирования и восстановления файлов настроек или восстановления заводской конфигурации P-791R v2.
	Restart	Этот экран служит для перезагрузки P-791R v2 без выключения питания.
Diagnostic	General	На этом экране отображаются данные, которые могут помочь вам при диагностике общих проблем, связанных с подключением P-791R v2.
	DSL Line	На этом экране отображаются данные, которые будут полезны для диагностики DSL-линии.

2.4 Экран состояния (Status)

Ниже дается краткое описание способов управления веб-конфигуратором из экрана **Status**.



Некоторые поля и ссылки недоступны, если на экране входа был введен пользовательский пароль (см. [рис. 4 на стр. 38](#)).

Рис. 8 Status



В следующей таблице описаны поля экрана **Status** screen.

Таблица 3 Экран Status

ПОЛЕ	ОПИСАНИЕ
Refresh Interval	В раскрывающемся списке выберите число секунд, чтобы автоматически обновлять статистику на экране с заданным интервалом, или None , чтобы отключить автоматическое обновление.
Apply	Выберите эту кнопку, чтобы обновить статистику на экране.
Device Information	
Host Name	Это имя системы, введенное в поле System Name на экране Maintenance > System > General . Оно необходимо в целях идентификации.
Model Number	В этом поле отображается наименование модели P-791R v2.
MAC Address	В этом поле отображается уникальный MAC или Ethernet-адрес P-791R v2.
ZyNOS Firmware Version	Это – версия и дата создания микропрограммы ZyNOS. ZyNOS является патентованной разработкой сетевой операционной системы ZyXEL.
DSL Firmware Version	В этом поле отображается версия и дата создания используемой микропрограммы P-791R v2. Эта информация может потребоваться техническим специалистам для диагностики неисправностей.
WAN Information	
DSL Mode	В этом поле отображается стандарт DSL, используемый устройством P-791R v2.
IP Address	В этом поле указан IP-адрес порта WAN.
IP Subnet Mask	В этом поле отображается маска подсети порта WAN.
Default Gateway (Основной шлюз)	В этом поле отображается IP-адрес шлюза по умолчанию, если он применим.
VPI/VCI	В этом поле отображаются идентификаторы виртуального пути и виртуального канала, введенные на экране WAN.
LAN Information	

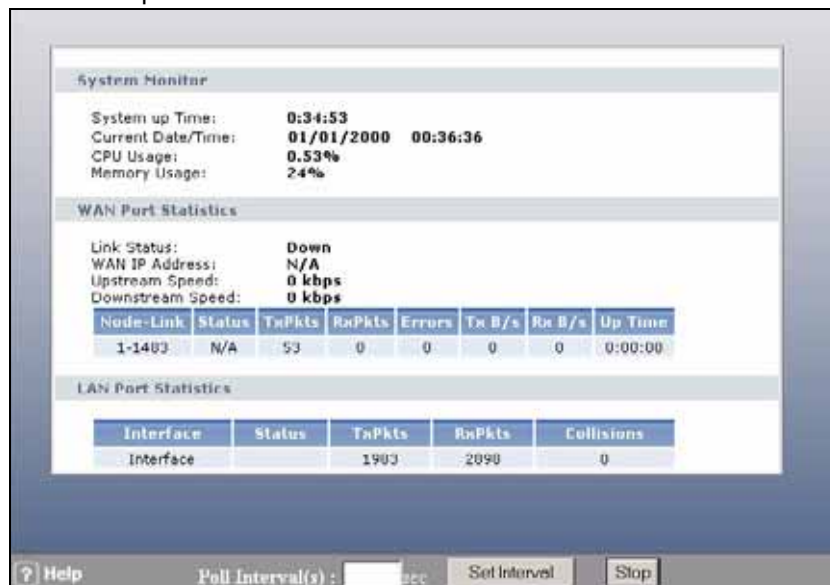
Таблица 3 Экран Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Address	В этом поле указан IP-адрес порта LAN.
IP Subnet Mask	В этом поле отображается маска подсети порта LAN.
DHCP	В этом поле отображается роль DHCP для порта WAN: Server (сервер), Relay (ретрансляция) или None (нет).
System Status	
System Uptime	В этом поле отображается суммарная продолжительность работы P-791R v2.
Current Date/Time	В этом поле отображаются текущие дата и время по часам P-791R v2.
System Mode	В этом поле отображается режим работы P-791R v2: маршрутизатор (router) или мост (bridge).
CPU Usage	Это число характеризует объем хипа, используемый P-791R v2 (в килобайтах). Хип – это оперативная память, которая не используется для системных нужд ZyNOS (сетевой операционной системы ZyXEL) и доступна таким активным процессам, как NAT. В этом поле отображается объем хипа, используемый P-791R v2 (в процентах). Когда объем приближается к максимуму, индикатор меняет цвет с зеленого на красный.
Memory Usage	В этом поле отображается суммарный объем хипа в P-791R v2 (в килобайтах). В этом поле отображается объем хипа, используемый P-791R v2 (в процентах). Когда объем приближается к максимуму, индикатор меняет цвет с зеленого на красный.
Interface Status	
Interface	В этом разделе отображаются интерфейсы P-791R v2.
Status	В этом поле отображается состояние: Down (канал разъединен), Up (канал соединен), если используется инкапсуляция Ethernet, и Down (канал разъединен), Up (канал соединен), Idle (соединение (ppp-сеанс) неактивно), Dial (начало вызова) и Drop (прерывание вызова), если используется инкапсуляция PPPoE.
Rate	Для порта LAN в этом поле отображается скорость порта и используемый режим дуплекса. Порты Ethernet могут быть подключены в полудуплексном (half) или полнодуплексном (full) режиме. Полнодуплексный режим позволяет устройству одновременно передавать и получать информацию, а в полудуплексном режиме информация в каждый момент времени может идти только в одном направлении. Параметры скорости и режима дуплекса для Ethernet-порта должны совпадать с параметрами, используемыми Ethernet-портом на другой стороне соединения. Возможность одновременной передачи по одному порту в обоих направлениях (полный дуплекс) фактически удваивает полосу пропускания. Для порта DSL сообщается скорость передачи по нисходящему и восходящему каналу.
Summary	При входе в веб-конфигуратор с паролем пользователя этот раздел недоступен.
Packet Statistics	Этот экран позволяет просмотреть состояние портов и статистику по пакетам.

2.4.1 Раздел Status: Packet Statistics

На экране **Status** пройдите по ссылке **Packet Statistics**. Информация, доступная только для чтения, касается состояния порта и пакетов. Также в ней содержится "продолжительность работы системы" и "интервал(ы) опроса". Поле **Poll Interval(s)** можно настраивать.

Рис. 9 Экран Status > Packet Statistics



Поля изображённого выше экрана описаны в следующей таблице.

Таблица 4 Экран Status > Packet Statistics

ПОЛЕ	ОПИСАНИЕ
System Monitor	
System up Time	В этом поле отображается суммарная продолжительность работы системы.
Current Date/Time	В этом поле отображаются текущие дата и время по часам P-791R v2.
CPU Usage	В этом поле отображается загрузка ЦП (в процентах).
Memory Usage	В этом поле отображается объем используемой оперативной памяти (в процентах).
WAN Port Statistics	
Link Status	В этом поле отображается состояние соединения с WAN.
WAN IP Address	В этом поле отображается IP-адрес в сети WAN, присвоенный устройству P-791R v2.
Upstream Speed	В этом поле отображается скорость восходящего канала P-791R v2.
Downstream Speed	В этом поле отображается скорость нисходящего канала P-791R v2.
Node-Link	В этом поле отображается порядковый номер и тип соединения с удаленным узлом. Возможны следующие типы соединений: PPPoA, ENET, RFC 1483 и PPPoE.

Таблица 4 Экран Status > Packet Statistics (продолжение)

ПОЛЕ	ОПИСАНИЕ
Status	В этом поле отображается состояние: Down (канал разъединен), Up (канал соединен), если используется инкапсуляция Ethernet, и Down (канал разъединен), Up (канал соединен), Idle (соединение (ppp-сеанс) неактивно), Dial (начало вызова) и Drop (прерывание вызова), если используется инкапсуляция PPPoE. Отсутствие соединения на порту обозначается N/A .
TxPkts	В этом поле отображается количество пакетов, отправленных через данный порт.
RxPkts	В этом поле отображается количество пакетов, принятых через данный порт.
Errors	В этом поле отображается количество пакетов с ошибками на данном порту.
Tx B/s	В этом поле отображается число байт, отправленных за последнюю секунду.
Rx B/s	В этом поле отображается число байт, принятых за последнюю секунду.
Up Time	В этом поле отображается суммарная продолжительность пребывания данного порта в активном состоянии.
LAN Port Statistics	
Interface	В этом поле отображается тип порта.
Status	В этом поле отображается состояние: Down (канал разъединен), Up (канал соединен), если используется инкапсуляция Ethernet, и Down (канал разъединен), Up (канал соединен), Idle (соединение (ppp-сеанс) неактивно), Dial (начало вызова) и Drop (прерывание вызова), если используется инкапсуляция PPPoE.
TxPkts	В этом поле отображается количество пакетов, отправленных через данный порт.
RxPkts	В этом поле отображается количество пакетов, принятых через данный порт.
Collisions	Это – количество коллизий на данный порт.
Help	Щелкните на значке Help, чтобы открыть встроенную справку.
Poll Interval(s)	Введите интервал времени для обновления системной статистики в браузере.
Set Interval	Нажмите эту кнопку, чтобы применить новый интервал опроса, введенный выше в поле Poll Interval .
Stop	Нажмите эту кнопку, чтобы приостановить обновление системной статистики.

2.5 Сброс P-791R v2

Если вы забыли пароль или не можете получить доступ к веб-конфигуратору, воспользуйтесь кнопкой **RESET** на задней панели P-791R v2 для восстановления заводских настроек. При этом будут потеряны все настройки, выполненные ранее, и значением пароля снова будет "1234".

2.5.1 Использование кнопки сброса

- 1 Убедитесь, что светодиод **POWER** горит (не мигает).
- 2 Нажмите кнопку **RESET** и удерживайте ее в течение приблизительно десяти секунд или до тех пор, пока светодиод **PWR** не начнет мигать, после чего отпустите кнопку. Когда светодиод **POWER** начинает мигать, это значит, что значения по умолчанию восстановлены, и устройство P-791R v2 перезагружается.

Мастер настройки доступа к Интернету

В данной главе содержится информация об экранах Wizard Setup (Мастера установки) в веб-конфигураторе.

3.1 Введение

Экраны мастеров настройки позволяют настроить вашу систему для доступа в Интернет, указав сведения, полученные от поставщика услуг Интернета.



Дополнительную информацию об этих полях см. в главах о меню расширенной настройки.

3.2 Мастер настройки доступа к Интернету


- 1 После указания пароля администратора для входа в веб-конфигуратор выберите **Go to Wizard setup** и нажмите **Apply**. Либо нажмите значок мастера () в верхнем правом углу веб-конфигуратора , чтобы перейти к основному экрану мастера.

Рис. 10 Выбор режима



2 Щелкните **INTERNET SETUP**, чтобы настроить доступ системы к Интернету.

Рис. 11 Мастер: экран приветствия



3 На экране мастера введите данные о доступе к Интернету, предоставленные вам вашим поставщиком услуг Интернета. Если они не были предоставлены, оставьте их установленными по умолчанию.

Рис. 12 Мастер настройки доступа к Интернету: параметры поставщика услуг Интернета

STEP 1 + STEP 2

Internet Configuration

ISP Parameters for Internet Access

Please verify the following settings with your Internet Service Provider (ISP). Your ISP may have given you a welcome letter or network setup letter including this information.

Mode
 Select 'Routing' (default) if your ISP allows multiple computers to share an Internet account. Otherwise, select 'Bridge' mode.

Encapsulation
 Select the encapsulation method used by your ISP. Your ISP may list 'ENET ENCAP' as 'Static IP' or 'Dynamic IP'.

Multiplexing
 Select the multiplexing type used by your ISP.

Virtual Circuit ID

VPI
VCI
 Select the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) used by your ISP. The valid range for the VPI is 0 to 255 and VCI is 32 to 65535.

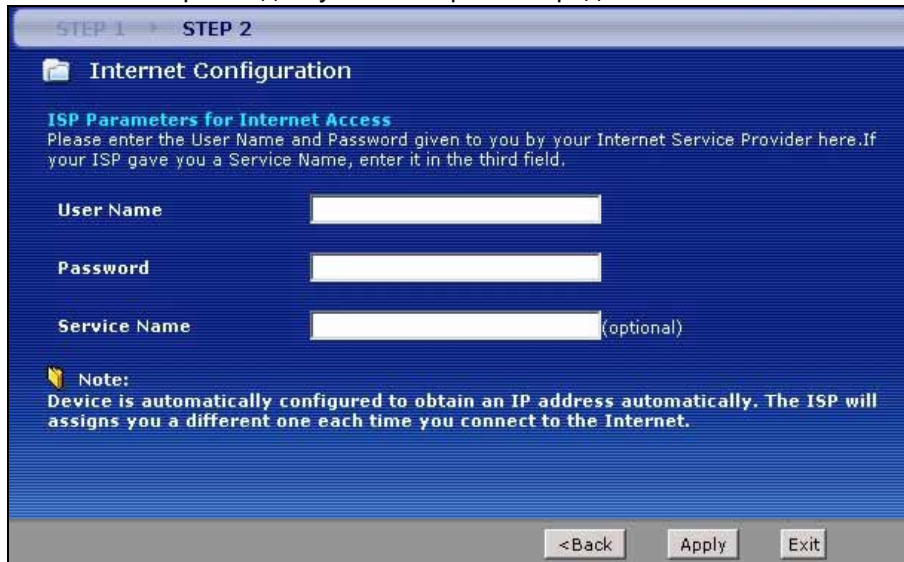
Поля изображённого выше экрана описаны в следующей таблице.

Таблица 5 Мастер настройки доступа к Интернету: параметры поставщика услуг Интернета

ПОЛЕ	ОПИСАНИЕ
Mode	Если ваш поставщик услуг Интернета позволяет использовать одну учетную запись с нескольких компьютеров, в поле Mode выберите Routing (этот режим действует по умолчанию). В противном случае выберите режим моста - Bridge .
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка Encapsulation . Доступные варианты зависят от режима, выбранного в поле Mode . Если в поле Mode выбран режим Bridge , выберите PPPoA или RFC 1483 . Если в поле Mode выбран режим Routing , выберите PPPoA , RFC 1483 , ENET ENCAP или PPPoE .
Мультиплек- сирование	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка Multiplex : VC-based (мультиплексирование на основе виртуальных каналов) или LLC-based (мультиплексирование на основе управления логическим каналом связи).
Virtual Circuit ID	Совокупность VPI (идентификатора виртуального пути) и VCI (идентификатора виртуального канала) определяет виртуальную цепь. Подробное описание см. в приложении.
VPI	Введите присвоенный вам VPI. Это поле могло быть настроено заранее.
VCI	Введите присвоенный вам VCI. Это поле могло быть настроено заранее.
Back	Для возврата к предыдущему экрану нажмите кнопку Back .
Next	Для перехода к следующему экрану мастера нажмите кнопку Next . Экран мастера, который появится следующим, зависит от протокола, выбранного выше.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите Exit .

- 4 Вид следующего экрана мастера зависит от выбранного режима и типа инкапсуляции. Все экраны приведены для режима маршрутизации. Заполните поля и нажмите кнопку **Next** для продолжения.

Рис. 13 Настройка доступа в Интернет посредством PPPoE

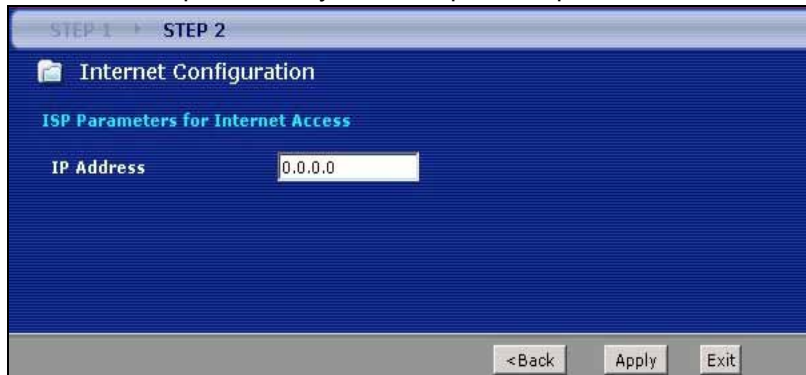


Поля изображённого выше экрана описаны в следующей таблице.

Таблица 6 Настройка доступа в Интернет посредством PPPoE

ПОЛЕ	ОПИСАНИЕ
User Name	Введите имя пользователя в точности так, как оно указано поставщиком услуг. Если поставщик присвоил имя пользователя в формате пользователь@домен, где доменом является название службы, следует ввести оба компонента в точном соответствии с указаниями.
Password	Введите пароль, связанный с указанным выше именем пользователя.
Service Name	Введите название службы PPPoE.
Back	Для возврата к предыдущему экрану нажмите кнопку Back .
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите Exit .

Рис. 14 Настройка доступа в Интернет посредством RFC 1483

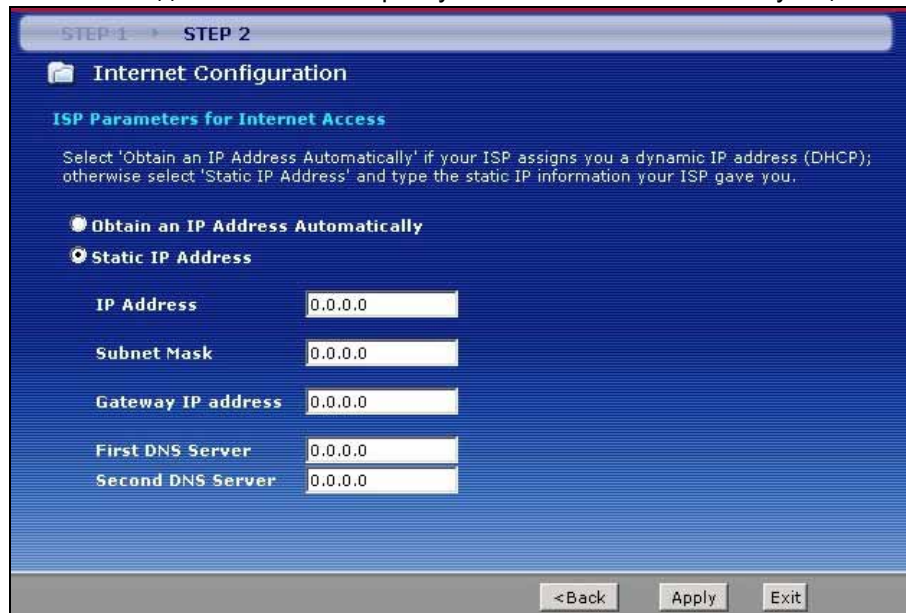


Поля изображённого выше экрана описаны в следующей таблице.

Таблица 7 Настройка доступа в Интернет посредством RFC 1483

ПОЛЕ	ОПИСАНИЕ
IP Address	Это поле доступно в том случае, если в поле Mode выбран режим Routing . Введите в этом поле IP-адрес, присвоенный поставщиком услуг Интернета.
Back	Для возврата к предыдущему экрану нажмите кнопку Back .
Next	Для перехода к следующему экрану мастера нажмите кнопку Next .
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите Exit .

Рис. 15 Подключение к Интернету с использованием инкапсуляции ENET ENCAP



Поля изображённого выше экрана описаны в следующей таблице.

Таблица 8 Подключение к Интернету с использованием инкапсуляции ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
Obtain an IP Address Automatically	Статический IP-адрес – это фиксированный адрес, выдаваемый поставщиком услуг Интернета. Динамический IP-адрес не имеет постоянного значения; поставщик услуг Интернета для каждого сеанса работы с Интернетом назначает новый адрес. Если вам назначается динамический IP-адрес, выберите Obtain an IP Address Automatically .
Static IP Address	Если поставщик услуг Интернета выделил вам фиксированный (статический) IP-адрес, выберите Static .
IP Address	Введите IP-адрес, выданный поставщиком услуг Интернета.
Маска подсети	Введите маску подсети в десятичном виде через точку. Способ расчета маски подсети при делении на подсети описан в приложении.
IP-адрес шлюза	Если на предыдущем экране в поле Encapsulation вы выбрали режим ENET ENCAP , то здесь необходимо указать IP-адрес шлюза (предоставляемый поставщиком услуг Интернета).
First DNS Server	Введите IP-адреса DNS-серверов. Адреса DNS-серверов передаются клиентским компьютерам вместе с присвоенными им IP-адресами и маской подсети.

Таблица 8 Подключение к Интернету с использованием инкапсуляции ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
Second DNS Server	См. выше.
Back	Для возврата к предыдущему экрану нажмите кнопку Back .
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите Exit .

Рис. 16 Настройка доступа в Интернет посредством PPPoA



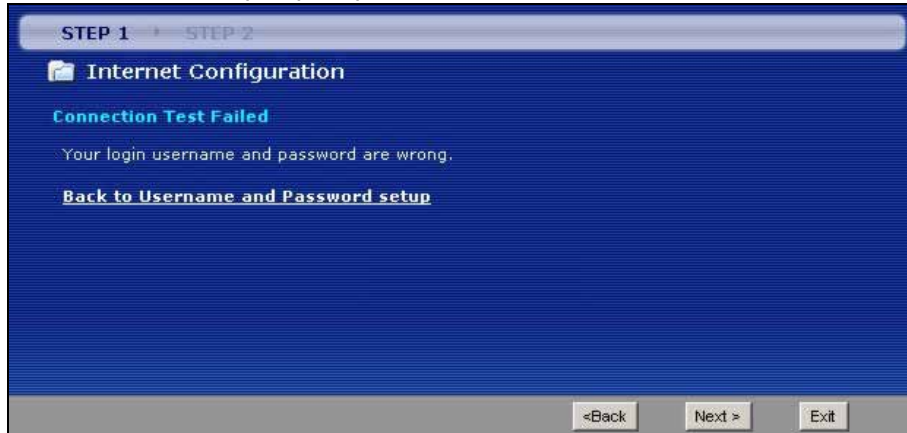
Поля изображённого выше экрана описаны в следующей таблице.

Таблица 9 Настройка доступа в Интернет посредством PPPoA

ПОЛЕ	ОПИСАНИЕ
User Name	Введите имя пользователя, предоставленное поставщиком услуг Интернета.
Password	Введите пароль, связанный с указанным выше именем пользователя.
Back	Для возврата к предыдущему экрану нажмите кнопку Back .
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите Exit .

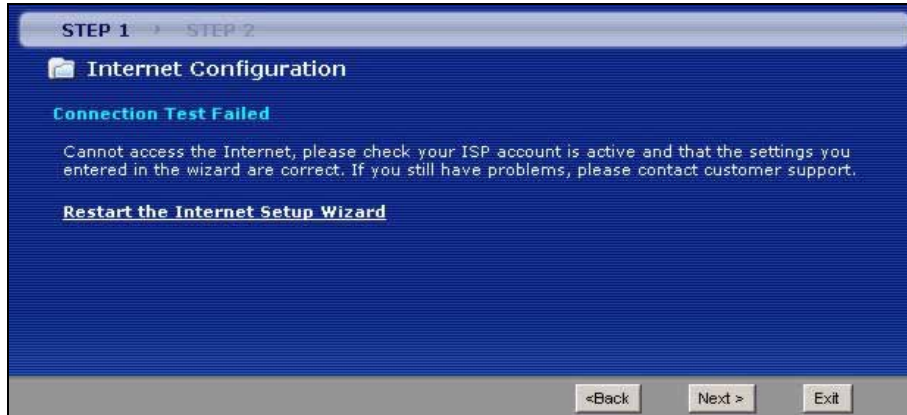
- Если для подключения по протоколам PPPoE или PPPoA было неверно введено имя пользователя или пароль, появится следующий экран. Чтобы возвратиться на предыдущий экран и изменить их, выберите **Back to Username and Password setup**.

Рис. 17 Ошибка при проверке подключения – 1



- Если появился показанный ниже экран, проверьте, активирована ли ваша учетная запись, или вернитесь на экран для проверки настроек доступа в Интернет, выбрав **Restart the Internet Setup Wizard**.

Рис. 18 Ошибка при проверке подключения – 2



Если установка мастера настройки Интернет успешно завершена, то на приведенном ниже экране отображаются сведения о вашей конфигурации. Щелкните **Finish**, чтобы завершить работу мастера.

Рис. 19 Мастер настройки доступа в Интернет



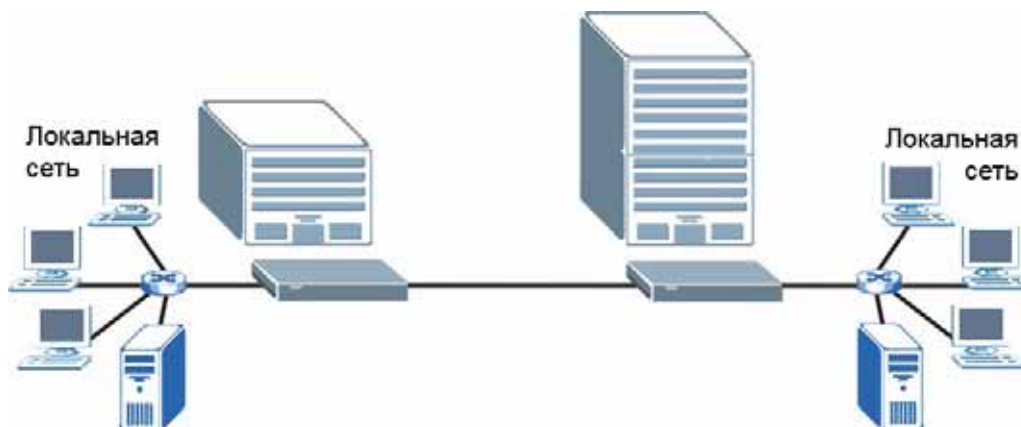
Прямые соединения

В этой главе описаны прямые соединения.

4.1 Общие сведения

Между двумя устройствами P-791R v2 можно установить соединение по схеме “точка-точка”. Это недорогой вариант высокоскоростного канала для таких требовательных к полосе пропускания задач, как видеоконференции и дистанционное обучение. Ниже показан пример такого соединения.

Рис. 20 Пример: обзор соединений по схеме "точка-точка"



В соединении по схеме “точка-точка” DSL-порты обоих устройств P-791R v2 напрямую соединены друг с другом и не используются для подключения к поставщику услуг Интернета.



Для соединения по схеме “точка-точка” можно использовать RFC 1483 в режиме моста или ENET ENCAP в режиме маршрутизатора.



В соединении “точка-точка” оба P-791R v2 должны использовать одинаковые VPI, VCI, режим мультиплексирования и метод инкапсуляции.

При установлении соединения по схеме “точка-точка” одно из устройств P-791R v2 становится сервером (заменяя поставщика услуг Интернета). Сервер управляет некоторыми параметрами DSL-соединения, включая скорости передачи и режим работы DSL. В остальном различия между сервером и клиентом отсутствуют. Любая из сторон может инициировать соединение по схеме “точка-точка”.

Соединения по схеме “точка-точка” могут устанавливаться только между устройствами P-791R v2, поддерживающими такой клиент-серверный режим.

4.2 Настройка соединения по схеме “точка-точка”

Ниже приведены указания для установления соединения по схеме “точка-точка”.

- 1 [Настройка сервера.](#)
- 2 [Настройка клиента.](#)
- 3 [Соединение двух устройств P-791R v2.](#)

4.2.1 Настройка сервера

- 1 Войдите в управление устройством P-791R v2, которое будет выступать в качестве сервера. (См. [гл. 2 на стр. 37.](#))
- 2 Выберите **Network > WAN > Internet Connection**.
- 3 В полях **VPI**, **VCI**, **Multiplexing** и **Encapsulation** укажите параметры, которые будут использоваться для прямого соединения. В поле **Encapsulation** выберите режим инкапсуляции: **RFC 1483** или **ENET ENCAP**.
- 4 Пролистайте экран до раздела **Service Type**. Появится изображённый ниже экран.

Рис. 21 Экран WAN > Internet Connection > Service Type

Service Type	
Service Mode	2-wire
Service Type	Client
Enable Rate Adaption	Enable
Transfer Max Rate(Kbps)	5896
Transfer Min Rate(Kbps)	192
Standard Mode	ANSI(ANNEX_A)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>	

- 5 В поле **Service Type** выберите **Server**. Станут доступны остальные поля экрана.
- 6 Заполните необходимые оставшиеся поля. В частности, можно ограничить максимальную скорость передачи в поле **Transfer Max Rate**.
- 7 Выберите **Apply**.

4.2.2 Настройка клиента

- 1 Войдите в управление устройством P-791R v2, которое будет выступать в качестве клиента. (См. [гл. 2 на стр. 37.](#))
- 2 Выберите **Network > WAN > Internet Connection**.
- 3 В полях **VPI**, **VCI**, **Multiplexing** и **Encapsulation** продублируйте значения, заданные на сервере.
- 4 Пролистайте экран до раздела **Service Type**. См. выше [рис. 21 на стр. 58.](#)
- 5 В поле **Service Mode** выберите тот же тип соединения, который был выбран для сервера.
- 6 В поле **Service Type** выберите **Client**. Значения остальных полей будут согласованы с сервером.
- 7 Выберите **Apply**.

4.2.3 Соединение двух устройств P-791R v2

Соедините между собой порты **DSL** на обоих устройствах P-791R v2 и дождитесь установления связи между двумя P-791R v2. Когда соединение установлено, горят светодиоды **DSL** и **INTERNET**. Установление соединения может занять полминуты. Если соединение между двумя P-791R v2 не удастся установить, необходимо проверить соответствие всех настроек (кроме **Service Type**).

ЧАСТЬ II

Настройка сети

[Настройка WAN \(63\)](#)

[Настройка LAN \(87\)](#)

[Экраны настройки NAT \(99\)](#)

Настройка WAN

В этой главе описывается настройка параметров глобальной сети.

5.1 Обзор параметров WAN

Понятие WAN (глобальная вычислительная сеть) относится к соединению с некоторой внешней сетью или Интернетом.

5.1.1 Encapsulation

Необходимо использовать тот метод инкапсуляции, которого требует поставщик услуг Интернета. P-791R v2 поддерживает следующие методы.

5.1.1.1 ENET ENCAP

Протокол звеньев маршрутизации с инкапсуляцией MAC-адресов (ENET ENCAP) реализуется только на основе сетевого протокола IP. Пакеты IP пересылаются по маршруту между интерфейсом Ethernet и интерфейсом WAN и затем переформатируются для адаптации к мостовому соединению. В частности кадры Ethernet инкапсулируются в ячейки ATM для передачи через сетевой мост. Для использования ENET ENCAP необходимо указать IP-адрес шлюза в поле **ENET ENCAP Gateway** на втором экране мастера. Эту информацию можно получить у поставщика услуг Интернета.

5.1.1.2 PPP по Ethernet (PPPoE)

PPPoE обеспечивает механизмы контроля доступа и тарификации методами, подобными применяемым при коммутируемом соединении с использованием PPP. PPPoE – это стандарт IETF (RFC 2516), определяющий способ взаимодействия персонального компьютера (ПК) с модемом (DSL, кабельным, беспроводным и т.д.), обеспечивающим широкополосное соединение.

Поставщику услуг PPPoE предоставляет способ доступа и аутентификации, совместимый с существующими системами контроля доступа (например, Radius).

Одним из преимуществ PPPoE является способность давать пользователям возможность доступа к одной из нескольких сетевых услуг – функция, известная под названием "динамический выбор службы". Она позволяет поставщику услуг легко создавать и предлагать новые IP-сервисы для отдельных пользователей.

Протокол PPPoE позволяет снизить затраты труда как абонента, так и поставщика услуг или оператора, поскольку для него не требуется производить специальную настройку широкополосного модема на стороне клиента.

Реализация PPPoE непосредственно в P-791R v2 (а не на отдельных компьютерах) снимает необходимость в установке ПО для PPPoE на компьютерах локальной сети, поскольку эту часть задачи выполняет P-791R v2. Кроме того, благодаря NAT доступ будут иметь все компьютеры в LAN.

5.1.1.3 PPP по ATM (PPPoA)

PPPoA означает протокол "точка-точка" поверх 5-го уровня адаптации ATM (AAL5). PPPoA функционирует так же, как модемное коммутируемое соединение с Интернетом. P-791R v2 инкапсулирует PPP-сеанс по стандарту RFC1483 и передает его через постоянный виртуальный канал (ATM PVC) на оборудовании DSLAM (мультиплексор цифровых абонентских каналов) у поставщика услуг. Подробное описание PPPoA см. в RFC 2364. Подробное описание PPP см. в RFC 1661.

5.1.1.4 RFC 1483

В RFC 1483 описаны два метода многопротокольной инкапсуляции поверх 5-го уровня адаптации ATM (AAL5). Первый метод позволяет мультиплексировать несколько протоколов по одному виртуальному каналу ATM (мультиплексирование на основе управления логическим каналом связи – LLC), а второй метод предполагает, что каждый протокол передается по отдельному виртуальному каналу ATM (мультиплексирование на основе виртуальных цепей/каналов – VC). Подробную информацию см. в соответствующем документе RFC.

5.1.2 Мультиплексирование

Существует два способа идентификации протоколов, реализуемых через виртуальный канал (VC). Необходимо использовать тот метод мультиплексирования, которого требует поставщик услуг Интернета.

5.1.2.1 Мультиплексирование VC

В этом случае по предварительному двустороннему соглашению каждый протокол назначается на определенный виртуальный канал, например, VC1 несет IP и т.д. Мультиплексирование на основе VC чаще используется в средах, где динамическое создание большого числа виртуальных каналов ATM является быстрым и экономичным.

5.1.2.2 Мультиплексирование LLC

В этом случае один VC несет несколько протоколов, а в заголовке каждого пакета содержится информация, позволяющая идентифицировать протокол. Несмотря на дополнительные требования к пропускной способности и обработке, этот метод может оказаться предпочтительным в случае, когда невыгодно иметь отдельный виртуальный канал для каждого протокола, например, если стоимость сильно зависит от количества одновременных виртуальных каналов.

5.1.3 VPI и VCI

Убедитесь, что вы правильно задали идентификатор виртуального пути (VPI) и идентификатор виртуального канала (VCI), назначенные поставщиком услуг. Допустимый диапазон для идентификатора виртуального пути – от 0 до 255, для идентификатора виртуального канала – от 32 до 65535 (диапазон от 0 до 31 зарезервирован для локального управления трафиком ATM). Подробности см. в приложении.

5.1.4 Присвоение IP-адресов

Статический IP-адрес – это фиксированный адрес, выдаваемый поставщиком услуг Интернета. Динамический IP-адрес не имеет постоянного значения; поставщик услуг Интернета каждый раз назначает новый адрес. При наличии одного динамического или статического IP-адреса можно включать и отключать функцию SUA (Single User Account – учетная запись одного пользователя). Однако процедура выбора IP-адреса и шлюза ENET ENCAP зависит от используемого метода инкапсуляции.

5.1.4.1 Назначение IP-адресов при использовании инкапсуляции PPPoA или PPPoE

Если вам выдается динамический IP-адрес, то поля **IP Address** и **ENET ENCAP Gateway** неприменимы (N/A). Если вам выдан статический IP-адрес, необходимо *только* заполнить поле **IP Address** и *не* заполнять поле **ENET ENCAP Gateway**.

5.1.4.2 Назначение IP-адресов при использовании инкапсуляции RFC 1483

В этом случае *должен* присваиваться только статический IP-адрес; изложенные выше требования в отношении полей **IP Address** и **ENET ENCAP Gateway** остаются в силе.

5.1.4.3 Назначение IP-адресов при использовании инкапсуляции ENET ENCAP

В этом случае вы можете иметь или статический или динамический IP-адрес. Для статического IP-адреса необходимо заполнить поля **IP Address** и **ENET ENCAP Gateway** сведениями, полученными от поставщика услуг Интернета. Однако в случае динамического IP-адреса устройство P-791R v2 будет выступать DHCP-клиентом в сети WAN, и поля **IP Address** и **ENET ENCAP Gateway** будут неприменимы, поскольку P-791R v2 получает соответствующие значения от DHCP-сервера.

5.1.5 Закрепленное соединение (в режиме PPP)

Закрепленное соединение – это коммутируемая линия, где соединение всегда установлено независимо от требований к трафику. Реализация закрепленного соединения в P-791R v2 сводится к тому, что отключается время ожидания, а кроме того, при каждом разрыве сеанса P-791R v2 будет пытаться автоматически восстановить соединение. Закрепленное соединение может оказаться чрезвычайно дорогостоящим по очевидным причинам.

Не указывайте закрепленное соединение, за исключением случаев, когда оператор связи предлагает услуги по фиксированной ставке или если необходимо постоянное соединение, а его стоимость не имеет значения.

5.1.6 NAT

NAT (Network Address Translation - трансляция сетевых адресов, RFC 1631) представляет собой механизм преобразования IP-адреса хоста в пакете, например адреса отправителя в исходящем пакете, при котором адреса, используемые в одной сети, заменяются адресами, известными в другой сети.

5.2 Метрика

Метрика обозначает “стоимость” передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой “стоимостью”. Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключённым сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже “стоимость”.

Метрика устанавливает приоритеты маршрутов, используемых P-791R v2 для связи с Интернетом. Если два маршрута по умолчанию имеют одно и то же значение метрики, P-791R v2 использует следующие предопределенные приоритеты:

- Обычный маршрут: определяется поставщиком услуг Интернета (см. [разд. 5.4 на стр. 68](#))
- Маршрут для переадресации трафика (см. [разд. 5.6 на стр. 78](#))
- Резервный маршрут WAN, также называемый маршрутом резервирования через коммутируемый доступ (см. [разд. 5.9 на стр. 80](#))

Например, если обычный маршрут имеет метрику 1, маршрут переадресации трафика – метрику 2, а маршрут резервирования через коммутируемый доступ – метрику 3, то в качестве основного маршрута по умолчанию действует обычный маршрут. Если через обычный маршрут соединение с Интернетом отсутствует, то затем P-791R v2 пробует маршрут переадресации трафика. Если маршрут переадресации также оказывается неработоспособен, P-791R v2 использует маршрут резервирования через коммутируемый доступ.

Если необходимо, чтобы маршрут резервирования через коммутируемый доступ был приоритетен по сравнению с маршрутом переадресации трафика или даже обычным маршрутом, то достаточно установить для маршрута резервирования через коммутируемый доступ метрику 1, а для других маршрутов – 2 (или больше).

Маршрутизация по политикам IP отменяет стандартные правила маршрутизации и имеет приоритет над всеми упомянутыми выше маршрутами.

5.3 Ограничение трафика

Ограничение трафика - это соглашение между оператором и абонентом, регламентирующее средние скорости и флуктуации при передаче данных по ATM-сети. Такие соглашения позволяют избежать перегрузки сети, которая способна нарушить передачу данных в режиме реального времени – в частности, видео и аудио.

Пиковая скорость ячеек (Peak Cell Rate, PCR) устанавливает максимальную скорость, с которой ячейки могут поступать от отправителя. Этот параметр может быть ниже (но не выше), чем максимальная скорость линии. Одна ATM-ячейка имеет длину 53 байта (424 бита), поэтому максимальная скорость 832 Кбит/с соответствует максимальной PCR 1962 ячейки в секунду. Эта скорость не гарантирована, поскольку она зависит от скорости линии.

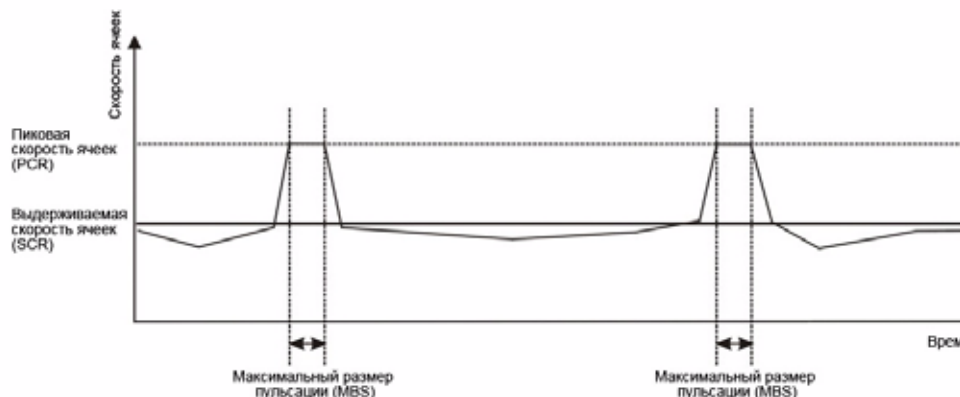
Выдерживаемая скорость ячеек (Sustained Cell Rate, SCR) - средняя скорость ячеек для каждого источника пульсирующего трафика. Она задаёт максимальную среднюю скорость, с которой ячейки могут пересылаться по виртуальному соединению. SCR не должна превышать PCR.

Максимальный размер пульсации (Maximum Burst Size, MBS) - это максимальное число ячеек, при посылке которого будет соблюдаться PCR. При превышении MBS скорость передачи ячеек будет опущена ниже SCR, пока усреднённая скорость вновь не уравнивается с SCR. Очередная порция ячеек (числом не более MBS) после этого может быть снова передана на скорости PCR.

Если скорость PCR, SCR или MBS по умолчанию имеет значение 0, система назначит максимальное значение, соответствующее скорости линии в направлении от абонента к ADSL-модулю.

Взаимосвязь PCR, SCR and MBS продемонстрирована на следующем рисунке.

Рис. 22 Пример ограничения трафика



5.3.1 Классы трафика в ATM

Основные классы трафика определены в спецификации форума ATM Forum Traffic Management 4.0.

5.3.1.1 Постоянная скорость (CBR)

Постоянная битовая скорость (CBR) обеспечивает фиксированную полосу пропускания, которая доступна всегда, даже в отсутствие передаваемых данных.

CBR-трафик обычно чувствителен к временным параметрам (не допускает задержек).

CBR применяется для соединений, непрерывно требующих определённой полосы пропускания. Устанавливается пиковая скорость передачи ячеек (PCR), при превышении которой ячейки могут отбрасываться. Примерами соединений, требующих CBR, являются видео высокой чёткости и голосовая связь.

5.3.1.2 Переменная скорость (VBR)

Класс ATM-трафика с переменной битовой скоростью (Variable Bit Rate, VBR) применяется для соединений с резкими кратковременными пульсациями трафика. Соединения с трафиком класса VBR можно разделить на соединения в режиме реального времени (VBR-RT) и соединения без режима реального времени (VBR-nRT).

Тип VBR-RT (переменная скорость в режиме реального времени) используется в случаях, когда задержку и ее вариацию необходимо сильно ограничивать. В этом режиме также обеспечивается фиксированная полоса пропускания (нормируется PCR), но она доступна только во время передачи данных. Примером соединений, использующих режим VBR-RT, являются видеоконференции. Для видеоконференций необходима передача данных в режиме реального времени, а требования к полосе пропускания изменяются с учётом динамики видеопотока.

К типу nrt-VBR (переменная битовая скорость без требований реального времени) относятся соединения, в которых задержки и колебания задержек контролируются нестрого. Он обычно используется для пульсирующего трафика, типичного в локальных сетях. PCR и MBS определяют уровни пульсаций, а SCR определяет минимальный уровень. Примером таких соединений может быть передача файлов данных, нечувствительная к временным параметрам.

5.3.1.3 Неуказанная битовая скорость (UBR)

Класс ATM-трафика с неопределённой битовой скоростью (Unspecified Bit Rate, UBR) применяется для пульсирующего трафика. Отличие UBR состоит в том, что он не даёт никаких гарантий в отношении полосы пропускания и разрешает доставку трафика только при наличии запаса пропускной способности сети. Пример применения – передача файлов в фоновом режиме.

5.4 Настройка подключения к Интернету

Чтобы изменить настройки удаленного узла для P-791R v2, выберите **Network > WAN > Internet Connection**. Данный экран может быть различным в зависимости от инкапсуляции.

Дополнительные сведения см. в [разд. 5.1 на стр. 63](#).

Рис. 23 Экран WAN > Internet Connection

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 10 Экран WAN > Internet Connection

ПОЛЕ	ОПИСАНИЕ
General	
Name	Введите имя поставщика услуг Интернета, например, "MyISP". Эти сведения используются только для описания.
Mode	Если ваш поставщик услуг Интернета позволяет использовать одну учетную запись с нескольких компьютеров, выберите режим маршрутизации – Routing (этот режим действует по умолчанию). В противном случае выберите режим моста - Bridge .
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка. Доступные для выбора варианты зависят от режима, выбранного в поле Mode . Если в поле Mode выбран режим Bridge , выберите PPPoA или RFC 1483 . Если в поле Mode выбран режим Routing , выберите PPPoA , RFC 1483 , ENET ENCAP или PPPoE . При установке соединения по схеме "точка – точка" или "точка – две точки" выберите один из двух вариантов: ENET ENCAP или RFC 1483 .

Таблица 10 Экран WAN > Internet Connection (продолжение)

ПОЛЕ	ОПИСАНИЕ
User Name	(Только для PPPoA и PPPoE) Введите имя пользователя в точности так, как оно указано поставщиком услуг. Если поставщик присвоил имя пользователя в формате пользователь@домен, где доменом является название службы, следует ввести оба компонента в точном соответствии с указаниями.
Password	(Только для PPPoA и PPPoE) Введите пароль, связанный с указанным выше именем пользователя.
Service Name	(Только для инкапсуляции PPPoE) Введите название службы PPPoE.
Multiplexing	Выберите тип мультиплексирования, используемый поставщиком услуг Интернета, из раскрывающегося списка. Варианты выбора: VC или LLC .
Virtual Circuit ID	Совокупность VPI (идентификатора виртуального пути) и VCI (идентификатора виртуального канала) определяет виртуальную цепь. Подробное описание см. в приложении.
VPI	Допустимый диапазон значений VPI – от 0 до 255. Введите присвоенный вам VPI.
VCI	Допустимый диапазон значений VCI – от 32 до 65535 (диапазон от 0 до 31 зарезервирован для локального управления трафиком ATM). Введите присвоенный вам VCI.
IP Address	Эти поля доступны в том случае, если в поле Mode выбран режим Routing . Статический IP-адрес – это фиксированный адрес, выдаваемый поставщиком услуг Интернета. Динамический IP-адрес не имеет постоянного значения; поставщик услуг Интернета для каждого сеанса работы с Интернетом назначает новый адрес.
Obtain an IP Address Automatically	(Только для PPPoE, PPPoA и ENET ENCAP) Выберите этот переключатель, если IP-адрес вам присваивается в динамическом режиме.
Static IP Address	(Только для PPPoE, PPPoA и ENET ENCAP) Выберите этот переключатель, если вам присвоен статический IP-адрес.
IP Address	Введите статический IP-адрес, предоставленный поставщиком услуг Интернета.
Subnet Mask	(Только для ENET ENCAP) Это поле доступно в том случае, если выбран статический IP-адрес (Static IP Address). Введите маску подсети, предоставленную поставщиком услуг Интернета.
Gateway IP Address	(Только для ENET ENCAP) Это поле доступно в том случае, если выбран статический IP-адрес (Static IP Address). Введите IP-адрес шлюза, предоставленный поставщиком услуг Интернета. Для доступа в Интернет адрес должен быть указан верно. Если введен адрес 0.0.0.0, соединение с Интернетом функционировать не будет.
Connection	Этот раздел доступен только в том случае, если в поле Encapsulation указаны значения PPPoE или PPPoA .
Nailed-Up Connection	Выберите Nailed-Up Connection , чтобы использовать закрепленное соединение, которое активно все время. P-791R v2 будет пытаться автоматически восстановить соединение при разрыве сеанса.
Connect on Demand	Если соединение не требуется поддерживать постоянно, выберите Connect on Demand и укажите интервал неактивности в поле Max Idle Timeout .
Max Idle Timeout	Если вы выбрали режим Connect on Demand , в поле Max Idle Timeout укажите интервал неактивности. Значение по умолчанию – 0, при котором сеанс соединения с Интернетом не завершается никогда.
Service Type	

Таблица 10 Экран WAN > Internet Connection (продолжение)

ПОЛЕ	ОПИСАНИЕ
Service Mode	В этом поле указывается, что P-791R v2 использует 2-проводной режим для подключения к линии DSL. В 2-проводном режиме максимальная скорость передачи данных не превышает 5,69 Мбит/с. Это поле настроить невозможно.
Service Type	Укажите, на какой из сторон DSL-соединения (сервер, клиент) находится P-791R v2. Выберите Server , если устройство P-791R v2 выполняет в соединении “точка – точка” роль сервера. (См. гл. 4 на стр. 57.) В противном случае выберите Client .
Enable Rate Adaption	Это поле активно, если в поле Service Type выбрано значение Server . Укажите, следует ли включить для P-791R v2 режим согласования скорости соединения с другим устройством.
Transfer Max Rate(Kbps)	Это поле активно, если в поле Service Type выбрано значение Server . Выберите максимальную скорость отправки и приема информации для P-791R v2. Фактическая скорость будет лежать в диапазоне между настроенной вами максимальной скоростью и этим значением.
Transfer Min Rate(Kbps)	Это поле активно, если в поле Service Type выбрано значение Server . Выберите минимальную скорость отправки и приема информации для P-791R v2. Фактическая скорость будет лежать в диапазоне между этим значением и настроенной вами максимальной скоростью.
Standard Mode	Это поле активно, если в поле Service Type выбрано значение Server . Выберите режим DSL-соединения для P-791R v2. Режим “Annex A” предназначен для соединений, использующих аналоговые телефонные сети общего пользования (ТфОП), а режим “Annex B” – для соединений по цифровым линиям ISDN.
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран Advanced WAN Setup для настройки дополнительных параметров глобальной сети.

5.4.1 Расширенная настройка соединения с Интернетом

Этот экран используется для редактирования расширенных параметров P-791R v2 при определении соединений с Интернетом. На экране **Internet Connection** нажмите кнопку **Advanced Setup**. Появится изображенный ниже экран.

Рис. 24 Экран WAN > Internet Connection > Advanced Setup

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 11 Экран WAN > Internet Connection > Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Поле RIP Direction управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: Both (вход-выход), In Only (только вход) или Out Only (только выход), None (нет). Если выбраны значения Both или Out Only , P-791R v2 будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения Both или In Only , устройство будет объединять получаемые параметры RIP; если выбрано значение None , устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.
RIP Version	Это поле доступно в том случае, если в поле RIP Direction выбран любой параметр, кроме None . Поле RIP Version управляет форматом и способом широковещательной рассылки RIP-пакетов с P-791R v2 (устройство принимает пакеты обоих форматов). RIP-1 поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации RIP-2B и RIP-2M передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в RIP-2B используется широковещательная рассылка по подсетям, а в RIP-2M – многоадресная рассылка. Многоадресная рассылка может уменьшить нагрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.
Multicast	IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки. P-791R v2 поддерживает IGMP версии 1 (IGMP-v1) и IGMP-v2 . Чтобы отключить этот протокол, выберите None .
ATM QoS	

Таблица 11 Экран WAN > Internet Connection > Advanced Setup (продолжение)

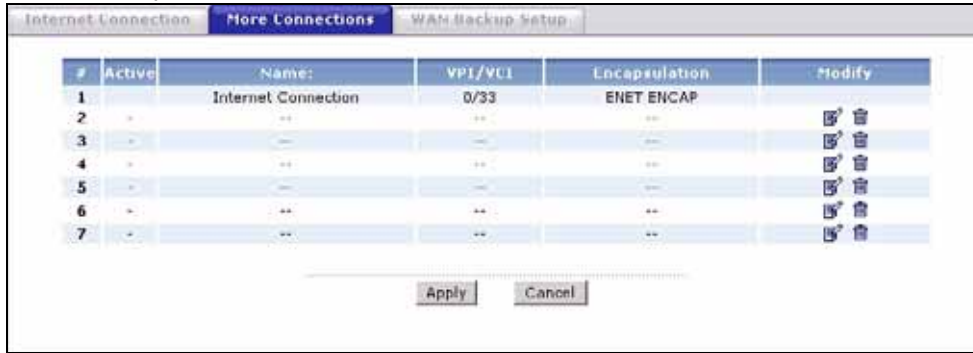
ПОЛЕ	ОПИСАНИЕ
ATM QoS Type	Выберите CBR (постоянная скорость передачи), если нужно задать фиксированную полосу пропускания для передачи голоса или данных. Выберите UBR (незаданная скорость передачи), если изменение скорости передачи со временем не имеет большого значения, например, в случае электронной почты. Выберите VBR-nRT (переменная битовая скорость - без режима реального времени) или VBR-RT (переменная битовая скорость - в режиме реального времени) для пульсирующего трафика и совместного использования полосы пропускания другими приложениями.
Peak Cell Rate	Разделите скорость DSL-линии (бит/с) на 424 (размер ATM-ячейки). Получится пиковая скорость передачи ячеек (PCR). Полученное значение будет соответствовать максимальной скорости отправки ячеек отправителем. Введите значение PCR в этом поле.
Sustain Cell Rate	Средняя скорость передачи ячеек (Sustained Cell Rate, SCR) – средняя скорость передачи ячеек (усреднение выполняется на большом промежутке времени). Введите SCR (значение SCR должно быть меньше PCR). Необходимо помнить, что по умолчанию система использует значение 0 ячеек в секунду.
Maximum Burst Size	Максимальный размер пульсации (Maximum Burst Size, MBS) – это максимальное число ячеек, при отправке которого будет соблюдаться PCR. Введите MBS (меньше 65535).
PPPoE Passthrough	Это поле действует только для соединений, использующих инкапсуляцию PPPoE. В дополнение к встроенному в устройство ZyXEL PPPoE-клиенту можно включить режим сквозного прохождения PPPoE, чтобы разрешить использование PPPoE-клиентов на хостах в локальной сети для соединения с поставщиком услуг Интернета через устройство ZyXEL. Каждый хост может иметь отдельную учетную запись и глобальный IP-адрес на стороне WAN. Сквозной режим PPPoE – альтернатива NAT для тех применений, где использование NAT невозможно. Отключите сквозной режим PPPoE, чтобы запретить хостам в локальной сети с помощью программных клиентов PPPoE соединяться с поставщиком услуг Интернета.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку Back .
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

5.5 Настройка дополнительных соединений

В этом разделе описаны параметры удаленной сети, не зависящие от протокола. Они требуются для связи с удаленным шлюзом и находящейся за ним сетью по соединению с WAN. При настройке доступа в Интернет на экране **WAN > Internet Connection** настраивается первое соединение с сетью WAN.

Чтобы перейти на показанный ниже экран, выберите **Network > WAN > More Connections**.

Рис. 25 Экран WAN > More Connections



Поля изображённого выше экрана описаны в следующей таблице.

Таблица 12 Экран WAN > More Connections

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер соединения.
Active	В этом поле отображается состояние активности соединения. Снимите флажок, чтобы запретить соединение. Чтобы снова разрешить соединение, отметьте флажок.
Name	В этом поле отображается описательное название данного соединения.
VPI/VCI	В этом поле отображаются значения VPI и VCI, используемые данным соединением.
Encapsulation	В этом поле отображается метод инкапсуляции, используемый данным соединением.
Modify	Первое соединение (с поставщиком услуг Интернета) на этом экране доступно только для чтения. Его можно отредактировать на экране WAN > Internet Connection . Чтобы перейти на экран для редактирования соединения, щелкните на значке редактирования. Для удаления существующего соединения щелкните на значке удаления. Удалить первое соединение нельзя.
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

5.5.1 Редактирование дополнительных соединений

Следующий экран служит для настройки соединения и вызывается щелчком на значке редактирования на экране **More Connections**.

Рис. 26 Экран WAN > More Connections > Edit

General	
<input checked="" type="checkbox"/> Active	
Name:	ChangeMe
Mode	Routing
Encapsulation	PPPoA
User Name	
Password	
Multiplexing	VC
VPI	0
VCI	33
IP Address	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Connection	
<input type="radio"/> Nailed-Up Connection	
<input checked="" type="radio"/> Connect on Demand	
Max Idle timeout	0 sec
NAT	
<input checked="" type="radio"/> None	
<input type="radio"/> SUA Only Edit	
<input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>	

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 13 Экран WAN > More Connections > Edit

ПОЛЕ	ОПИСАНИЕ
General	
Active	Чтобы активировать соединение, отметьте флажок; чтобы сделать соединение неактивным, снимите флажок.
Name	Введите уникальное описательное название (до 13 знаков ASCII), позволяющее идентифицировать данное соединение.
Mode	Если ваш поставщик услуг Интернета позволяет использовать одну учетную запись с нескольких компьютеров, выберите режим маршрутизации – Routing . Если выбран режим Bridge , то P-791R v2 будет пересылать на этот удаленный узел пакеты, не отправленные посредством маршрутизации, в противном случае такие пакеты удаляются.
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка. Возможны следующие варианты: PPPoA , RFC 1483 , ENET ENCAP или PPPoE . При настройке соединения по схеме “точка-точка” выберите режим ENET ENCAP или RFC 1483 .

Таблица 13 Экран WAN > More Connections > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
User Name	(Только для инкапсуляции PPPoA и PPPoE) Введите имя пользователя в точности так, как оно указано поставщиком услуг. Если поставщик присвоил имя пользователя в формате пользователь@домен, где доменом является название службы, следует ввести оба компонента в точном соответствии с указаниями.
Password	(Только для инкапсуляции PPPoA и PPPoE) Введите пароль, связанный с указанным выше именем пользователя.
Service Name	(Только для инкапсуляции PPPoE) Введите название службы PPPoE.
Multiplexing	Выберите тип мультиплексирования, используемый поставщиком услуг Интернета, из раскрывающегося списка. Варианты выбора: VC или LLC . По предварительному согласованию протоколы назначаются соответствующим виртуальным цепям, например, VC1 используется для передачи по протоколу IP. Если вы выбрали режим VC, укажите отдельные номера VPI и VCI для каждого протокола. При мультиплексировании на основе LLC или инкапсуляции PPP одна виртуальная цепь несет в себе несколько протоколов. Идентификационные параметры протокола содержатся в заголовках пакетов. В этом случае для всех протоколов достаточно одного набора номеров VPI и VCI.
VPI	Допустимый диапазон значений VPI – от 0 до 255. Введите присвоенный вам VPI.
VCI	Допустимый диапазон значений VCI – от 32 до 65535 (диапазон от 0 до 31 зарезервирован для локального управления трафиком ATM). Введите присвоенный вам VCI.
IP Address	Эти поля доступны в том случае, если в поле Mode выбран режим Routing . Статический IP-адрес – это фиксированный адрес, выдаваемый поставщиком услуг Интернета. Динамический IP-адрес не имеет постоянного значения; поставщик услуг Интернета для каждого сеанса работы с Интернетом назначает новый адрес.
IP Address	Введите статический IP-адрес, предоставленный поставщиком услуг Интернета.
Subnet Mask	Введите маску подсети, предоставленную поставщиком услуг Интернета.
Gateway IP Address	Введите IP-адрес шлюза, предоставленный поставщиком услуг Интернета.
Connection	Этот раздел доступен только в том случае, если в поле Encapsulation указаны значения PPPoE или PPPoA .
Nailed-Up Connection	Выберите Nailed-Up Connection , чтобы использовать закрепленное соединение, которое активно все время. P-791R v2 будет пытаться автоматически восстановить соединение при разрыве сеанса.
Connect on Demand	Если соединение не требуется поддерживать постоянно, выберите Connect on Demand и укажите интервал неактивности в поле Max Idle Timeout .
Max Idle Timeout	Если вы выбрали режим Connect on Demand , в поле Max Idle Timeout укажите интервал неактивности. Значение по умолчанию – 0, при котором сеанс соединения с Интернетом не завершается никогда.
NAT	Режим трансляции SUA Only доступен только в том случае, если в поле Mode выбран режим Routing . Выберите SUA Only , если NAT требуется использовать всего с одним глобальным IP-адресом. Для редактирования набора привязки серверов нажмите Edit , чтобы перейти на экран Port Forwarding . В противном случае выберите None , чтобы отключить NAT.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку Back .

Таблица 13 Экран WAN > More Connections > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран More Connections Advanced для редактирования дополнительных параметров соединения с WAN.

5.5.2 Расширенная настройка дополнительных соединений

Этот экран служит для настройки дополнительных параметров WAN в P-791R v2. На экране **More Connections Edit** нажмите кнопку **Advanced Setup**. Появится изображенный ниже экран.

Рис. 27 Экран WAN > More Connections > Advanced Setup

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 14 Экран WAN > More Connections > Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Поле RIP Direction управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: Both (вход-выход), In Only (только вход) или Out Only (только выход), None (нет). Если выбраны значения Both или Out Only , P-791R v2 будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения Both или In Only , устройство будет объединять получаемые параметры RIP; если выбрано значение None , устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.

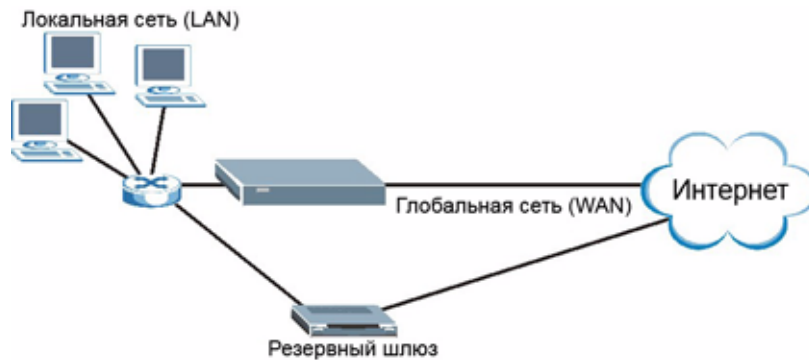
Таблица 14 Экран WAN > More Connections > Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
RIP Version	Это поле доступно в том случае, если в поле RIP Direction выбран любой параметр, кроме None . Поле RIP Version управляет форматом и способом широковещательной рассылки RIP-пакетов с P-791R v2 (устройство принимает пакеты обоих форматов). RIP-1 поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации RIP-2B и RIP-2M передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в RIP-2B используется широковещательная рассылка по подсетям, а в RIP-2M – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.
Multicast	IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки. P-791R v2 поддерживает IGMP версии 1 (IGMP-v1) и IGMP-v2 . Чтобы отключить этот протокол, выберите None .
ATM QoS	
ATM QoS Type	Выберите CBR (постоянная скорость передачи), если нужно задать фиксированную полосу пропускания для передачи голоса или данных. Выберите UBR (незаданная скорость передачи), если изменение скорости передачи со временем не имеет большого значения, например, в случае электронной почты. Выберите VBR-nRT (переменная битовая скорость - без режима реального времени) или VBR-RT (переменная битовая скорость - в режиме реального времени) для пульсирующего трафика и совместного использования полосы пропускания другими приложениями.
Peak Cell Rate	Разделите скорость DSL-линии (бит/с) на 424 (размер ATM-ячейки). Получится пиковая скорость передачи ячеек (PCR). Полученное значение будет соответствовать максимальной скорости посылки ячеек отправителем. Введите значение PCR в этом поле.
Sustain Cell Rate	Средняя скорость передачи ячеек (Sustained Cell Rate, SCR) – средняя скорость передачи ячеек (усреднение выполняется на большом промежутке времени). Введите SCR (значение SCR должно быть меньше PCR). Необходимо помнить, что по умолчанию система использует значение 0 ячеек в секунду.
Maximum Burst Size	Максимальный размер пульсации (Maximum Burst Size, MBS) – это максимальное число ячеек, при посылке которого будет соблюдаться PCR. Введите MBS (меньше 65535).
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку Back .
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

5.6 Переадресация трафика

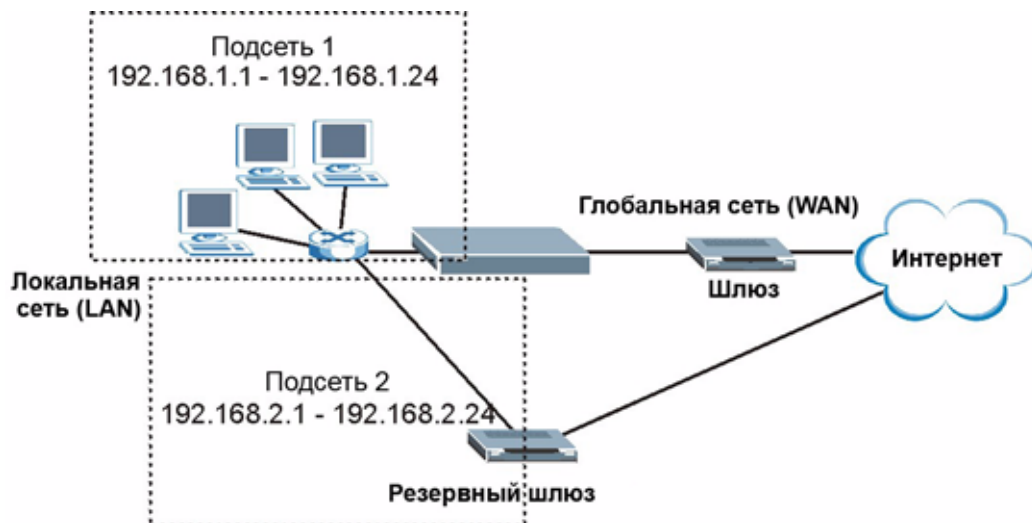
Переадресация трафика направляет трафик к резервному шлюзу, когда P-791R v2 не может подключиться к Интернету. Пример приведен на следующем рисунке.

Рис. 28 Пример переадресации трафика



Следующая топология сети позволяет избежать проблем безопасности, свойственных треугольному маршруту, когда резервный шлюз связан с LAN. Используйте совмещение IP-адресов использования, чтобы организовать в составе LAN две или три логических сети, шлюзом между которыми будет являться P-791R v2. Поместите защищенную LAN в одну подсеть (подсеть 1 на следующем рисунке), а резервный шлюз – в другую подсеть (подсеть 2). Настройте фильтры, разрешающие прохождение пакетов из защищенной LAN (подсеть 1) к резервному шлюзу (подсеть 2).

Рис. 29 Настройка LAN для переадресации трафика



5.7 Интерфейс резервирования через коммутируемый доступ

Порт **Dial Backup** может использоваться для резервного доступа через обычное коммутируемое соединение при нарушении связи на порту WAN. Перед использованием вспомогательного порта (**Dial Backup**) для резервирования убедитесь, что переключатель установлен правильно, а порт подключен. Дополнительные сведения см. в [разд. 5.8 на стр. 80](#).

5.8 Порт резервирования CON/AUX

Порт CON/AUX используется для настройки P-791R v2 для резервирования через модем. Установите переключатель CON/AUX устройства P-791R v2 в положение AUX (вспомогательный порт) для использования порта CON/AUX как резервного порта для доступа к Интернету через модем. Подключите разъем RJ-45 кабеля консоли к порту CON/AUX устройства ZyXEL, а другой конец кабеля — к последовательному порту (COM1, COM2 или другой порт COM) модема.

5.9 Настройка резервирования WAN

Этот экран служит для настройки переадресации трафика на резервный шлюз или подключения через порт резервирования при невозможности соединения P-791R v2 с Интернетом по обычному каналу. Чтобы перейти на этот экран, выберите **WAN > WAN Backup Setup**. Появится изображенный ниже экран.

Рис. 30 Экран WAN > WAN Backup Setup

The screenshot shows the 'WAN Backup Setup' configuration page. At the top, there are three tabs: 'Internet Connection', 'More Connections', and 'WAN Backup Setup'. The main content is organized into three sections:

- WAN Backup Setup:**
 - Backup Type: DSL Link (dropdown)
 - Check WAN IP Address 1: 0.0.0.0
 - Check WAN IP Address 2: 0.0.0.0
 - Check WAN IP Address 3: 0.0.0.0
 - Fail Tolerance: 0
 - Recovery Interval: 0 sec
 - Timeout: 0 sec
- Traffic Redirect:**
 - Active Traffic Redirect:
 - Metric: 15
 - Backup Gateway: 0.0.0.0
- Dial Backup:**
 - Active Dial Backup:
 - Metric: 15
 - Port Speed: 115200 (dropdown)
 - User Name: (empty text box)
 - Password: (empty text box)
 - Primary Phone Number: (empty text box)
 - Advanced Setup: (button)

At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 15 Экран WAN > WAN Backup Setup

ПОЛЕ	ОПИСАНИЕ
Backup Type	<p>Выберите метод, которым P-791R v2 будет проверять наличие DSL-соединения.</p> <p>Выберите DSL Link, чтобы устройство P-791R v2 проверяло наличие физического соединения с DSLAM. Выберите ICMP, чтобы периодически отправлять эхозапросы с P-791R v2 на IP-адреса, заданные в полях Check WAN IP Address.</p>
Check WAN IP Address 1-3	<p>Это поле задает адреса, с помощью которых P-791R v2 будет проверять доступность WAN. Введите IP-адрес ближайшего надежного компьютера (например, адрес DNS-сервера поставщика услуг).</p> <p>Примечание. Если вы активируете переадресацию трафика или резервирование через коммутируемый доступ, здесь необходимо указать по крайней мере один IP-адрес.</p> <p>При использовании резервирования WAN P-791R v2 периодически отправляет эхозапросы на указанные здесь адреса и при неполучении ответа переключается на резервное соединение с WAN (если оно настроено).</p>
Fail Tolerance	<p>Укажите число раз (рекомендуемое значение – 2), которое P-791R v2 может отправить эхозапросы на указанные в поле Check WAN IP Address IP-адреса без получения отклика, прежде чем переключится на резервное соединение с WAN (или на другой вид резервного соединения с WAN).</p>
Recovery Interval	<p>Когда P-791R v2 использует соединение с меньшим приоритетом (обычно – резервное соединение с WAN), устройство периодически проверяет возможность перехода на более приоритетное соединение.</p> <p>Введите длительность интервала в секундах (рекомендуется 30), выдерживаемого P-791R v2 между проверками доступности сети. Увеличьте интервал, если целевой IP-адрес обрабатывает много трафика.</p>
Timeout	<p>Введите число секунд (рекомендуется 3), в течение которого P-791R v2 будет ожидать отклика на один из эхозапросов, отправленных по указанным в поле Check WAN IP Address адресам, прежде чем запрос будет сочтен превысившим время ожидания. Соединение с WAN будет признано недоступным после того, как P-791R v2 обнаружит истечение времени ожидания указанное в поле Fail Tolerance число раз. Если ваша сеть занята или переполнена, введите в этом поле более высокое значение.</p>
Traffic Redirect	<p>Переадресация трафика направляет трафик к резервному шлюзу, когда P-791R v2 не может подключиться к Интернету.</p>
Active Traffic Redirect	<p>Отметьте этот флажок, чтобы устройство P-791R v2 использовало переадресацию трафика при недоступности обычного соединения с WAN.</p> <p>Примечание. Чтобы активировать переадресацию трафика, необходимо настроить как минимум один проверяемый IP-адрес в разделе “Check WAN IP Address”.</p>
Metric	<p>Это поле задает приоритет маршрута среди других маршрутов, используемых P-791R v2.</p> <p>Метрика обозначает “стоимость” передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой “стоимостью”. Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключенным сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже “стоимость”.</p>

Таблица 15 Экран WAN > WAN Backup Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Backup Gateway	Введите IP-адрес резервного межсетевых шлюза в десятичном виде через точку. P-791R v2 автоматически переадресует трафик на этот IP-адрес, если разрывается соединение P-791R v2 с Интернетом.
Dial Backup	
Active Dial Backup	Отметьте этот флажок, чтобы устройство P-791R v2 использовало резервное соединение через коммутируемый доступ при недоступности обычного соединения с WAN. Примечание. Для работы этой функции необходимо указать как минимум в одном из полей "Check WAN IP Address" проверяемый IP-адрес.
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-791R v2. Метрика обозначает "стоимость" передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой "стоимостью". Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключенным сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже "стоимость".
Port Speed	В раскрывающемся списке выберите скорость соединения между WAN-портом и внешним устройством.
User Name	Введите имя пользователя, предоставленное поставщиком услуг Интернета.
Password	Введите пароль, предоставленный поставщиком услуг Интернета.
Primary Phone Number	Введите первый (основной) телефонный номер поставщика услуг Интернета для данного удаленного узла. В тех случаях, когда основной номер занят или не отвечает, устройство набирает запасной номер (Secondary Phone), если он указан. (См. раздел Advanced Setup .) В некоторых телефонных сетях для вызова местных номеров перед ними необходимо набирать решетку (#). В этом случае перед номером нужно указать знак #.
Advanced Setup	Нажмите эту кнопку, чтобы настроить дополнительные параметры резервного соединения.
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

5.9.1 Расширенная настройка резервирования

Этот экран служит для изменения расширенных настроек резервирования через коммутируемый доступ в P-791R v2. Выберите **WAN > WAN Backup Setup > Advanced Setup**. Появится изображенный ниже экран.

Рис. 31 Экран WAN > WAN Backup Setup > Advanced Setup

Basic	
Authentication Type	CHAP/PAP
Secondary Phone Number	
Dial Backup Port Speed	115200
AT Command Initial String	at&fs0=0
Advanced Modem Setup	Edit
TCP/IP Options	
Metric	15
<input checked="" type="checkbox"/> Enable SUA	
<input type="checkbox"/> Enable RIP	
RIP Version	RIP-1
RIP Direction	Both
<input type="checkbox"/> Enable Multicast	
Multicast	IGMP-v2
PPP Options	
Encapsulation	Standard PPP
<input type="checkbox"/> Compression	
Connection	
<input type="radio"/> Nailed-Up Connection	
<input checked="" type="radio"/> Connect on Demand	Max Idle Timeout 100 sec
Budget	
Allocated Budget	0 min
Period	0 hr
<input type="button" value=" < Back"/> <input type="button" value=" Apply"/> <input type="button" value=" Cancel"/>	

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 16 Экран WAN > WAN Backup Setup > Advanced Setup

ПОЛЕ	ОПИСАНИЕ
Basic	
Authentication Type	В раскрывающемся списке выберите протокол аутентификации для исходящих вызовов. Возможны следующие значения: CHAP/PAP - P-791R v2 принимает для данного удаленного узла запросы аутентификации CHAP и PAP. CHAP - P-791R v2 принимает только запросы CHAP. PAP - P-791R v2 принимает только запросы PAP.
Secondary Phone Number	Введите запасной телефонный номер, сообщенный поставщиком услуг Интернета. В тех случаях, когда основной номер занят или не отвечает, устройство набирает запасной номер (Secondary Phone), если он указан. В некоторых телефонных сетях для вызова местных номеров перед ними необходимо набирать решетку (#). В этом случае перед номером нужно указать знак #.
Dial Backup Port Speed	Выберите скорость соединения между портом резервирования через коммутируемый доступ и внешним устройством. Доступны следующие значения: 9600 , 19200 , 38400 , 57600 , 115200 или 230400 бит/с.
AT Command Initial String	Введите AT-строку инициализации устройства, используемого для доступа в WAN. Описание конкретных AT-команд см. в документации на устройство, подключаемое к порту резервирования.
Advanced Modem Setup	Нажмите кнопку Edit , чтобы отредактировать дополнительные настройки модема.

Таблица 16 Экран WAN > WAN Backup Setup > Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
TCP/IP Options	
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-791R v2. Метрика обозначает “стоимость” передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой “стоимостью”. Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключённым сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже “стоимость”.
Enable SUA	Отметьте этот флажок, если требуется использовать NAT, имея один глобальный IP-адрес. Снимите флажок, чтобы отключить NAT.
Enable RIP	Отметьте этот флажок, чтобы включить поддержку протокола RIP для резервного коммутируемого соединения. RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Снимите флажок, чтобы запретить P-791R v2 отправлять пакеты RIP и игнорировать все поступающие пакеты RIP.
RIP Version	Поле RIP Version управляет форматом и способом широковещательной рассылки RIP-пакетов с P-791R v2 (устройство принимает пакеты обоих форматов). RIP-1 поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации RIP-2B и RIP-2M передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в RIP-2B используется широковещательная рассылка по подсетям, а в RIP-2M – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.
RIP Direction	Поле RIP Direction управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: Both (оба направления) / In Only (только вход) / Out Only (только выход). Если выбраны значения Both или Out Only , P-791R v2 будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбрано значение Both или In Only , устройство будет учитывать информацию, получаемую в пакетах RIP.
Enable Multicast	Отметьте этот флажок, чтобы включить поддержку протокола IGMP для резервного коммутируемого соединения. IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки.
Multicast	P-791R v2 поддерживает IGMP версии 1 (IGMP-v1) и IGMP-v2 .
PPP Options	
Encapsulation	Если устройство, через которое осуществляется резервирование, использует протокол инкапсуляции Cisco для PPP-соединений, выберите в раскрывающемся списке CISCO PPP , в противном случае выберите Standard PPP .
Compression	Отметьте этот флажок, чтобы включить сжатие STAC.
Connection	
Nailed-Up Connection	Выберите Nailed-Up Connection , чтобы использовать закрепленное соединение, которое активно все время. P-791R v2 будет пытаться автоматически восстановить соединение при разрыве сеанса.

Таблица 16 Экран WAN > WAN Backup Setup > Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Connect on Demand	Если соединение не требуется поддерживать постоянно, выберите Connect on Demand и укажите интервал неактивности в поле Max Idle Timeout .
Max Idle Timeout	Если вы выбрали режим Connect on Demand , в поле Max Idle Timeout укажите интервал неактивности. Значение по умолчанию – 0, при котором сеанс соединения с Интернетом не завершается никогда.
Budget	
Allocated Budget	Введите максимальную продолжительность каждого вызова (в минутах). Чтобы снять ограничение на продолжительность вызова, введите 0. Поле Period позволяет ограничить суммарную продолжительность исходящего вызова с P-791R v2. Если общее время исходящих вызовов превышает лимит, текущий вызов отбрасывается, и все последующие исходящие вызовы блокируются.
Period	Введите количество часов, по истечении которого параметр Allocated Budget будет сбрасываться. Например, если в течение каждого часа под исходящие вызовы выделяется 30 минут, установите параметр Allocated Budget равным 30, а в этом поле введите 1.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку Back .
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

5.9.2 Расширенные настройки модема для резервирования через коммутируемый доступ

Этот экран служит для изменения расширенных настроек модема для резервирования через коммутируемый доступ в P-791R v2. Выберите **WAN > WAN Backup Setup > Advanced Setup > Edit**. Появится изображенный ниже экран.

Рис. 32 Экран WAN > WAN Backup Setup > Advanced Setup > Edit

The screenshot shows the following configuration details:

- AT Command Strings:**
 - Dial: atd
 - Drop: rnm+++mwrath
 - Answer: ata
 - Drop DTR When Hang Up
- AT Response Strings:**
 - CLID: NMBR =
 - Called ID: (empty)
 - Speed: CONNECT
- Call Control:**
 - Dial Timeout: 60 sec
 - Retry Count: 0
 - Retry Interval: 10 sec
 - Drop Timeout: 20 sec
 - Call Back Delay: 15 sec

Buttons at the bottom: <Back, Apply, Cancel

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 17 Экран WAN > WAN Backup Setup > Advanced Setup > Edit

ПОЛЕ	ОПИСАНИЕ
AT Command Strings	
Dial	Введите AT-команду для осуществления вызова.
Drop	Введите AT-команду для завершения вызова. Символ “~” кодирует 1-секундную задержку. Например, для модемов с медленным откликом можно использовать строку “~~~+++~ath”.
Answer	Введите AT-команду для ответа на входящий вызов.
Drop DTR When Hang Up	Отметьте этот флажок, чтобы осуществлять сброс линии DTR после отправки строки, указанной в поле Drop .
AT Response Strings	
CLID	Введите ключевое слово, после которого в AT-строке отклика приводится CLID (идентификация вызывающей линии). Это позволяет P-791R v2 извлекать CLID из AT-строки доступа, полученной от устройства, через которое осуществляется доступ в WAN. Идентификатор CLID применяется для CLID-аутентификации.
Called ID	Введите ключевое слово, которое предшествует набираемому номеру.
Speed	Введите ключевое слово, которое предшествует скорости соединения.
Call Control	
Dial Timeout	Укажите число секунд, в течение которых P-791R v2 будет ожидать установления исходящего соединения перед прекращением операции. P-791R v2 сообщает об истечении времени ожидания и прекращает попытку установления исходящего соединения, если его не удалось установить за указанное время.
Retry Count	Укажите число повторных попыток набора номера, которые P-791R v2 будет предпринимать при обнаружении сигнала “занято” или при отсутствии ответа удаленной стороны, прежде чем номер будет занесен в черный список.
Retry Interval	Укажите продолжительность паузы (в секундах), которую P-791R v2 будет выдерживать между попытками повторного набора номера. Эта пауза действует до занесения номера в черный список.
Drop Timeout	Введите число секунд, по истечении которых P-791R v2 сбросит сигнал DTR, если не будет получено явное подтверждение разъединения.
Call Back Delay	Укажите длительность паузы (в секундах), которую P-791R v2 будет выдерживать между завершением запроса встречного вызова (callback) и началом соответствующего встречного вызова.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку Back .
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

Настройка LAN

В этой главе описывается настройка параметров локальной сети.

6.1 Обзор локальной сети

Локальная вычислительная сеть (LAN, ЛВС) - общедоступная система связи, к которой подключено множество компьютеров. Локальная сеть объединяет компьютеры, сосредоточенные на определённой площади, обычно – находящиеся в одном здании или на одном этаже. Экраны LAN помогают настраивать DHCP-сервер для локальной сети и управлять IP-адресами.

Выполнение настроек на экранах LAN описано в [разд. 6.3 на стр. 91](#).

6.1.1 Сети LAN, WAN и P-791R v2

От непосредственного физического подключения зависит, являются ли порты P-791R v2 портами WAN или LAN. Как показано ниже, существуют две отдельных IP-сети: внутренняя (сеть LAN) и внешняя (сеть WAN).

Рис. 33 IP-адреса в сетях LAN и WAN



6.1.2 Настройка DHCP

DHCP (протокол динамической настройки хоста, RFC 2131 и RFC 2132) позволяет клиентам в момент запуска получать настройки TCP/IP с сервера. P-791R v2 позволяет включить или отключить встроенный DHCP-сервер. Когда устройство P-791R v2 настроено в качестве DHCP-сервера, оно сообщает настройки TCP/IP клиентам. Если служба DHCP отключена, необходимо иметь в своей LAN другой DHCP-сервер или настраивать компьютеры вручную.

6.1.2.1 Настройка IP-пула

В P-791R v2 имеется предварительно настроенный диапазон IP-адресов для клиентов DHCP (пул DHCP). См. техническое описание в приложениях. Не назначайте компьютерам в локальной сети статические адреса, принадлежащие пулу DHCP.

6.1.3 Адрес DNS-сервера

DNS (система доменных имен) предназначена для установки соответствия доменного имени соответствующему IP-адресу и наоборот. DNS-сервер крайне важен, потому что без него для получения доступа к компьютеру пришлось бы выяснять его IP-адрес. Адреса DNS-серверов, указанные в настройках DHCP, передаются клиентским компьютерам вместе с присвоенными им IP-адресами и маской подсети.

Поставщик услуг Интернета может распространять адреса серверов DNS двумя способами. Первый способ - адреса DNS-серверов сообщаются абоненту в информационном бюллетене при подключении к услугам. Если ваш поставщик услуг Интернета сообщил вам адреса DNS-серверов, введите их в полях **DNS Server** на экране **DHCP Setup**, в противном случае оставьте эти поля пустыми.

Некоторые поставщики услуг Интернета передают информацию о DNS-серверах посредством специальных расширений управляющего протокола IP (IPCP) после установки PPP-соединения. Если ваш поставщик услуг Интернета не сообщил адреса DNS-серверов в явном виде, возможно, что эти адреса будут переданы во время согласования IPCP. P-791R v2 поддерживает расширения IPCP для передачи информации о DNS-серверах посредством функции прокси-сервера для DNS.

Если поля **Primary** и **Secondary DNS Server** на экране **DHCP Setup** не заполнены (в частности, если в них оставлено значение **0.0.0.0**), устройство P-791R v2 будет сообщать DHCP-клиентам, что DNS-сервером является оно само. Когда компьютер в сети LAN отправляет запрос DNS в P-791R v2, P-791R v2 переадресует запрос на DNS-сервер, адрес которого получен в IPCP, и передает отклик обратно компьютеру.

Необходимо отметить, что функция прокси-сервера для DNS работает только тогда, когда поставщик услуг Интернета использует расширения управляющего протокола IP (IPCP) для передачи информации о DNS-серверах. Это не означает, что во всех случаях можно не указывать DNS-серверы в настройках DHCP. Если ваш поставщик услуг Интернета сообщил вам IP-адреса DNS-серверов в явном виде, не забудьте ввести эти адреса на экране **DHCP Setup**. Это позволит P-791R v2 передавать DNS-серверы на компьютеры, которые в свою очередь смогут выполнять запрос DNS-сервера непосредственно без участия P-791R v2.

6.1.4 Присвоение адресов DNS-серверов

DNS (система доменных имен) предназначена для установки соответствия имени домена с соответствующим IP-адресом и наоборот. DNS-сервер крайне важен, потому что без него для получения доступа к компьютеру пришлось бы выяснять его IP-адрес.

Поставщик услуг Интернета может распространять адреса серверов DNS двумя способами.

- Первый способ – адреса DNS-серверов сообщаются абоненту в информационном бюллетене при подключении к услугам. Если ваш поставщик услуг Интернета сообщил вам адреса DNS-серверов, введите их на экране **DHCP Setup**.
- P-791R v2 выступает в роли прокси-сервера для DNS, когда поля **Primary** и **Secondary DNS Server** на экране **DHCP Setup** оставлены со значениями **0.0.0.0**.

6.2 Параметры TCP/IP для локальной сети

P-791R v2 имеет встроенный DHCP-сервер, который назначает IP-адреса и сообщает адреса DNS-серверов системам с функцией DHCP-клиента.

Параметры локальной сети в P-791R v2 предварительно установлены на заводе и имеют следующие значения:

- IP-адрес 192.168.1.1 с маской подсети 255.255.255.0 (24 бита)
- DHCP-сервер, выдающий до 32 клиентских IP-адресов, начиная с 192.168.1.33.

Эти параметры должны быть работоспособны в большинстве случаев. Если провайдер предоставляет конкретные адреса (адреса) DNS-сервера, обращайтесь к встроенной справочной системе веб-конфигуратора для выяснения того, какие поля необходимо настроить.

6.2.1 IP-адрес и маска подсети

Подобно домам на улице, для которых общим является название улиц, компьютеры в составе локальной сети связаны общим номером сети.

В зависимости от конкретной ситуации этот номер присваивается различными службами. Если поставщик услуг Интернета или администратор вашей сети присвоил вам блок зарегистрированных IP-адресов, необходимо следовать его указаниям по выбору IP-адресов и маски подсети.

Если поставщик услуг Интернета не сообщил вам номер IP-подсети в явном виде, то наиболее вероятно, что вы используете единственную учетную запись пользователя, и поставщик услуг Интернета назначит вам динамический IP-адрес при установлении соединения. В этом случае рекомендуется выбрать номер сети от 192.168.0.0 до 192.168.255.0. Также потребуется разрешить в P-791R v2 функцию трансляции сетевых адресов (NAT). Комитет по цифровым адресам в Интернете (Internet Assigned Number Authority, IANA) зарезервировал определённые диапазоны адресов специально для частных применений; все адреса, которые не принадлежат этим диапазонам, не должны использоваться без специальных на то указаний. Предположим, что в качестве номера

сети выбран 192.168.1.0. Он содержит 254 отдельных адреса, от 192.168.1.1 до 192.168.1.254 (ноль и 255 зарезервированы). Иначе говоря, первые три числа составляют номер сети, а последнее число идентифицирует конкретный компьютер в этой сети.

После выбора номера сети выберите для P-791R v2 легкозапоминающийся IP-адрес, например, 192.168.1.1, но этот адрес не должен использоваться никаким другим устройством в вашей сети.

Маска подсети указывает на долю номеров IP-адресов в сети. P-791R v2 автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. В отсутствие специальных указаний изменять маску подсети, предлагаемую P-791R v2, не следует.

6.2.1.1 Частные IP-адреса

Каждому компьютеру в Интернете должен соответствовать уникальный адрес. В сетях, которые отделены от Интернета - например, в сети между двумя филиалами, можно назначать хостам любые IP-адреса, не испытывая каких-либо затруднений. Тем не менее, Комитет по цифровым адресам в Интернете (IANA) специально для частных сетей зарезервировал следующие три блока IP-адресов:

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

IP-адрес может быть выдан IANA или провайдером, либо присвоен в рамках частной сети. Для небольших организаций, получающих доступ в Интернет от поставщика услуг Интернета, Интернет-адреса для локальных сетей могут выдаваться непосредственно поставщиком услуг. В то же время подразделениям более крупных организаций следует согласовывать назначение IP-адресов с сетевым администратором.



Независимо от конкретных обстоятельств выбирать произвольные IP-адреса ни в коем случае не следует; всегда необходимо придерживаться приведенных выше указаний. Более подробно присвоение адресов описано в документах RFC 1597 (*выделение адресов для частных интрасетей*) и RFC 1466 (*регламент адресного пространства IP*).

6.2.2 Настройка RIP

RIP (информационный протокол маршрутизации) позволяет маршрутизатору обмениваться сведениями о маршрутах с другими маршрутизаторами. Поле **RIP Direction** управляет процессом отправки и приема RIP-пакетов. Возможные значения:

- **Both** - P-791R v2 будет периодически распространять таблицу маршрутизации по ширококвещательному запросу и объединять принимаемые параметры RIP.
- **In Only** - P-791R v2 не будет отправлять RIP-пакеты, но будет обрабатывать все принимаемые RIP-пакеты.

- **Out Only** - P-791R v2 будет отправлять RIP-пакеты, но не будет обрабатывать поступающие RIP-пакеты.
- **None** - P-791R v2 не будет отправлять RIP-пакеты и будет игнорировать все поступающие RIP-пакеты.

Поле **Version** управляет форматом и способом широковещательной рассылки RIP-пакетов со стороны P-791R v2 (устройство принимает пакеты обоих форматов). **RIP-1** поддерживается всеми устройствами, а **RIP-2** позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией.

Модификации **RIP-2B** и **RIP-2M** передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в **RIP-2B** используется широковещательная рассылка по подсетям, а в **RIP-2M** – многоадресная рассылка.

6.2.3 Multicast

Традиционно существует два способа передачи IP-пакетов: одноадресный (один отправитель – один получатель) и широковещательный (от одного отправителя ко всем узлам сети). При многоадресной рассылке пакеты IP адресуются некоторой группе хостов в сети – не всем, но и не одному.

IGMP (межсетевой протокол многоадресной групповой рассылки) представляет собой протокол сетевого уровня для установления членства в группе многоадресной рассылки – он не применяется для пересылки каких-либо пользовательских данных. Версия 2 IGMP (RFC 2236) – развитие версии 1 (RFC 1112), первая версия протокола IGMP продолжает широко использоваться. Более подробно информацию о функциональной совместимости между версией 2 и версией 1 IGMP можно узнать в разделах 4 и 5 документа RFC 2236. IP-адреса класса D используются для идентификации групп хостов и могут находиться в диапазоне от 224.0.0.0 до 239.255.255.255. Адрес 224.0.0.0 не присвоен ни одной группе и используется компьютерами для многоадресной рассылки IP. Адрес 224.0.0.1 используется для сообщений запроса и назначен постоянной группе всех хостов IP (включая шлюзы). Для участия в IGMP все хосты должны войти в состав группы 224.0.0.1. Адрес 224.0.0.2 назначен группе маршрутизаторов многоадресной рассылки.

P-791R v2 поддерживает версию 1 IGMP (**IGMP-v1**) и версию 2 (**IGMP-v2**). При запуске P-791R v2 опрашивает все непосредственно связанные с ним сети, чтобы собрать информацию о принадлежности к группам. Впоследствии P-791R v2 периодически обновляет эту информацию. Многоадресную рассылку IP на LAN- и/или WAN-интерфейсах P-791R v2 можно разрешить/запретить с помощью веб-конфигуратора (**LAN**; **WAN**). Чтобы отключить многоадресную рассылку на этих интерфейсах, выберите **None**.

6.3 Настройка параметров IP для локальной сети

Этот экран позволяет настроить IP-адрес P-791R v2 со стороны LAN. Выберите **LAN > IP**. Дополнительные сведения см. в [разд. 6.1 на стр. 87](#).

Рис. 34 Экран LAN > IP

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 18 Экран LAN > IP

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите IP-адрес P-791R v2 в виде десятичных чисел через точку, например: 192.168.1.1 (заводская настройка по умолчанию).
IP Subnet Mask	Введите маску подсети, которая используется вашей сетью. Дополнительные сведения см. в разд. 6.2.1 на стр. 89 .
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран Advanced LAN Setup для настройки дополнительных параметров локальной сети.

6.3.1 Настройка дополнительных параметров локальной сети

Этот экран используется для редактирования расширенных параметров настройки LAN в P-791R v2. На экране **LAN IP** нажмите кнопку **Advanced Setup**. Появится изображенный ниже экран.

Рис. 35 Экран LAN > IP > Advanced Setup

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 19 Экран LAN > IP > Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Поле RIP Direction управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: Both (вход-выход), In Only (только вход) или Out Only (только выход), None (нет). Если выбраны значения Both или Out Only , P-791R v2 будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения Both или In Only , устройство будет объединять получаемые параметры RIP; если выбрано значение None , устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.
RIP Version	Это поле доступно в том случае, если в поле RIP Direction выбран любой параметр, кроме None . Поле RIP Version управляет форматом и способом широковещательной рассылки RIP-пакетов с P-791R v2 (устройство принимает пакеты обоих форматов). RIP-1 поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации RIP-2B и RIP-2M передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в RIP-2B используется широковещательная рассылка по подсетям, а в RIP-2M – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.
Multicast	IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки. P-791R v2 поддерживает IGMP версии 1 (IGMP-v1) и IGMP-v2 . Чтобы отключить этот протокол, выберите None .
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (базовая сетевая система ввода-вывода) представляет собой широковещательные пакеты TCP или UDP, позволяющие компьютеру подключаться и взаимодействовать с локальной сетью. Пакеты NetBIOS могут приводить к вызову служб коммутируемого доступа посредством PPPoE или PPTP, даже если эти службы не были запрошены пользователем. В других случаях требуется разрешить пакетам NetBIOS проходить в сеть WAN, чтобы найти компьютер на стороне WAN.
Allow between LAN and WAN	Отметьте этот флажок, чтобы разрешить пересылку пакетов NetBIOS из LAN в WAN и из WAN в LAN. Снимите этот флажок, чтобы блокировать пакеты NetBIOS, пересылаемые из LAN в WAN и из WAN в LAN.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку Back .
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

6.4 Настройка DHCP

Этот экран служит для настройки параметров DNS-сервера, которые P-791R v2 сообщает DHCP-клиентам в локальной сети.

Рис. 36 Экран LAN > DHCP Setup

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 20 Экран LAN > DHCP Setup

ПОЛЕ	ОПИСАНИЕ
DHCP Setup	
DHCP	<p>Выберите тип DHCP-службы, который P-791R v2 будет предоставлять в локальной сети. Возможны следующие варианты:</p> <p>None – P-791R v2 не предоставляет службу DHCP в локальной сети. В сети уже имеется DHCP-сервер.</p> <p>Relay – P-791R v2 пересылает DHCP-запросы на DHCP-сервер. DHCP-сервер может находиться в другой сети.</p> <p>Server – P-791R v2 присваивает сетевым клиентам IP-адреса и предоставляет им маску подсети, адрес шлюза и параметры DNS-серверов. P-791R v2 выступает в качестве DHCP-сервера в сети.</p>
IP Pool Starting Address	Это поле доступно в том случае, если P-791R v2 выступает в качестве сервера (Server). Введите начальный адрес непрерывного пула IP-адресов.
Pool Size	Это поле доступно в том случае, если P-791R v2 выступает в качестве сервера (Server). Введите размер DHCP-пула (количество IP-адресов).
Remote DHCP Server	Это поле доступно в том случае, если P-791R v2 работает в режиме ретрансляции (Relay). Введите IP-адрес DHCP-сервера, которому устройство P-791R v2 должно ретранслировать запросы.
DNS Server	
DNS Servers Assigned by DHCP Server	P-791R v2 передает IP-адрес сервера DNS (системы доменных имен) клиентам DHCP.
Primary DNS Server Secondary DNS Server	<p>Это поле доступно в том случае, если параметр DHCP установлен в значение Relay.</p> <p>Введите IP-адреса DNS-серверов. Адреса DNS-серверов передаются клиентским компьютерам вместе с присвоенными им IP-адресами и маской подсети.</p> <p>Если в этих полях оставлено значение 0.0.0.0, P-791R v2 выступает в качестве прокси-сервера для DNS, передавая запрос на DNS-сервер, адрес которого получен в IPCP, и возвращая отклик компьютеру.</p>
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

6.5 Список клиентов в локальной сети

Эта таблица позволяет закрепить локальные IP-адреса за компьютерами с конкретными MAC-адресами.

Каждое устройство Ethernet имеет уникальный MAC-адрес (MAC - контроль доступа к передающей среде). MAC-адрес назначается на заводе и состоит из шести пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02.

Этот экран служит для изменения статических настроек DHCP в P-791R v2. Выберите **Network > LAN > Client List**. Появится изображенный ниже экран.

Рис. 37 Экран LAN > Client List

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 21 Экран LAN > Client List

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите IP-адрес, который требуется присвоить компьютеру в локальной сети с указанным ниже MAC-адресом. IP-адрес DHCP-клиента должен находиться в диапазоне IP-адресов, указанном в поле DHCP Setup .
MAC Address	Введите MAC-адрес компьютера в локальной сети.
Add	Нажмите Add , чтобы добавить статическую запись DHCP.
#	В данном поле отображается порядковый номер (строка) в статической таблице IP-адресов.
Status	В данном поле отображается состояние соединения клиента с P-791R v2.
Host Name	В данном поле отображается имя - хост компьютера.
IP Address	В данном поле отображается IP-адрес, соответствующий полю #, указанному в списке выше.
MAC Address	MAC-адрес, также называемый Ethernet-адресом локальной сети, уникален для каждого компьютера (адрес состоит из шести пар шестнадцатеричных символов). Плата сетевого интерфейса, например, Ethernet-адаптер, имеет жёстко запрограммированный заводской адрес. Порядок присвоения таких адресов является промышленным стандартом и позволяет исключить появление двух адаптеров с одинаковым адресом.
Reserve	Отметьте флажками записи, которым P-791R v2 всегда будет присваивать выбранные IP-адреса в соответствии с указанными MAC-адресами (и именами хостов). В таблице можно выбрать до 32 записей.
Modify	Щелкните на значке редактирования, чтобы сделать поле IP-адреса доступным для редактирования и изменить адрес.
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.

Таблица 21 Экран LAN > Client List (продолжение)

ПОЛЕ	ОПИСАНИЕ
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .
Refresh	Чтобы повторно загрузить таблицу DHCP, нажмите кнопку Refresh .

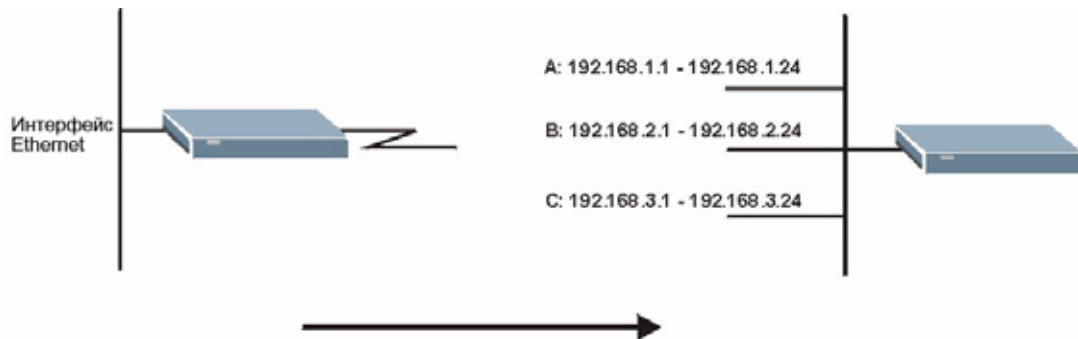
6.6 Совмещение IP-адресов в локальной сети

Функция совмещения IP-адресов (IP aliasing) позволяет разделить физическую сеть на различные логические сети, использующие один и тот же интерфейс Ethernet. P-791R v2 поддерживает до трех логических интерфейсов LAN на одном физическом интерфейсе Ethernet, при этом P-791R v2 будет выступать в качестве межсетевого шлюза для каждой сети LAN.



Следите за тем, чтобы подсети логических сетей не перекрывались.

На следующем рисунке показана сеть LAN, разделенная на подсети А, В, и С.

Рис. 38 Физическая сеть и отдельные логические сети

Этот экран служит для настройки подсетей в сети LAN. Выберите **Network > LAN > IP Alias**. Появится изображенный ниже экран.

Рис. 39 Экран LAN > IP Alias

The screenshot shows the 'IP Alias' configuration window. It has a tabbed interface with 'IP Alias' selected. There are two sections, 'IP Alias 1' and 'IP Alias 2'. Each section contains a checkbox to enable the alias, and four fields: 'IP Address' (text input with '0.0.0.0'), 'IP Subnet Mask' (text input with '0.0.0.0'), 'RIP Direction' (dropdown menu with 'None' selected), and 'RIP Version' (dropdown menu with 'N/A' selected). At the bottom of the window are 'Apply' and 'Cancel' buttons.

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 22 Экран LAN > IP Alias

ПОЛЕ	ОПИСАНИЕ
IP Alias 1, 2	Отметьте флажок, чтобы настроить другую сеть LAN для P-791R v2.
IP Address	Введите IP-адрес вашего P-791R v2 в десятичном виде через точку. Вместо этого можно щелкнуть правой кнопкой мыши, чтобы скопировать и/или вставить IP-адрес.
IP Subnet Mask	P-791R v2 автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. Если вам не требуется деление на подсети, используйте маску подсети, рассчитанную P-791R v2.
RIP Direction	RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Поле RIP Direction управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: Both (вход-выход), In Only (только вход) или Out Only (только выход), None (нет). Если выбраны значения Both или Out Only , P-791R v2 будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения Both или In Only , устройство будет объединять получаемые параметры RIP; если выбрано значение None , устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.
RIP Version	Это поле доступно в том случае, если в поле RIP Direction выбран любой параметр, кроме None . Поле RIP Version управляет форматом и способом широковещательной рассылки RIP-пакетов с P-791R v2 (устройство принимает пакеты обоих форматов). RIP-1 поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации RIP-2B и RIP-2M передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в RIP-2B используется широковещательная рассылка по подсетям, а в RIP-2M – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.

Таблица 22 Экран LAN > IP Alias (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

Экраны настройки NAT

В этой главе поясняется способ настройки NAT в P-791R v2.

7.1 Краткий обзор NAT

NAT (Network Address Translation - трансляция сетевых адресов, RFC 1631) представляет собой механизм преобразования IP-адреса хоста в пакете, например адреса отправителя в исходящем пакете, при котором адреса, используемые в одной сети, заменяются адресами, известными в другой сети.

7.1.1 Определения, относящиеся к NAT

Термины "внешний" и "внутренний" определяют положение хоста относительно P-791R v2, например, компьютеры абонентов - это внутренние хосты, а веб-серверы в Интернете являются внешними хостами.

Термины "глобальный" и "локальный" характеризуют IP-адрес хоста в пакетах, проходящих через маршрутизатор, например, локальный адрес - это адрес хоста при нахождении пакета в локальной сети, а глобальный адрес - это адрес, соответствующий данному хосту при нахождении пакета в глобальной сети.

Обратите внимание на то, что "внутренний" / "внешний" относится к местоположению хоста, в то время как "глобальный" / "локальный" – к IP-адресу хоста, используемому в пакете. Таким образом, внутренний локальный адрес (ILA) – это IP-адрес внутреннего хоста в пакете, когда пакет все еще находится в локальной сети, в то время как внутренний глобальный адрес (IGA) – IP-адрес того же самого внутреннего хоста, когда пакет находится в WAN. Эти сведения обобщены в следующей таблице.

Таблица 23 Определения, относящиеся к NAT

ТЕРМИН	ОПИСАНИЕ
Внутренний	Термин относится к хосту в сети LAN.
Внешний	Термин относится к хосту в сети WAN.
Local	Термин относится к адресу пакета (адресу отправки или назначения) при его перемещении по LAN.
Глобальный	Термин относится к адресу пакета (адресу отправки или назначения) при его перемещении по WAN.

NAT никогда не приводит к изменению IP-адреса (локального или глобального) внешнего хоста.

7.1.2 Назначение NAT

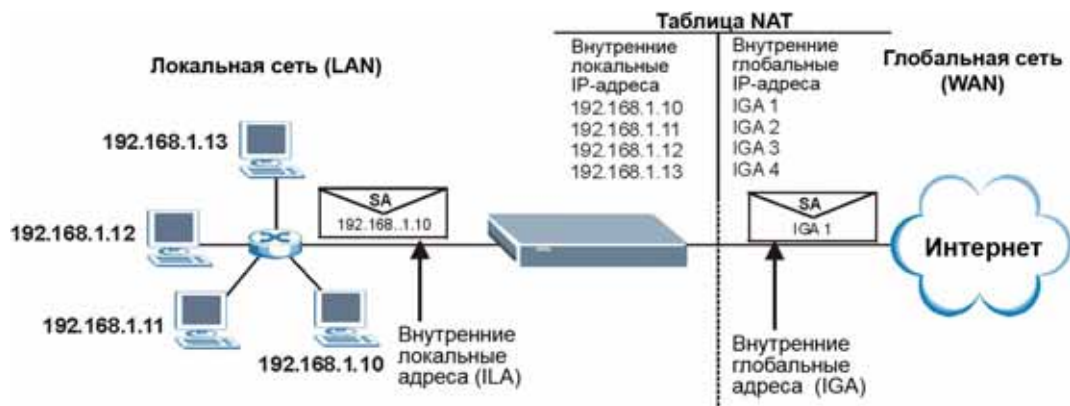
В самой простой форме NAT заменяет исходный IP-адрес в пакете, полученном от абонента (внутреннего локального адреса), на другой адрес (внутренний глобальный адрес) перед отправлением пакета на сторону WAN. Когда ответ возвращается, NAT преобразовывает адрес получателя (внутренний глобальный адрес) обратно во внутренний локальный адрес перед его отправкой исходному внутреннему хосту. Обратите внимание на то, что IP-адрес (локальный или глобальный) внешнего хоста никогда не изменяется.

Глобальные IP-адреса для внутренних хостов могут назначаться ISP статически или динамически. Кроме того, можно определять серверы (например, веб-сервер и telnet-сервер) в локальной сети и делать их доступными для внешнего мира. Если серверы не определены (для схем трансляции “многие к одному” и “многие ко многим с перегрузкой” – см. таб. 24 на стр. 102), NAT обеспечивает дополнительную защиту, играя роль сетевого экрана. Если серверы не определены, P-791R v2 отфильтровывает все поступающие запросы, таким образом препятствуя проникновению в сеть злоумышленников. Для получения дополнительной информации о преобразовании IP-адреса обращайтесь к *RFC 1631, Преобразователь IP-адресов сети (NAT)*.

7.1.3 Принцип работы NAT

Каждый пакет имеет два адреса – адрес источника и адрес получателя. Для исходящих пакетов ILA (Внутренний локальный адрес) – исходный адрес в LAN, а IGA (Внутренний глобальный адрес) – исходный адрес в WAN. Для поступающих пакетов ILA - адрес места назначения в LAN, а IGA - в WAN. NAT привязывает частные (локальные) IP-адреса к глобальным уникальным, требуемым для обмена данными с хостами в других сетях. В каждом пакете заменяется исходный IP-адрес (а в режимах “многие к одному” и “многие ко многим с перегрузкой” – также и номер исходного порта TCP/UDP), после чего пакет пересылается в Интернет. P-791R v2 отслеживает оригинальные адреса и номера портов, чтобы в поступающих ответных пакетах восстанавливались исходные значения. Это проиллюстрировано на следующем рисунке.

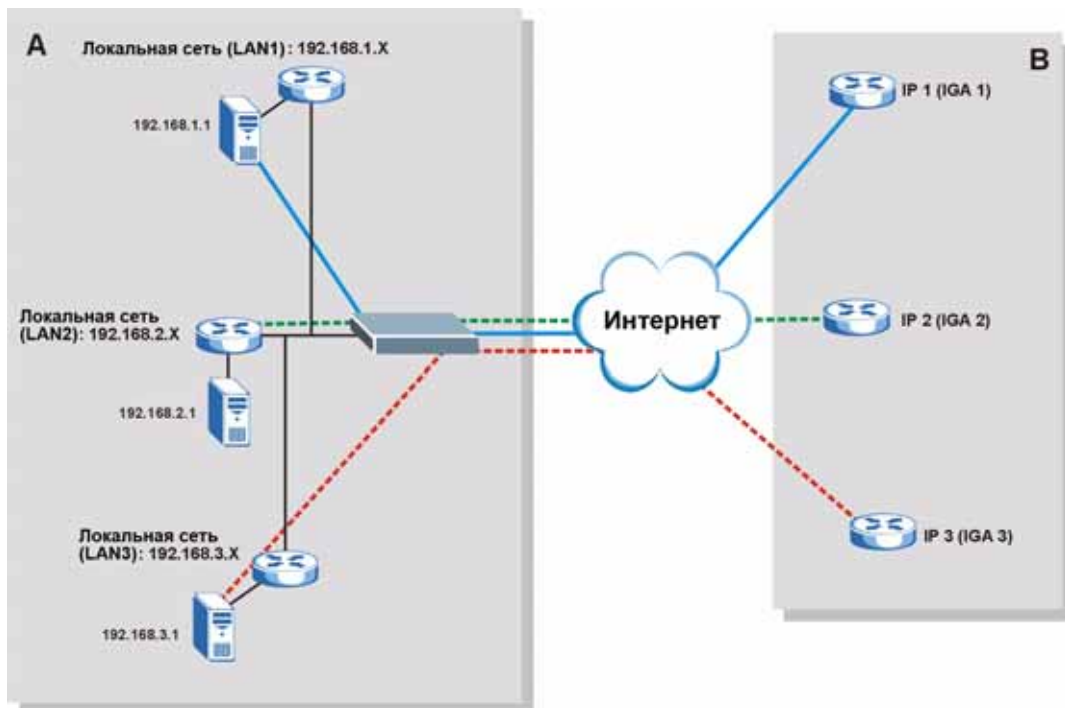
Рис. 40 Принцип работы NAT



7.1.4 Применение NAT

На следующем рисунке иллюстрируется возможное применение NAT, в котором три внутренние сети LAN (логические LAN, использующие совмещение IP-адресов) за P-791R v2 могут обмениваться данными с тремя отдельными сетями WAN. Дополнительные примеры приводятся в конце этой главы.

Рис. 41 Применение NAT с IP-псевдонимом



7.1.5 Типы привязки NAT

NAT поддерживает пять типов привязки IP/порта. А именно:

- **Один - один:** в режиме “один к одному” P-791R v2 привязывает один локальный IP-адрес к одному глобальному IP-адресу.
- **Многие к одному:** в режиме “многие к одному” P-791R v2 привязывает несколько локальных IP-адресов к одному глобальному IP-адресу. Этот режим эквивалентен режиму SUA (Single User Account), использовавшемуся в прежних маршрутизаторах ZyXEL (в текущих моделях ему соответствует параметр **SUA Only**). Фактически данный режим представляет собой PAT – трансляцию адресов портов.
- **Многие ко многим с перегрузкой:** в режиме “многие ко многим с перегрузкой” P-791R v2 привязывает несколько локальных IP-адресов к общим глобальным IP-адресам.
- **Многие ко многим без перегрузки:** в режиме “многие ко многим без перегрузки” P-791R v2 привязывает каждый локальный IP-адрес к уникальному глобальному IP-адресу.
- **Server:** этот режим позволяет указывать внутренние серверы различных служб в NAT, которые должны быть доступными для внешнего мира.

В режимах привязки NAT “один к одному” и “многие к одному” номера портов NE изменяются.

В следующей таблице дается сводная информация об этих типах.

Таблица 24 Типы привязки NAT

ТИП	ПРИВЯЗКА IP
Один к одному	ILA1 ↔ IGA1
Многие к одному (SUA/PAT)	ILA1 ↔ IGA1 ILA2 ↔ IGA1 ...
Многие ко многим с перегрузкой	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA1 ILA4 ↔ IGA2 ...
Многие ко многим без перегрузки	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA3 ...
Server	IP-адрес сервера 1 ↔ IGA1 IP-адрес сервера 2 ↔ IGA1 IP-адрес сервера 3 ↔ IGA1

7.2 Сравнение SUA и NAT

SUA (Single User Account – одна учетная запись) представляет собой подмножество NAT, реализуемое операционной системой ZyNOS и включающее два типа привязки: “многие к одному” и “сервер”. P-791R v2 также поддерживает полноценный режим NAT (**Full Feature**), в котором несколько глобальных IP-адресов привязываются к нескольким IP-адресам клиентов или серверов в частных сетях LAN с помощью одного из способов, перечисленных в таб. 24 на стр. 102.

- Если для P-791R v2 выделен только один глобальный IP-адрес в сети WAN, выберите **SUA Only**.
- Если для P-791R v2 выделено несколько глобальных IP-адресов в сети WAN, выберите **Full Feature**.

7.2.1 SIP ALG

Некоторые приложения, например SIP, не могут работать через NAT (“недружественны” к NAT), поскольку они вставляют IP-адреса и номера портов в полезную нагрузку пакетов.

Некоторые маршрутизаторы с функцией NAT имеют поддержку шлюза прикладного уровня (ALG) для протокола SIP. Шлюз прикладного уровня управляет определенным протоколом (например SIP, H.323 или FTP) на прикладном уровне.

SIP ALG позволяет пропускать вызовы SIP через NAT, проверяя и преобразуя IP-адреса в составе потока данных.

Когда VoIP устройство регистрируется на сервере регистрации SIP, SIP ALG преобразует частный IP-адрес P-791R v2 в потоке данных в глобальный IP-адрес. Если P-791R v2 располагается за SIP ALG, использовать STUN или прокси-сервер для исходящих запросов не требуется.

7.3 Общая настройка NAT

Чтобы разрешить пересылку трафика из WAN через P-791R v2, в дополнение к настройке SUA/NAT необходимо создать правило для сетевого экрана. Выберите **Network > NAT**, чтобы открыть следующий экран.

Рис. 42 Экран NAT > General



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 25 Общие настройки NAT

ПОЛЕ	ОПИСАНИЕ
Active Network Address Translation (NAT)	Установите этот флажок, чтобы активировать NAT.
SUA Only	Выберите этот переключатель, если для P-791R v2 выделен только один глобальный IP-адрес в сети WAN.
Full Feature	Выберите этот переключатель, если для P-791R v2 выделено несколько глобальных IP-адресов в сети WAN.
Max NAT/Firewall Session Per User	Для компьютеров, работающих в одноранговых (P2P) сетях, например, в файлообменных сетях, необходимо устанавливать сеансы через NAT. В отсутствие ограничения на число сеансов NAT, открываемых одним клиентом, все сеансы NAT могут оказаться исчерпаны. В этом случае невозможно установить новые сеансы NAT, и пользователи не могут выходить в Интернет. Если в вашей сети P2P-приложениями пользуется мало клиентов, можно увеличить это значение, чтобы ограничение числа устанавливаемых сеансов NAT не ухудшало производительность. Если в вашей сети P2P-приложениями пользуется большое число клиентов, можно уменьшить это число, чтобы исключить перерасходование набора сеансов NAT отдельными клиентами.
Enable SIP ALG	Отметьте этот флажок, если необходима корректная работа SIP (VoIP) с переадресацией портов и триггерными портами.
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Чтобы вернуть настройки на этом экране в их прежнее состояние, нажмите Cancel .

7.4 Port Forwarding

Набор адресов для переадресации портов – это список внутренних серверов (работающих благодаря трансляции сетевых адресов (NAT) в LAN), например, обслуживающих веб-сайты или FTP-сайты, которые можно сделать видимыми внешнему миру, несмотря на то, что NAT представляет всю внутреннюю сеть внешнему миру как один компьютер.

Вы можете ввести один номер порта или диапазон номеров портов, которые должны перенаправляться, и локальный IP-адрес нужного сервера. Номер порта идентифицирует сетевую службу; например, служба WWW функционирует на порту 80, а FTP – на порту 21. В некоторых случаях, например, если службы неизвестны или если один сервер может поддерживать несколько служб (и FTP, и WWW), более предпочтительным вариантом может быть указание диапазона номеров портов. Можно выделить IP-адрес сервера, который соответствует порту или диапазону портов.

Многие поставщики услуг Интернета, обслуживающие жилой сектор, запрещают своим пользователям запускать какие-либо серверные процессы (например, веб- или FTP-серверы). Поставщик услуг может периодически проверять наличие серверов у своих пользователей и приостанавливать действие учетной записи при выявлении активных сетевых служб. Для получения дополнительной информации следует обращаться к поставщику услуг Интернета.

7.4.1 IP-адрес сервера по умолчанию

В дополнение к серверам для заданных типов сетевых служб NAT поддерживает IP-адрес сервера по умолчанию. Сервер по умолчанию получает пакеты для портов, не указанных на этом экране.



Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-791R v2 будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.

7.4.2 Переадресация портов: сетевые службы и номера портов

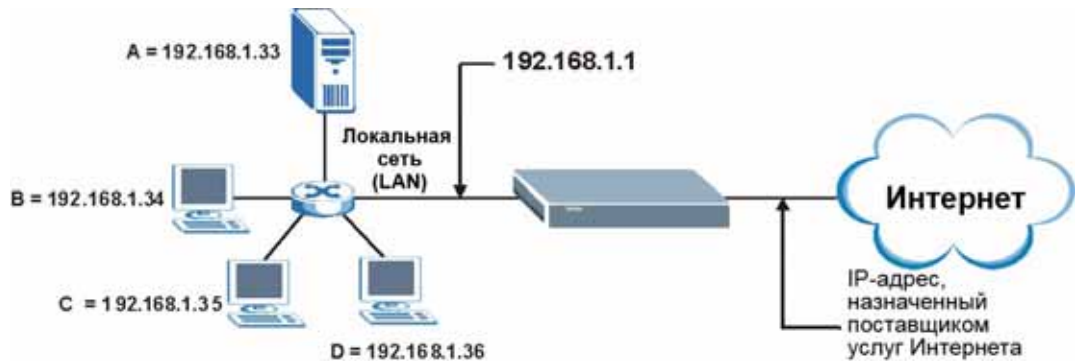
Экран **Port Forwarding** служит для переадресации входящих обращений к сетевым службам на серверы в локальной сети.

[Приложение F на стр. 341](#) содержит список распространенных номеров портов. Дополнительные сведения о номерах портов см. в документе RFC 1700.

7.4.3 Настройка серверов с переадресацией портов (пример)

Предположим, что порты в диапазоне 21-25 требуется присвоить одному серверу, обслуживающему FTP, Telnet и SMTP (обозначен буквой **A**), а порт 80 – другому серверу (обозначен буквой **B**). Также требуется присвоить IP-адрес сервера по умолчанию 192.168.1.35 третьему серверу (обозначен буквой **C**). Вы назначаете IP-адреса в локальной сети, а поставщик услуг Интернета – IP-адрес в глобальной сети. Сеть NAT представлена в Интернете как один хост.

Рис. 43 Пример нескольких серверов, закрытых функцией NAT



7.5 Настройка переадресации портов



Экран **Port Forwarding** доступен, если на экране **NAT > General** выбран параметр **SUA Only**, а также при редактировании набора привязки сервера в режиме **Full Feature NAT**.



Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-791R v2 будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.

Чтобы открыть следующий экран, выберите **Network > NAT > Port Forwarding**.

Номера портов для ряда распространенных сетевых служб см. в [Приложении F на стр. 341](#).

Рис. 44 Экран NAT > Port Forwarding

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 26 Экран NAT > Port Forwarding

ПОЛЕ	ОПИСАНИЕ
Default Server Setup	
Default Server	В дополнение к серверам для заданных типов сетевых служб NAT поддерживает сервер по умолчанию. Сервер по умолчанию получает пакеты для портов, не указанных на этом экране. Если IP-адрес сервера по умолчанию (Default Server) не указан, P-791R v2 будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.
Port Forwarding	
Service Name	Выберите тип сетевой службы для данного правила. Чтобы перейти на экран Rule Setup для задания собственных типов служб, выберите User define .
Server IP Address	Введите IP-адрес сервера для указанной сетевой службы.
Add	Нажмите эту кнопку, чтобы добавить правило в расположенную ниже таблицу.
#	В этом поле отображается порядковый номер правила (только для чтения).
Active	Отметьте этот флажок, чтобы активировать правило.
Service Name	В этом поле отображается название сетевой службы.
Start Port	В этом поле отображается первый номер порта, соответствующий данной службе.
End Port	В этом поле отображается последний номер порта, соответствующий данной службе.
Server IP Address	В этом поле отображается IP-адрес сервера.
Modify	Чтобы перейти на экран для редактирования правила переадресации портов, щелкните на значке редактирования. Для удаления существующего правила переадресации портов щелкните на значке удаления. При удалении одного правила все последующие правила смещаются вверх.
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Нажмите Cancel , чтобы вернуться к прежнему состоянию настроек.

7.5.1 Редактирование правил переадресации портов

Этот экран служит для редактирования правил переадресации портов. Щелкните на значке редактирования для соответствующего правила на экране **Port Forwarding**. Появится экран, показанный ниже.

Рис. 45 Экран NAT > Port Forwarding > Edit

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 27 Экран NAT > Port Forwarding > Edit

ПОЛЕ	ОПИСАНИЕ
Active	Отметьте этот флажок, чтобы активировать правило.
Service Name	Введите название для идентификации данного правила переадресации портов.
Start Port	Введите номер порта. Если переадресация требуется только для одного порта, введите его номер повторно в поле End Port . Чтобы включить переадресацию для диапазона портов, введите в данном поле номер первого порта, а в поле End Port – номер последнего порта.
End Port	Введите номер порта. Если переадресация требуется только для одного порта, в поле Start Port и в этом поле укажите один и тот же номер порта. Чтобы включить переадресацию для нескольких портов, введите номер последнего порта в диапазоне. Началом диапазона будет порт, введенный выше в поле Start Port .
Server IP Address	Здесь вводится внутренний IP-адрес сервера.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку Back .
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

7.6 Address Mapping



Экран **Address Mapping** доступен только в том случае, если на экране **NAT > General** был выбран параметр **Full Feature**.

Порядок следования правил имеет важное значение, поскольку P-791R v2 применяет правила в том порядке, в котором они определены. Когда правило соответствует текущему пакету, P-791R v2 выполняет соответствующее действие, и остальные правила игнорируются. Если перед настроенным правилом есть пустые правила, это созданное правило передвинется вверх на определенное число пустых правил. Например, если в текущем наборе правила 1 - 6 уже конфигурированы, а теперь ведется настройка правила номер 9. На экране с резюме набора правило будет правилом 7, а не 9. Если удалить правило 4, то правила 5 - 7 передвинутся вверх на 1 правило, поэтому старые правила 5, 6 и 7 станут новыми правилами 4, 5 и 6.

Этот экран позволяет изменить параметры DDNS в P-791R v2. Чтобы открыть следующий экран, выберите **Network > NAT > Address Mapping**.

Рис. 46 Экран NAT > Address Mapping

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	-	-	-	-	-	⊞ ⊞
2	-	-	-	-	-	⊞ ⊞
3	-	-	-	-	-	⊞ ⊞
4	-	-	-	-	-	⊞ ⊞
5	-	-	-	-	-	⊞ ⊞
6	-	-	-	-	-	⊞ ⊞
7	-	-	-	-	-	⊞ ⊞
8	-	-	-	-	-	⊞ ⊞
9	-	-	-	-	-	⊞ ⊞
10	-	-	-	-	-	⊞ ⊞

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 28 Экран NAT > Address Mapping

ПОЛЕ	ОПИСАНИЕ
#	В этом поле указан порядковый номер правила.
Local Start IP	Это начальный внутренний локальный адрес (ILA). Локальные IP-адреса недоступны (N/A) в режиме привязки Server .
Local End IP	Это конечный внутренний локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, в графе Local Start IP будет указан адрес 0.0.0.0, а в графе Local End IP – адрес 255.255.255.255. Это поле недоступно (N/A) для типов привязки One-to-One и Server .
Global Start IP	Это начальный внутренний глобальный IP-адрес (IGA). Если поставщик услуг Интернета предоставляет динамический IP-адрес, введите 0.0.0.0. Это возможно только при типах привязки Many-to-One и Server .
Global End IP	Это - конечный Внутренний глобальный IP-адрес (IGA). Это поле недоступно (N/A) для типов привязки One-to-one , Many-to-One и Server .

Таблица 28 Экран NAT > Address Mapping (продолжение)

ПОЛЕ	ОПИСАНИЕ
Type	<p>1-1: режим One-to-One (Один – один) привязывает один локальный IP-адрес к одному глобальному IP-адресу. Примечание: номера портов не изменяются для типа привязки NAT One-to-one (Один – один).</p> <p>M-1: режим "многие к одному" привязывает несколько локальных IP-адресов к одному глобальному IP-адресу. Этот режим эквивалентен однопользовательскому режиму SUA (фактически представляющему собой PAT – трансляцию адресов портов), который использовался в прежних маршрутизаторах ZyXEL.</p> <p>M-M Ov (с перегрузкой): режим "многие ко многим с перегрузкой" привязывает несколько локальных IP-адресов к совместно используемым глобальным IP-адресам.</p> <p>MM No (без перегрузки): режим "многие ко многим без перегрузки" привязывает каждый локальный IP-адрес к уникальным глобальным IP-адресам.</p> <p>Server: этот режим позволяет указывать внутренние серверы различных служб в NAT, которые должны быть доступными для внешнего мира.</p>
Modify	<p>Чтобы перейти на экран для редактирования правила привязки адресов, щелкните на значке редактирования.</p> <p>Для удаления существующего правила привязки адресов щелкните на значке удаления. При удалении одного правила все последующие правила смещаются вверх.</p>

7.6.1 Редактирование правила привязки адресов

Этот экран служит для редактирования правил привязки адресов. Щелкните на значке редактирования для соответствующего правила на экране **Address Mapping**. Появится экран, показанный ниже.

Рис. 47 Экран NAT > Address Mapping > Edit

The screenshot shows a configuration window titled "Edit Address Mapping Rule2". It contains the following fields and controls:

- Type**: A dropdown menu set to "One-to-One".
- Local Start IP**: A text input field containing "0.0.0.0".
- Local End IP**: A text input field containing "N/A".
- Global Start IP**: A text input field containing "0.0.0.0".
- Global End IP**: A text input field containing "N/A".
- Server Mapping Set**: A dropdown menu set to "N/A" with a blue "Edit Details" link next to it.
- At the bottom, there are three buttons: "Back", "Apply", and "Cancel".

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 29 Экран NAT > Address Mapping > Edit

ПОЛЕ	ОПИСАНИЕ
Type	<p>Выберите тип привязки порта из числа следующих вариантов.</p> <p>One-to-One: в режиме “один к одному” привязывает один локальный IP-адрес к одному глобальному IP-адресу. Примечание: номера портов не изменяются для типа привязки NAT One-to-one (Один – один).</p> <p>Many-to-One: режим “многие к одному” привязывает несколько локальных IP-адресов к одному глобальному IP-адресу. Этот режим эквивалентен однопользовательскому режиму SUA (фактически представляющему собой PAT – трансляцию адресов портов), который использовался в прежних маршрутизаторах ZyXEL.</p> <p>Many-to-Many Overload: режим “многие ко многим с перегрузкой” привязывает несколько локальных IP-адресов к совместно используемым глобальным IP-адресам.</p> <p>Many-to-Many No Overload: режим “многие ко многим без перегрузки” привязывает каждый локальный IP-адрес к уникальным глобальным IP-адресам.</p> <p>Server: этот режим позволяет указывать внутренние серверы различных служб в NAT, которые должны быть доступными для внешнего мира.</p>
Local Start IP	Это начальный локальный IP-адрес (ILA). Локальные IP-адреса недоступны (N/A) в режиме привязки Server .
Local End IP	<p>Это конечный локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, введите 0.0.0.0 в поле Local Start IP и 255.255.255.255 в поле Local End IP.</p> <p>Это поле недоступно (N/A) для типов привязки One-to-One и Server.</p>
Global Start IP	Это начальный глобальный IP-адрес (IGA). Если поставщик услуг Интернета предоставляет динамический IP-адрес, введите 0.0.0.0.
Global End IP	Это конечный глобальный IP-адрес (IGA). Это поле недоступно (N/A) для типов привязки One-to-One , Many-to-One и Server .
Server Mapping Set	<p>Этот параметр доступен только в том случае, если поле Type имеет значение Server.</p> <p>Чтобы выбрать новый набор привязки сервера, в раскрывающемся меню укажите его порядковый номер.</p>
Edit Details	Выберите эту ссылку, чтобы перейти на экран Port Forwarding (разд. 7.5 на стр. 105) для редактирования набора привязки сервера, выбранного в поле Server Mapping Set .
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку Back .
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

ЧАСТЬ III

Безопасность

Фильтр (113)

Фильтр

В этой главе описывается настройка фильтров Интернет-безопасности в P-791R v2.

8.1 Настройка фильтра

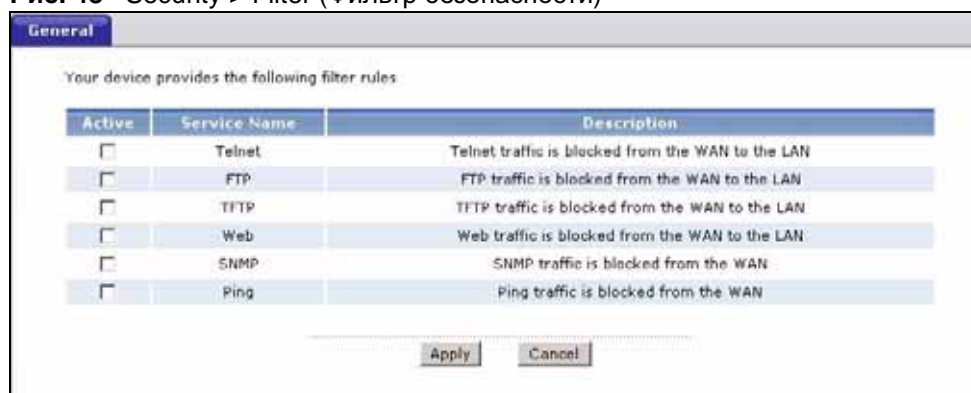
P-791R v2 может использовать предварительно настроенные фильтры для прекращения передачи пакетов определенных типов из WAN в LAN.



Если необходимо включить удаленное управление P-791R v2 из WAN, убедитесь, что параметры этого окна разрешают прохождение пакетов определенного типа из WAN.

Чтобы перейти на показанный ниже экран, на панели навигации выберите **Security > Filter (Фильтр безопасности)**.

Рис. 48 Security > Filter (Фильтр безопасности)



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 30 Защищенная реализация IP

ПОЛЕ	ОПИСАНИЕ
Telnet	Выберите этот параметр для прекращения передачи всех пакетов telnet из WAN в LAN. Трафик Telnet из LAN может по-прежнему проходить в WAN.
FTP	Выберите этот параметр для прекращения передачи всего трафика FTP из WAN в LAN. Трафик FTP из LAN может по-прежнему проходить в WAN.

Таблица 30 Защищенная реализация IP

ПОЛЕ	ОПИСАНИЕ
TFTP	Выберите этот параметр для прекращения передачи всего трафика TFTP из WAN в LAN. Трафик TFTP из LAN может по-прежнему проходить в WAN.
Web	Выберите этот параметр для прекращения передачи всего трафика HTTP из WAN в LAN.
SNMP	Выберите этот параметр для прекращения передачи всего трафика SNMP из WAN в P-791R v2. Трафик SNMP из LAN может по-прежнему входить в P-791R v2.
Ping	Выберите этот параметр для прекращения передачи всего трафика ICMP Echo из WAN в LAN.
Apply	Чтобы сохранить изменения, выберите Apply .
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

ЧАСТЬ IV

Расширенная настройка

Статическая маршрутизация (117)

Настройка DNS для динамических адресов (121)

Настройка удаленного управления (125)

Универсальная технология “включи и работай” (UPnP) (135)

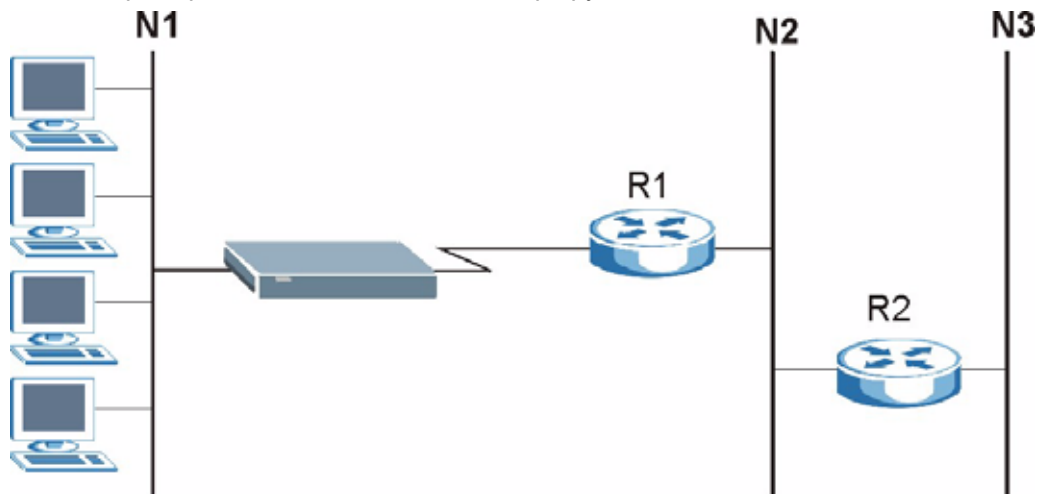
Статическая маршрутизация

В этой главе описывается настройка статических маршрутов для P-791R v2.

9.1 Статический маршрут

Каждый удаленный узел определяет только ту сеть, к которой непосредственно подключен маршрутизатор, и P-791R v2 не имеет информации о сетях, расположенных за ее пределами. Например, на следующем рисунке P-791R v2 получает сведения о сети N2 через удаленный маршрутизатор R1. Однако P-791R v2 не имеет возможности отправить пакет в сеть N3, поскольку ему неизвестно о существовании маршрута через удаленный маршрутизатор R1 (и далее через R2). Статические маршруты позволяют сообщать P-791R v2 о сетях, находящихся за пределами удаленных узлов.

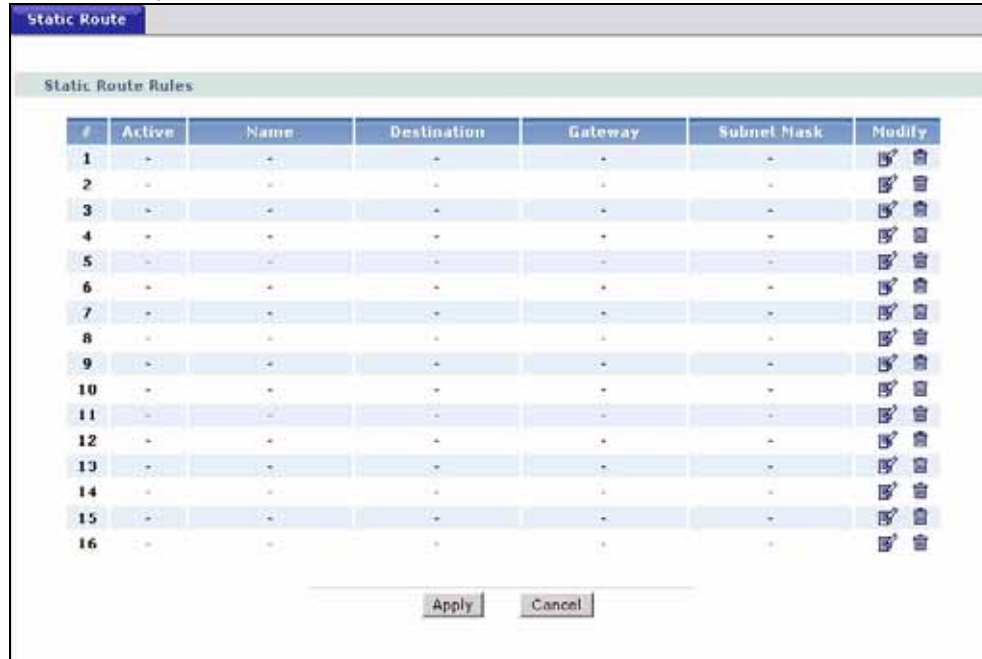
Рис. 49 Пример топологии статической маршрутизации



9.2 Настройка статических маршрутов

Этот экран служит для просмотра статических маршрутов в P-791R v2. Чтобы перейти на экран **Static Route**, выберите **Advanced > Static Route**.

Рис. 50 Экран Static Route > Static Route



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 31 Экран Static Route > Static Route

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается номер статического маршрута.
Active	Это поле показывает, активен ли данный статический маршрут: Yes (Да) или No (Нет) .
Name	В этом поле выводится описание или идентификация данного маршрута.
Destination	Этот параметр указывает IP-адрес конечной точки маршрута. Маршрутизация всегда подразумевает диапазон сетевых адресов.
Gateway	Это – IP-адрес шлюза. Шлюз - это маршрутизатор или коммутатор, расположенный в одном сегменте с LAN- или WAN-портом устройства. Шлюз пересылает пакеты к месту назначения.
Subnet Mask	В этом поле отображается маска подсети статического маршрута.
Modify	Чтобы перейти на экран задания статических маршрутов для P-791R v2, щелкните на значке редактирования. Щелкните на значке удаления, чтобы удалить статический маршрут из P-791R v2. Появится окно с просьбой подтвердить удаление маршрута.
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

9.2.1 Редактирование статического маршрута

Выберите номер индекса статического маршрута и щелкните команду **Edit**. Появляется экран, показанный ниже. На этом экране указываются все необходимые сведения для настройки статического маршрута.

Рис. 51 Экран Static Route > Static Route > Edit

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 32 Экран Static Route > Static Route > Edit

ПОЛЕ	ОПИСАНИЕ
Active	Это поле позволяет активировать/деактивировать данный статический маршрут.
Route Name	Введите имя статического IP-маршрута. Для удаления данного статического маршрута оставьте это поле пустым.
Destination IP Address	Этот параметр указывает IP-адрес конечной точки маршрута. Маршрутизация всегда подразумевает диапазон сетевых адресов. Если требуется указать маршрут до отдельного хоста, в поле "IP Subnet Mask" введите маску подсети 255.255.255.255 – при этом диапазон сетевых адресов будет ограничен до адреса хоста.
IP Subnet Mask	Введите маску подсети IP.
Gateway IP Address	Введите IP-адрес интернет-центра. Шлюз - это маршрутизатор или коммутатор, расположенный в одном сегменте с LAN- или WAN-портом устройства. Шлюз пересылает пакеты к месту назначения.
Back	Для возврата к предыдущему экрану без сохранения настроек нажмите кнопку Back .
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

Настройка DNS для динамических адресов

В этой главе поясняется способ настройки DNS для динамических адресов в P-791R v2.

10.1 Обзор поддержки DNS для динамических адресов

Поддержка DNS для динамических адресов постоянно перенастраивает один или несколько серверов DNS на ваш текущий динамический адрес, позволяя любому пользователю находить вашу систему (в NetMeeting, CU-SeeMe и т.д.). Доступ к FTP-серверу или веб-сайту на собственном компьютере можно получить с использованием доменного имени (например, myhost.dhs.org, где myhost – выбранное имя), которое никогда не будет изменяться, вместо использования IP-адреса, который изменяется при каждом новом подключении. Друзья или родственники всегда смогут вас найти, даже если не будут знать ваш IP-адрес.

Прежде всего, необходимо зарегистрировать динамическую учетную запись DNS на www.dyndns.org. Этот сервис предназначен для пользователей с динамическим IP (получаемым от поставщика услуг Интернета или через сервер DHCP), которым требуется иметь доменное имя. Пароль или ключ будет предоставлен оператором динамической DNS.

10.1.1 Шаблон DYNDNS

Включение функции шаблона (wildcard) для вашего хоста разрешает использовать любые адреса *.ваш_хост.dyndns.org, которые преобразуются в тот же IP-адрес, что и ваш_хост.dyndns.org. Эта функция полезна тем, что позволяет обращаться к вашему хосту по таким адресам, как www.ваш_хост.dyndns.org.

При наличии частного IP-адреса в глобальной сети динамическую DNS использовать нельзя.

Указания по настройке см. в [разд. 10.2 на стр. 121](#).

10.2 Настройка динамической DNS

Этот экран позволяет изменить параметры DDNS в P-791R v2. Выберите **Advanced > Dynamic DNS**. Появится изображенный ниже экран.

Дополнительные сведения см. в [разд. 10.1 на стр. 121](#).

Рис. 52 Экран Dynamic DNS > Dynamic DNS

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 33 Экран Dynamic DNS > Dynamic DNS

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS Setup	
Active Dynamic DNS	Установите этот флажок, чтобы использовать динамическую DNS.
Service Provider	Это название поставщика услуг динамической DNS.
Dynamic DNS Type	Выберите тип услуги, зарегистрированной у поставщика услуг DDNS.
Host Name	Введите доменное имя, присвоенное вашему P-791R v2 поставщиком услуг DDNS. В каждом поле можно указать до двух имен хостов, отделенных запятыми.
User Name	Введите имя пользователя.
Password	Введите присвоенный вам пароль.
Enable Wildcard Option	Чтобы активировать шаблон DynDNS, отметьте флажок.
Enable off line option	Это поле доступно только в том случае, если в поле DDNS Type выбрано значение Custom DNS . Узнайте у поставщика услуг динамической DNS о возможности переадресации трафика на указанный вами URL в то время, когда вы не подключены к сети.
IP Address Update Policy	
Use WAN IP Address	Выберите этот параметр, чтобы использовать для обновления IP-адресов указанных имен хостов IP-адрес со стороны WAN.

Таблица 33 Экран Dynamic DNS > Dynamic DNS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS server auto detect IP Address	<p>Этот параметр следует выбирать только в том случае, если между P-791R v2 и сервером DDNS присутствуют один или несколько маршрутизаторов с поддержкой NAT. Эта функция указывает DDNS-серверу автоматически определять и использовать IP-адрес NAT-маршрутизатора, имеющего глобальный IP-адрес.</p> <p>Примечание. DDNS-сервер может неверно определить IP-адрес, если между P-791R v2 и DDNS-сервером присутствует прокси-сервер HTTP.</p>
Use specified IP Address	Введите IP-адреса для имен хостов. Используйте эту функцию, если вам выделен статический IP-адрес.
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

Настройка удаленного управления

В этой главе содержится информация о настройке удаленного управления.

11.1 Обзор удаленного управления

Удаленное управление позволяет определять, какие службы/протоколы могут получать доступ к определенному интерфейсу P-791R v2 (если это возможно) и с каких компьютеров.

Устройством P-791R v2 можно управлять удаленно через:

- Интернет (только WAN)
- ВСЕ сети (LAN и WAN)
- Только LAN
- Ни одну из сетей (удаленное управление отключено).

Для отключения удаленного управления через одну из служб выберите **Disable** в соответствующем поле **Access Status**.

В каждый момент времени может выполняться только один сеанс удаленного управления. P-791R v2 автоматически разъединяет менее приоритетный сеанс удаленного управления, когда начинается выполнение другого сеанса удаленного управления с более высоким приоритетом. Существуют следующие приоритеты для различных типов сеансов удаленного управления.

- 1 Telnet
- 2 HTTP

11.1.1 Ограничения удаленного управления

Удаленное управление через LAN или WAN не работает в следующих случаях:

- Пользователь отключил данную службу на одном из экранов удаленного управления.
- IP-адрес в поле **Secured Client IP** не соответствует IP-адресу клиента. При таком несоответствии P-791R v2 немедленно прерывает сеанс.
- Уже выполняется другой сеанс удаленного управления с равным или более высоким приоритетом. В каждый момент времени может выполняться только один сеанс удаленного управления.

11.1.2 Удаленное управление и NAT

При включенной системе NAT:

- Если настройка выполняется через WAN, укажите IP-адрес P-791R v2 на стороне WAN.
- Если настройка выполняется через LAN, укажите IP-адрес P-791R v2 на стороне LAN.

11.1.3 Системный таймер неактивности

Для управления системой установлен интервал неактивности. P-791R v2 автоматически отменяет регистрацию пользователя, если сеанс управления остается бездействующим дольше этого периода времени ожидания. Сеанс управления не прерывается при выполнении опроса на экране статистики. По умолчанию он равен пяти минутам. Настройка этого интервала и запрет разъединения по неактивности описаны в [разд. 13.1.2 на стр. 149](#).

11.2 WWW

Этот параметр позволяет настроить параметры веб-интерфейса для удаленного управления P-791R v2. Чтобы перейти на экран **WWW**, выберите **Advanced > Remote MGMT**.

Рис. 53 Экран Remote MGMT > WWW

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 34 Экран Remote MGMT > WWW

ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-791R v2 с использованием данной службы.
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается обмениваться данными с P-791R v2, используя эту службу. Выберите All , чтобы разрешить любому компьютеру получать доступ к P-791R v2 посредством этой службы. Выберите Selected , чтобы доступ к P-791R v2 посредством данной службы был разрешен только компьютеру с указанным IP-адресом.

Таблица 34 Экран Remote MGMT > WWW (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

11.3 Telnet

P-791R v2 можно настроить для удаленного доступа по Telnet, как показано ниже. Администратор использует Telnet с компьютера в удаленной сети для получения доступа к P-791R v2.

Рис. 54 Настройка Telnet в сети TCP/IP

11.4 Настройка Telnet

Дополнительные сведения см. в [разд. 11.1 на стр. 125](#). Этот экран служит для настройки доступа по Telnet к P-791R v2. Чтобы перейти на показанный ниже экран, выберите **Advanced > Remote MGMT > вкладка Telnet**.

Рис. 55 Экран Remote MGMT > Telnet

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 35 Экран Remote MGMT > Telnet

ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-791R v2 с использованием данной службы.

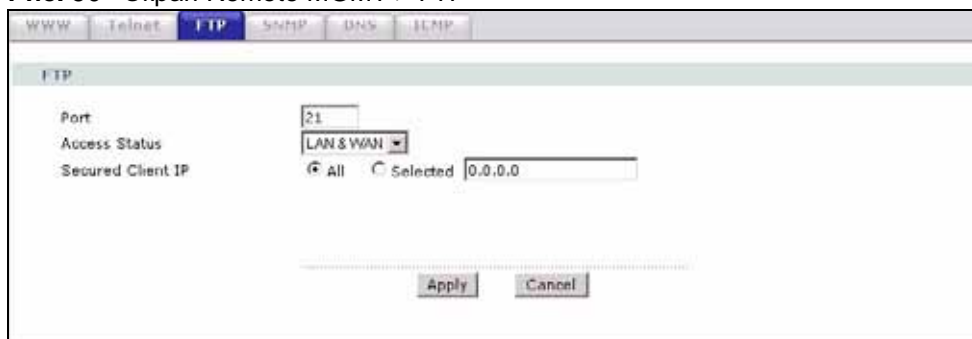
Таблица 35 Экран Remote MGMT > Telnet (продолжение)

ПОЛЕ	ОПИСАНИЕ
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается обмениваться данными с P-791R v2, используя эту службу. Выберите All , чтобы разрешить любому компьютеру получать доступ к P-791R v2 посредством этой службы. Выберите Selected , чтобы доступ к P-791R v2 посредством данной службы был разрешен только компьютеру с указанным IP- адресом.
Apply	Нажмите кнопку Apply для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

11.5 Настройка FTP

По протоколу FTP можно загружать в P-791R v2 файлы микропрограмм и настроек. Подробности см. в главе о работе с файлом настроек. Для использования этой возможности ваш компьютер должен иметь FTP-клиента.

Дополнительные сведения см. в [разд. 11.1 на стр. 125](#). Этот экран служит для управления доступом к P-791R v2 по FTP. Чтобы изменить параметры FTP для P-791R v2, выберите **Advanced > Remote MGMT >** закладка **FTP**. Появится изображенный ниже экран.

Рис. 56 Экран Remote MGMT > FTP

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 36 Экран Remote MGMT > FTP

ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-791R v2 с использованием данной службы.
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается обмениваться данными с P-791R v2, используя эту службу. Выберите All , чтобы разрешить любому компьютеру получать доступ к P-791R v2 посредством этой службы. Выберите Selected , чтобы доступ к P-791R v2 посредством данной службы был разрешен только компьютеру с указанным IP- адресом.
Apply	Нажмите кнопку Apply для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

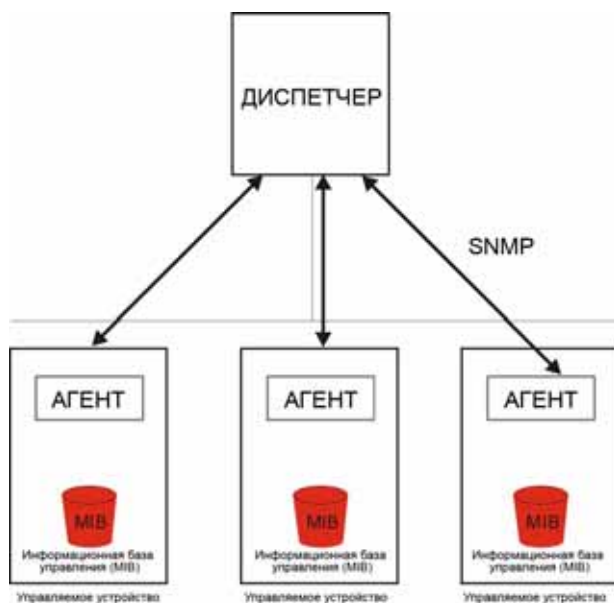
11.6 SNMP

Протокол SNMP (Simple Network Management Protocol - упрощенный протокол управления сетью) используется для обмена управляющей информацией между сетевыми устройствами. SNMP входит в семейство протоколов TCP/IP. P-791R v2 поддерживает функциональные возможности агента SNMP, что позволяет управляющей станции выполнять управление и мониторинг P-791R v2 через сеть. P-791R v2 поддерживает первую (SNMPv1) и вторую (SNMPv2) версии протокола SNMP. На следующем рисунке показана схема управления на основе SNMP.



SNMP доступен только в том случае, если настроены параметры TCP/IP.

Рис. 57 Модель управления по протоколу SNMP



Сеть с управлением через SNMP состоит из двух основных типов компонентов: агентов и диспетчера.

Агент – это программа, которая выполняется на управляемом устройстве (P-791R v2). Агент преобразует локальные параметры управления, используемые в управляемом устройстве, в формат, совместимый с SNMP. Менеджер – это консоль, через которую администратор сети управляет устройствами. Диспетчер выполняет ПО для управления и мониторинга управляемых устройств.

Управляемые устройства содержат объекты-переменные или управляемые объекты, характеризующие все виды сведений, которые можно получить об устройстве. Примерами таких переменных являются: число полученных пакетов, состояние портов узла и т.д. Информационная база управления (МИБ) представляет собой набор управляемых объектов. SNMP позволяет диспетчеру и агентам совместно получать доступ к этим объектам.

Сам SNMP представляет собой простой протокол вида “запрос–отклик”, построенный на модели “диспетчер–агент”. Направление запросов диспетчером и возвращение откликов агентом осуществляется с помощью следующих операций протокола:

- Get (“получить”) - позволяет диспетчеру запросить объект-переменную у агента.
- GetNext (“получить следующую“) - позволяет диспетчеру получать из принадлежащей агенту таблицы (или списка) следующую переменную объекта. В SNMPv1, если диспетчеру требуется получить от агента все элементы таблицы, он инициирует операцию Get, вслед за которой выполняет несколько операций GetNext.
- Set (“задать“) - позволяет диспетчеру задать значения для объектов-переменных агента.
- Trap (“прерывание“) - используется агентом для информирования диспетчера об определенных событиях.

11.6.1 Поддерживаемые базы MIB

P-791R v2 поддерживает базу MIB II, которая определена в RFC-1213 и RFC-1215. Основная задача баз MIB – дать администраторам возможность сбора статистических данных и мониторинга состояния и производительности.

11.6.2 Прерывания SNMP

P-791R v2 направляет прерывания диспетчеру SNMP при наступлении одного из следующих событий.

Таблица 37 Прерывания SNMPv1

ПРЕ-РЫВАНИЕ ‡,	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
0	coldStart (определяется в <i>RFC-1215</i>)	Прерывание отправляется после загрузки (включения питания).
1	warmStart (определяется в <i>RFC-1215</i>)	Прерывание отправляется после загрузки (программной перезагрузки).
6	whyReboot (определяется в ZYXEL-MIB)	Прерывание направляется по причине перезапуска перед перезагрузкой, когда система готовится к перезапуску (“теплая перезагрузка”).
6a	Для перезагрузки, запрошенной пользователем	Прерывание отправляется с сообщением “Перезагрузка системы пользователем!”, если перезагрузка выполняется по явному запросу, (например, после загрузки новых файлов, получения команды СI “перезагрузка системы” и т.д.).
6b	Из-за неустранимой ошибки	Прерывание отправляется с сообщением о превышенном коде, если система перезагружается из-за неустранимых ошибок.

Таблица 38 Прерывания SNMPv2

НАЗВАНИЕ ОБЪЕКТА	КОД ОБЪЕКТА	ОПИСАНИЕ
Прерывания SNMPv2		
Холодный запуск	1.3.6.1.6.3.1.1.5.1	Это прерывание отправляется при включении коммутатора.
Горячий запуск	1.3.6.1.6.3.1.1.5.2	Это прерывание направляется при перезагрузке коммутатора.
Разрыв связи	1.3.6.1.6.3.1.1.5.3	Это сообщение отправляется при исчезновении Ethernet-связи.
linkUp	1.3.6.1.6.3.1.1.5.4	Это сообщение отправляется при установлении Ethernet-соединения.

11.6.3 Настройка SNMP

Дополнительные сведения см. в [разд. 11.1 на стр. 125](#). Этот экран позволяет изменить настройки SNMP в P-791R v2. Выберите **Advanced > Remote MGMT > SNMP**. Появится изображенный ниже экран.

Рис. 58 Экран Remote MGMT > SNMP

The screenshot shows the SNMP configuration page. At the top, there are navigation tabs: WWW, Telnet, FTP, **SNMP**, DNS, and ICMP. Below the tabs, the page title is 'SNMP'. The configuration fields are as follows:

- Port:** 161
- Access Status:** LAN & WAN (dropdown menu)
- Secured Client IP:** All, Selected (0.0.0.0)
- SNMP Configuration:**
 - Get Community:** public
 - Set Community:** public
 - Trap Community:** public
 - Trap Destination:** 0.0.0.0

At the bottom, there is a note: "Note: You may also need to create a [Firewallrule](#)". Below the note are 'Apply' and 'Cancel' buttons.

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 39 Экран Remote MGMT > SNMP

ПОЛЕ	ОПИСАНИЕ
SNMP	
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-791R v2 с использованием данной службы.
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается обмениваться данными с P-791R v2, используя эту службу. Выберите All , чтобы разрешить любому компьютеру получать доступ к P-791R v2 посредством этой службы. Выберите Selected , чтобы доступ к P-791R v2 посредством данной службы был разрешен только компьютеру с указанным IP- адресом.

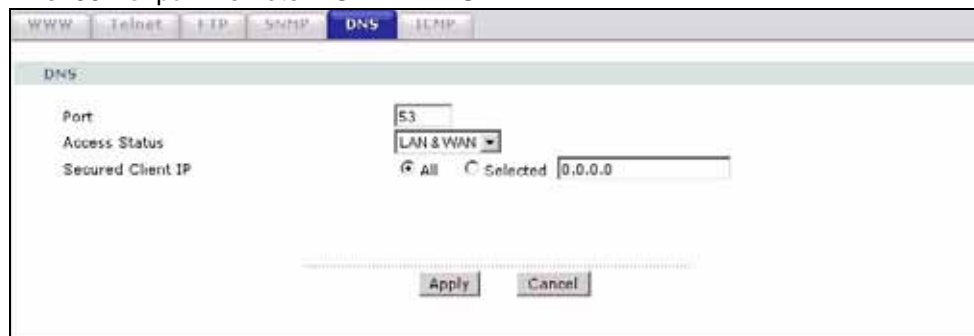
Таблица 39 Экран Remote MGMT > SNMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
SNMP Configuration	
Get Community	Введите Get Community ("получить сообщество") – пароль для всех входящих запросов Get и GetNext от диспетчерской станции. Значение по умолчанию – "общедоступно", все запросы разрешены.
Set Community	Введите Set community ("задать сообщество") – пароль для входящих запросов Set от диспетчерской станции. Значение по умолчанию – "общедоступно", все запросы разрешены.
Trap Community	Введите сообщество для прерываний, которое будет выступать в качестве пароля при отправке прерываний диспетчеру SNMP. Значение по умолчанию – "общедоступно", все запросы разрешены.
Trap Destination	Введите IP-адрес станции, которой следует направлять прерывания SNMP.
Apply	Нажмите кнопку Apply для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

11.7 Настройка DNS

DNS (служба доменных имён) обеспечивает преобразование доменных имён в соответствующие им IP-адреса и наоборот. Краткий обзор приведен в главе, посвященной LAN.

Дополнительные сведения см. в [разд. 11.1 на стр. 125](#). Выберите **Advanced > Remote MGMT > DNS**. Появится изображенный ниже экран. Этот экран позволяет задать IP-адреса, от которых P-791R v2 будет принимать DNS-запросы, и указать интерфейс, через который P-791R v2 будет рассылать параметры DNS на эти адреса.

Рис. 59 Экран Remote MGMT > DNS

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 40 Экран Remote MGMT > DNS

ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может отправлять запросы DNS на P-791R v2.

Таблица 40 Экран Remote MGMT > DNS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается отправлять запросы DNS на P-791R v2. Выберите переключатель All , чтобы разрешить любому компьютеру отправлять запросы DNS на P-791R v2. Выберите переключатель Selected , чтобы разрешить только компьютеру с указанным IP-адресом отправлять запросы DNS на P-791R v2.
Apply	Нажмите кнопку Apply для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

11.8 Настройка ICMP

Этот экран определяет режим обработки других видов запросов в P-791R v2. Выберите **Advanced > Remote MGMT > ICMP**. Появится изображенный ниже экран.

Если внешний пользователь попытается зондировать неподдерживаемый порт P-791R v2, автоматически будет возвращен пакет с откликом ICMP (протокол управляющих сообщений в Интернете). Это позволяет внешнему пользователю узнать о том, что P-791R v2 существует. P-791R v2 предусматривает защиту от зондирования, отключающую отправку пакета с откликом ICMP. Это препятствует обнаружению P-791R v2 посторонними при зондировании неподдерживаемых портов.

Рис. 60 Экран Remote MGMT > ICMP

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 41 Экран Remote MGMT > ICMP

ПОЛЕ	ОПИСАНИЕ
ICMP	Internet Control Message Protocol (межсетевой протокол управляющих сообщений) является протоколом управления сообщениями и предоставления отчетов об ошибках при взаимодействии между сервером хоста и шлюзом. В ICMP используются датаграммы меж сетевого протокола (IP), но сообщения обрабатываются программным обеспечением TCP/IP и отображаются в понятном виде для пользователя приложения.
Respond to Ping on	Если выбрано значение Disable , P-791R v2 не будет реагировать на входящие запросы. Выберите LAN , чтобы разрешить ответ на поступающие через локальную сеть эхозапросы. Выберите WAN , чтобы разрешить ответ на эхозапросы из WAN. В противном случае выберите LAN & WAN для передачи ответов на поступающие эхозапросы LAN и WAN.
Apply	Нажмите кнопку Apply для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

Универсальная технология “включи и работай” (UPnP)

В этом разделе описываются функции веб-конфигуратора, связанные с UPnP.

12.1 Обзор технологии UPnP

Универсальная система "включай и работай" (UPnP) является открытым сетевым стандартом для распределенной работы, в котором используется TCP/IP для простого однорангового сетевого соединения между устройствами. Устройство UPnP может динамически присоединяться к сети, получать IP-адрес, сообщать свои возможности и получать данные о других устройствах в сети. А когда в устройстве больше нет необходимости, оно может беспрепятственно покинуть сеть в автоматическом режиме.

Указания по настройке см. в [разд. 12.2.1 на стр. 136](#).

12.1.1 Как определить, используется ли UPnP?

Оборудование UPnP идентифицируется с помощью значка в папке Network Connections (Сетевые подключения) (Windows XP). Каждое UPnP-совместимое устройство, установленное в сети, обозначается отдельным значком. Выбор значка UPnP-устройства позволяет получать доступ к информации и свойствам этого устройства.

12.1.2 Прослеживание NAT

Прослеживание NAT UPnP автоматизирует процесс получения приложением разрешения на работу через NAT. Сетевые UPnP-устройства могут автоматически конфигурировать сетевую адресацию, объявлять о своем присутствии в сети другим UPnP-устройствам и обеспечивать обмен простыми описаниями продуктов и услуг. Прослеживание NAT обеспечивает:

- Динамическую привязку портов
- Получение данных об общедоступных IP-адресах
- Назначение сроков действия привязок

Мессенджер Windows - пример приложения, поддерживающего прослеживание NAT и UPnP.

Дополнительную информацию о NAT см. в главе, посвященной NAT.

12.1.3 Предостережения по отношению к UPnP

Автоматическое функционирование приложений для прослеживания NAT, устанавливающих собственные службы, может представлять угрозу для систем безопасности сетей. Кроме того, пользователи могут получать и изменять данные и конфигурации в некоторых сетевых средах.

Подключаясь к сети, UPnP-устройство объявляет о своем присутствии многоадресным сообщением. По соображениям безопасности P-791R v2 допускает передачу многоадресных сообщений только в сети LAN.

Все устройства с поддержкой UPnP могут свободно взаимодействовать друг с другом, для чего не требуется дополнительная настройка. Если этого не следует допускать, отключите UPnP.

12.2 UPnP и ZyXEL

Корпорация ZyXEL получила сертификат на UPnP от UIC (Universal Plug and Play Forum UPnP™ Implementers Corp. – объединение поставщиков, использующих универсальную технологию "включай и работай" – UPnP™). Реализация UPnP в оборудовании ZyXEL поддерживает спецификацию аппаратных Интернет-шлюзов IGD 1.0.

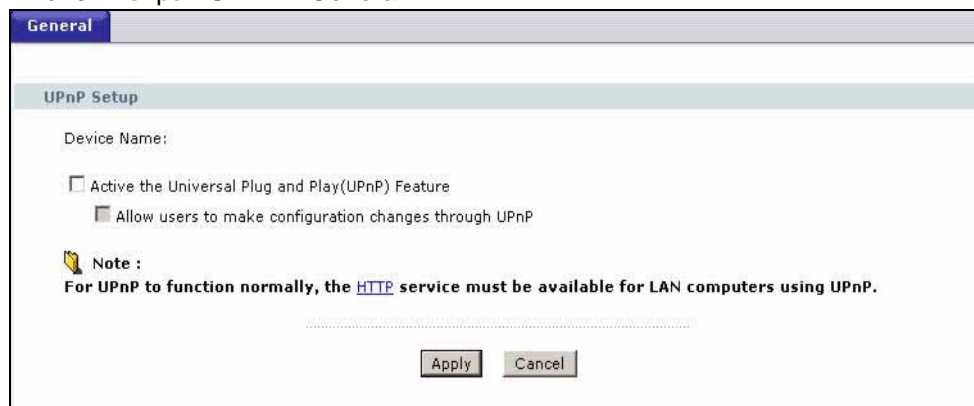
В следующих разделах рассмотрены примеры установки и использования UPnP.

12.2.1 Настройка UPnP

Этот экран служит для настройки UPnP в P-791R v2. Чтобы перейти на показанный ниже экран, выберите **Advanced > UPnP**.

Дополнительные сведения см. в [разд. 12.1 на стр. 135](#).

Рис. 61 Экран UPnP > General



Поля изображённого выше экрана описаны в следующей таблице.

Таблица 42 Экран UPnP > General

ПОЛЕ	ОПИСАНИЕ
Active the Universal Plug and Play (UPnP) Feature	Отметьте этот флажок, чтобы активировать UPnP. Помните, что любой пользователь сможет посредством приложения UPnP перейти на экран регистрации веб-конфигуратора, не вводя IP-адрес P-791R v2 (хотя для доступа к веб-конфигуратору по-прежнему потребуется вводить имя пользователя и пароль).
Allow users to make configuration changes through UPnP	Установите этот флажок, чтобы разрешить приложениям с поддержкой UPnP автоматически конфигурировать P-791R v2 так, чтобы они могли взаимодействовать через P-791R v2; например, используя прослеживание NAT, приложения UPnP автоматически резервируют порт для адресации NAT, чтобы взаимодействовать с другим устройством с поддержкой UPnP; это устраняет необходимость ручной настройки переадресации портов для приложения с поддержкой UPnP.
Apply	Нажмите кнопку Apply , чтобы сохранить настройки в P-791R v2.
Cancel	Чтобы вернуться к прежним настройкам, нажмите Cancel .

12.3 Пример установки UPnP в Windows

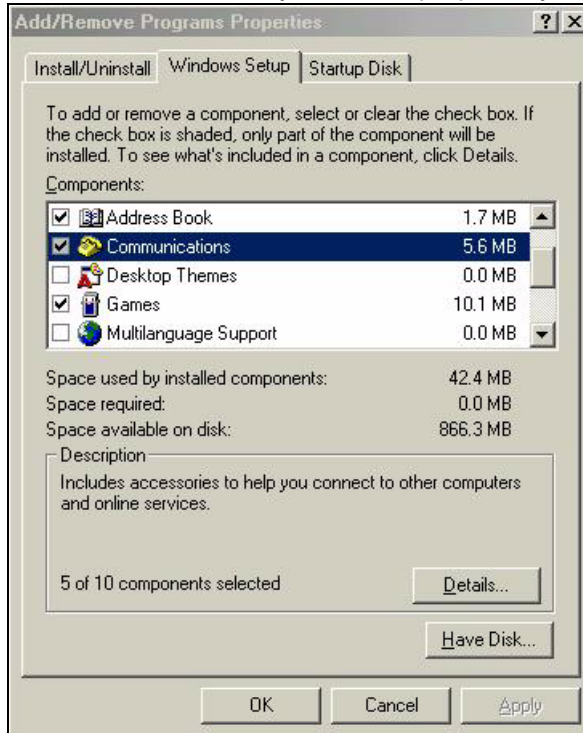
В этом разделе описана установка системы UPnP в Windows Me и Windows XP.

Установка UPnP в Windows Me

Для установки UPnP в Windows Me выполните указанные ниже действия.

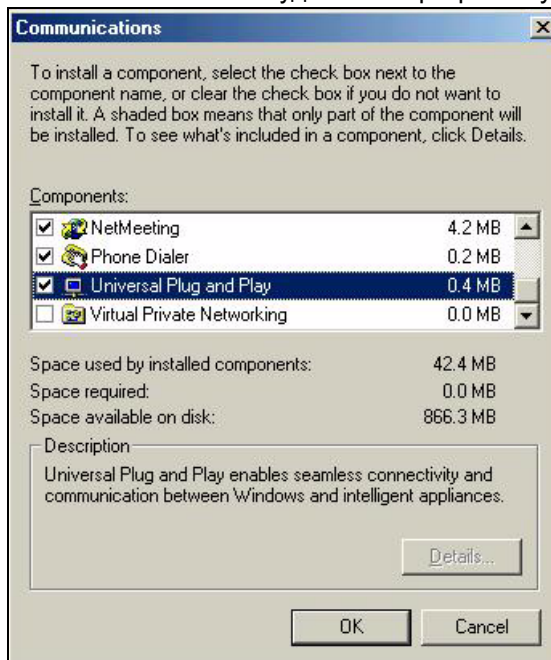
- 1 Нажмите кнопку **Start (Пуск)** и выберите **Control Panel (Панель управления)**. Выполните двойной щелчок на значке **Add/Remove Programs (Установка и удаление программ)**.
- 2 Щелкните вкладку **Windows Setup (Установка Windows)** и выберите строку **Communication (Связь)** в поле выбора **Components (Компоненты)**. Щелкните кнопку **Details (Состав)**.

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



3 В окне **Communications (Связь)** выберите флажок **Universal Plug and Play (Универсальная система "включай и работай")** в рамке выбора **Components (Компоненты)**.

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



4 Нажмите кнопку **ОК** для возвращения в окно **Add/Remove Programs Properties (Свойства установки и удаления программ)** и нажмите кнопку **Next (Далее)**.

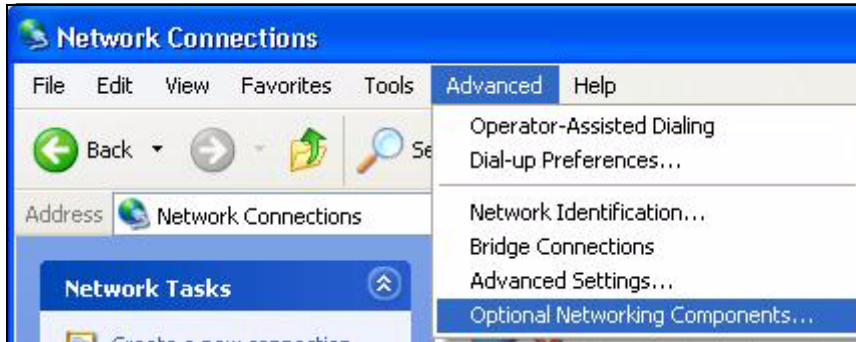
5 Перезапустите компьютер, когда это будет предложено.

Установка UPnP в Windows XP

Для установки UPnP в Windows XP выполните указанные ниже действия.

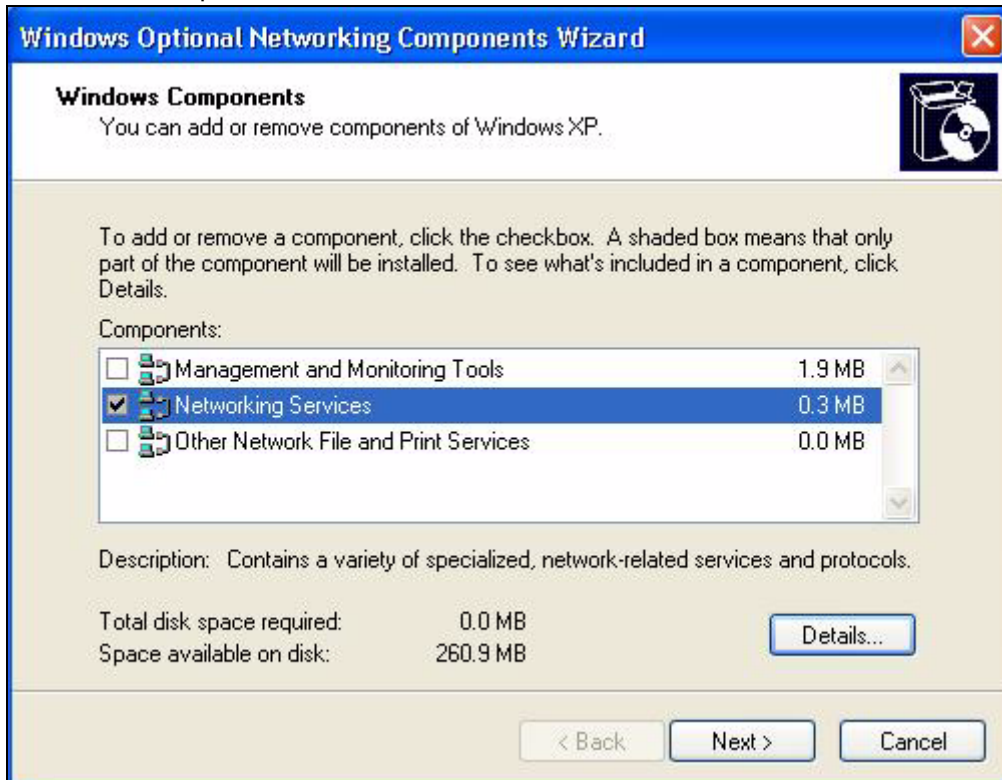
- 1 Нажмите кнопку **Start (Пуск)** и выберите **Control Panel (Панель управления)**.
- 2 Дважды щелкните на значке **Network Connections (Сетевые подключения)**.
- 3 В окне **Network Connections (Сетевые подключения)** щелкните кнопку **Advanced (Дополнительно)** в главном меню и выберите пункт **Optional Networking Components с (Дополнительные сетевые компоненты)**.

Рис. 64 Сетевые подключения



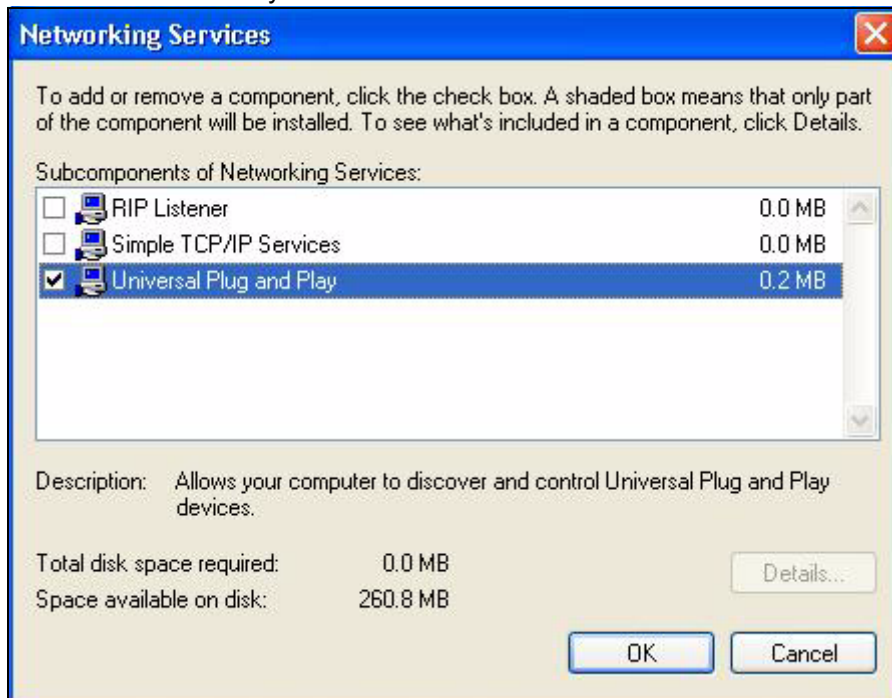
- 4 Появится окно **Windows Optional Networking Components Wizard (Мастер дополнительных сетевых компонентов Windows)**. Выберите **Networking Service (Сетевые службы)** в окне выбора **Components (Компоненты)** и щелкните кнопку **Details (Состав)**.

Рис. 65 Мастер дополнительных сетевых компонентов Windows



- 5 В окне **Networking Services (Сетевые службы)** установите флажок **Universal Plug and Play (Универсальная технология "включай и работай")**.

Рис. 66 Сетевые службы



- 6 Щелкните **ОК** для возвращения в окно **Windows Optional Networking Component Wizard (Мастер дополнительных сетевых компонентов Windows)** и кнопку **Next (Далее)**.

12.4 Пример использования UPnP в Windows XP

В данном разделе описано использование функции UPnP в Windows XP. Система UPnP уже должна быть установлена в Windows XP и активирована в P-791R v2.

Убедитесь в том, что компьютер подключен к порту LAN на P-791R v2. Включите компьютер и P-791R v2.

Автоматическое обнаружение сетевого устройства с поддержкой UPnP

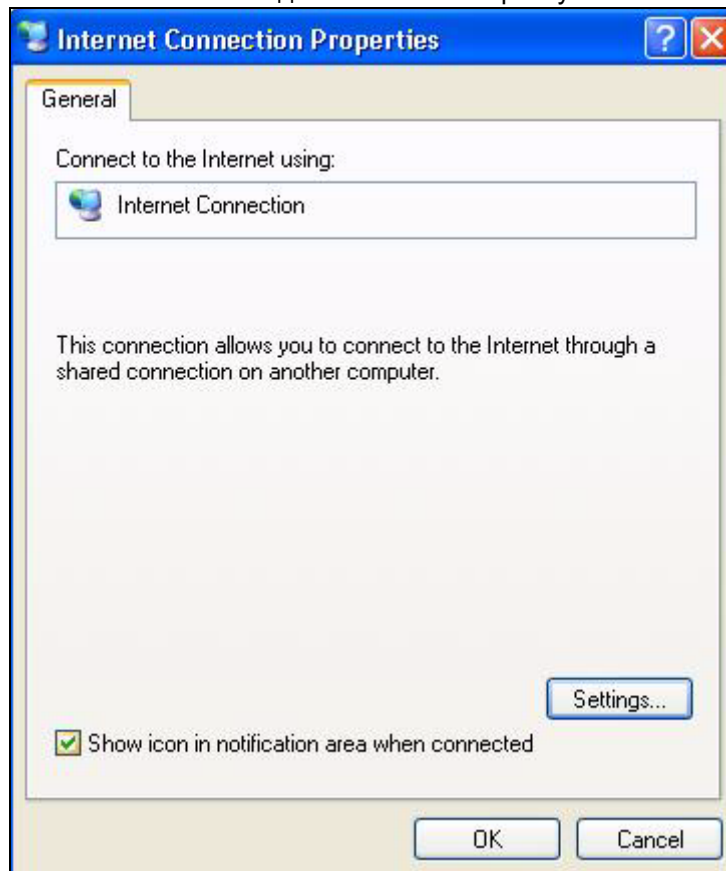
- 1 Нажмите кнопку **Start (Пуск)** и выберите **Control Panel (Панель управления)**. Дважды щелкните на значке **Network Connections (Сетевые подключения)**. Значок отображается под Internet Gateway (шлюзом).
- 2 Щелкните правой кнопкой мыши по этому значку и выберите **Properties (Свойства)**.

Рис. 67 Сетевые подключения



- 3 В окне **Internet Connection Properties (Свойства подключения к Интернету)** нажмите команду **Settings (Параметры)**, чтобы увидеть привязки к порту, которые были созданы автоматически.

Рис. 68 Свойства подключения к Интернету



- 4 Можно отредактировать или удалить привязки порта или щелкнуть **Add** (**Добавить**) для добавления привязок порта вручную.

Рис. 69 Свойства подключения к Интернету: дополнительные параметры

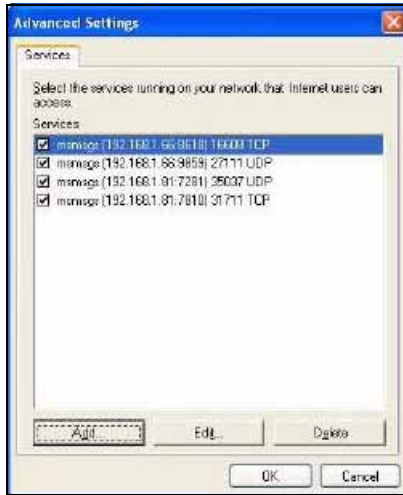
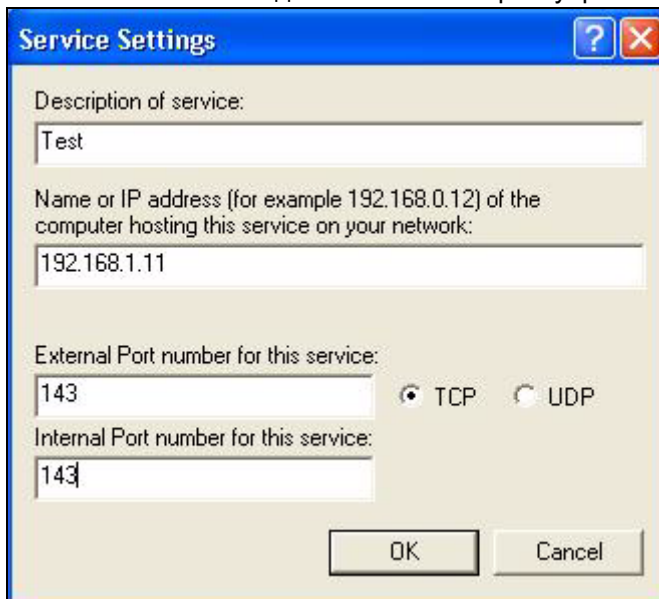
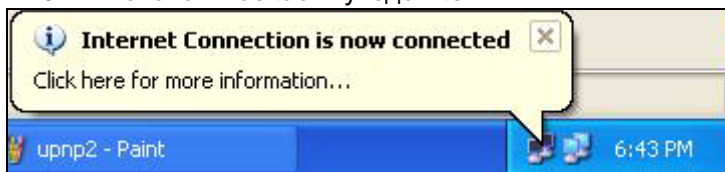


Рис. 70 Свойства подключения к Интернету: расширенные параметры: добавление



- 5 Когда устройство с поддержкой UPnP отключено от компьютера, все привязки порта удаляются автоматически.
- 6 Установите флажок **Show icon in notification area when connected** (**Показать значок в области уведомлений при наличии подключения**) и щелкните **ОК**. Значок отображается в области уведомлений на панели задач.

Рис. 71 Значок в области уведомлений



- 7 Чтобы просмотреть текущее состояние подключения к Интернету, дважды щелкните на значке.

Рис. 72 Состояние подключения к Интернету



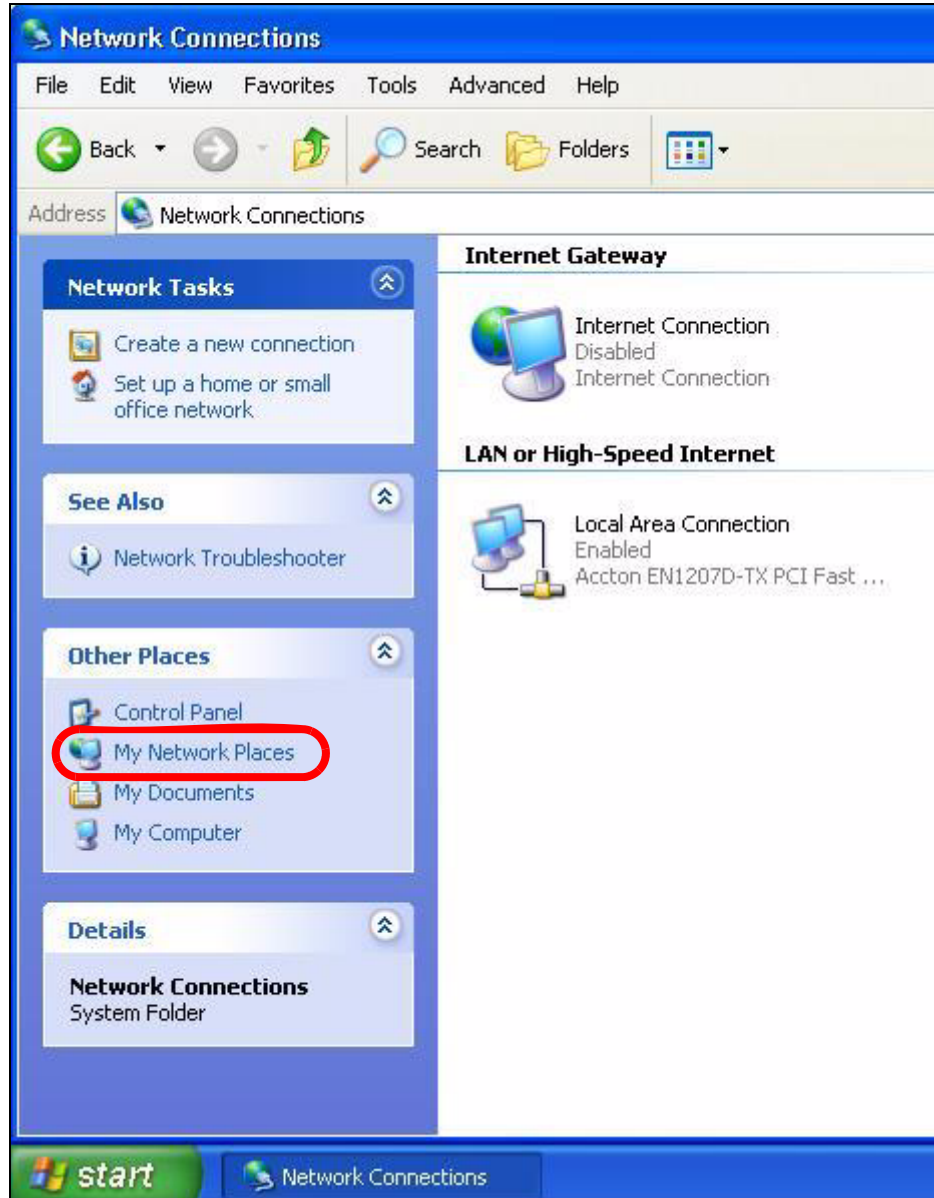
Упрощенный доступ к веб-конфигуратору

Благодаря системе UPnP можно получать доступ к веб-конфигуратору в P-791R v2 без выяснения IP-адреса P-791R v2. Это полезно, если неизвестен IP-адрес P-791R v2.

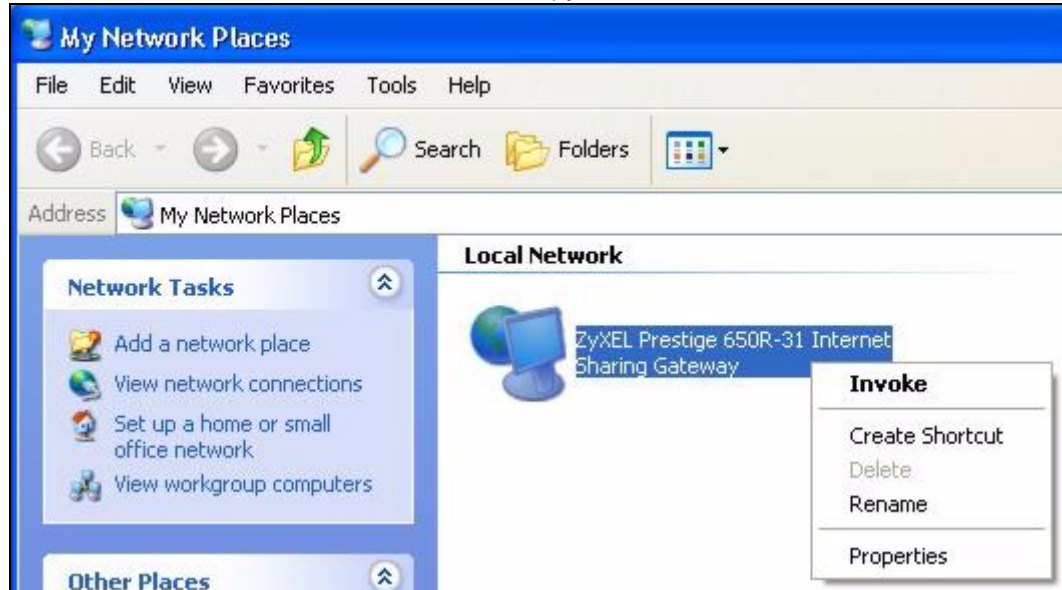
Чтобы вызвать веб-конфигуратор, выполните указанные ниже действия.

- 1 Нажмите кнопку **Start (Пуск)**, а затем – **Control Panel (Панель управления)**.
- 2 Дважды щелкните на значке **Network Connections (Сетевые подключения)**.
- 3 Выберите **My Network Places (Мои местоположения в сети)** под **Other Places**.

Рис. 73 Сетевые подключения



- 4 Под заголовком **Local Network** отображается значок с описанием каждого устройства с поддержкой UPnP.
- 5 Щелкните правой кнопкой мыши по значку P-791R v2 и выберите **Invoke** (Вызвать). Отображается экран регистрации веб-конфигуратора.

Рис. 74 Сетевые подключения: сетевое окружение

- 6 Щелкните правой кнопкой мыши по значку P-791R v2 и выберите **Properties** (Свойства). Отображается окно свойств с основной информацией о P-791R v2.

Рис. 75 Сетевые подключения: сетевое окружение: свойства: пример

ЧАСТЬ V

Сопровождение

Экран System (149)

Журналы (155)

Системные инструменты (159)

Диагностика (165)

Экран System

В этой главе описывается настройка имени системы, имени домена, пароля, а также времени и даты в P-791R v2.

13.1 Общая настройка

13.1.1 Разделы General Setup и System Name

Раздел **General Setup** содержит параметры, используемые для администрирования, и системную информацию. Поле **System Name** служит для идентификации устройства. Однако, поскольку некоторые поставщики услуг Интернета проверяют это имя, в нем следует ввести название вашего компьютера.

- В Windows 95/98 выберите **Start** (Пуск), **Settings** (Настройки), **Control Panel** (Панель управления), **Network** (Сеть). Щелкните вкладку **Identification** (Идентификация), обратите внимание на текст в поле **Computer name** (Имя компьютера) и введите его в поле **System Name**.
- В Windows 2000 нажмите **Start** (Пуск), **Settings** (Настройки), **Control Panel** (Панель управления) и дважды щелкните **System** (Система). Щелкните вкладку **Network Identification** (Идентификация сети), а затем – кнопку **Properties** (Свойства). Обратите внимание на текст в поле **Computer name** (Имя компьютера) и введите его в поле **System Name**.
- В Windows XP нажмите кнопку **Start** (Пуск), **My Computer** (Мой компьютер), **View system information** (Просмотр сведений о системе), а затем щелкните вкладку **Computer Name** (Имя компьютера). Обратите внимание на текст в поле **Full computer name** (Полное имя компьютера) и введите его в поле **System Name** на P-791R v2.

13.1.2 Общая настройка

В поле **Domain Name** указывается информация, распространяемая DHCP-клиентам в локальной сети. Если оставить это поле пустым, используется имя домена, полученное по DHCP от ISP. В то время как имя хоста (System Name – Имя системы) следует вводить на каждом отдельном компьютере, доменное имя назначается из P-791R v2 через DHCP.

Этот экран служит для настройки имени системы P-791R v2 и имени домена, установки таймера неактивности и задания паролей. Чтобы перейти на экран **General**, выберите **Maintenance > System**.

Рис. 76 Экран System > General

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 43 Экран System > General

ПОЛЕ	ОПИСАНИЕ
System Setup	
System Name	Выберите описательное название, позволяющее идентифицировать оборудование. Рекомендуется ввести в этом поле то же значение, что и в поле "Computer name" ("Имя компьютера"). Это имя может быть длиной до 30 буквенно-цифровых символов. Пробелы недопустимы, но тире "-" и символ подчеркивания "_" приемлемы.
Domain Name	Введите здесь имя домена (если оно известно). Если оставить это поле пустым, ISP может назначить имя домена через DHCP. Имя домена, введенное пользователем, получает приоритет над назначенным ISP именем домена.
Administrator Inactivity Timer	Укажите число минут неактивности сеанса управления (через веб-конфигуратор или интерфейс командной строки), по истечении которого сеанс разрывается. Значение по умолчанию - 5 минут. После истечения сеанса потребуется повторно войти в веб-конфигуратор и ввести пароль. Большая длительность периода неактивности является фактором риска для безопасности системы. Значение "0" означает, что сеанс никогда не разрывается, независимо от периода неактивности (использовать данное значение не рекомендуется).
Password	
User Password	Войдя в систему с паролем пользователя, вы можете только просматривать текущее состояние P-791R v2. Пароль пользователя по умолчанию – user .
New Password	Введите новый системный пароль (до 30 символов). Обратите внимание, что при вводе пароля вместо вводимых символов на экране отображаются звездочки "*". После смены пароля для обращения к P-791R v2 нужно использовать новый пароль.
Retype to Confirm	Снова введите новый пароль для подтверждения.

Таблица 43 Экран System > General (продолжение)

ПОЛЕ	ОПИСАНИЕ
Admin Password	В дополнение к настройке через мастер пользователь может настраивать специальные функции P-791R v2, войдя в систему с именем пользователя и паролем администратора.
Old Password	Для настройки специальных функций введите в этом поле пароль администратора по умолчанию (1234) или существующий пароль, используемый для доступа к системе.
New Password	Введите новый системный пароль (до 30 символов). Обратите внимание, что при вводе пароля вместо вводимых символов на экране отображаются звездочки "*". После смены пароля для обращения к P-791R v2 нужно использовать новый пароль.
Retype to Confirm	Снова введите новый пароль для подтверждения.
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

13.2 Установка часов

Для изменения даты и времени в P-791R v2 выберите **Maintenance > System > Time Setting**. Появится изображенный ниже экран. Используйте это окно для настройки времени в P-791R v2 с учетом вашего часового пояса.

Рис. 77 Экран System > Time Setting

The screenshot shows the 'Time Setting' configuration window. At the top, there are tabs for 'General' and 'Time Setting'. Below the tabs, the 'Current Time and Date' section displays 'Current Time' as 01:09:37 and 'Current Date' as 2000-01-01. The 'Time and Date Setup' section has two radio buttons: 'Manual' (selected) and 'Get from Time Server'. Under 'Manual', there are input fields for 'New Time (hh:mm:ss)' showing 01:09:34 and 'New Date (yyyy/mm/dd)' showing 2000/01/01. Under 'Get from Time Server', there are fields for 'Time Protocol' (Daytime (RFC-867)) and 'Time Server Address' (0.0.0.0). The 'Time Zone Setup' section has a dropdown menu for 'Time Zone' set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. Below it, there is a checkbox for 'Enable Daylight Savings' which is unchecked. The 'Start Date' and 'End Date' are both set to 'First Sunday of January (2000-01-02) at 0 o'clock'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 44 Экран System > Time Setting

ПОЛЕ	ОПИСАНИЕ
Current Time and Date	
Current Time	В этом поле отображается текущее время по часам P-791R v2. При каждом обновлении этой страницы в браузере P-791R v2 синхронизирует часы с сервером точного времени.
Current Date	В этом поле отображается текущая дата по часам P-791R v2. При каждом обновлении этой страницы в браузере P-791R v2 синхронизирует дату с сервером точного времени.
Time and Date Setup	
Manual	Выберите этот переключатель, чтобы ввести время и дату вручную. Если вы одновременно настроили новое время, дату, часовой пояс и режим летнего/зимнего времени, введенные вами время и дата имеют приоритет, а настройки часового пояса и летнего/зимнего времени на заданные значения не действуют.
New Time (hh:mm:ss)	В этом поле отображаются последние показания времени, полученные с сервера точного времени или настроенные вручную. Если вы установили параметр Time and Date Setup в значение Manual , введите в этом поле новое время и нажмите Apply .
New Date (yyyy/mm/dd)	В этом поле отображается последняя дата, полученная с сервера точного времени или настроенная вручную. Если вы установили параметр Time and Date Setup в значение Manual , введите в этом поле новую дату и нажмите Apply .
Get from Time Server	Чтобы устройство P-791R v2 получало показания даты и времени с указанного ниже сервера точного времени, выберите этот параметр.
Time Protocol	Выберите протокол службы точного времени, по которому P-791R v2 будет обращаться к серверу при включении питания. Не все серверы точного времени поддерживают полный набор протоколов; обратитесь к оператору/администратору сети или подберите работающий протокол методом проб и ошибок. Основные различия между ними заключаются в формате сообщаемого времени. Формат Daytime (RFC 867) : день/месяц/год/часовой пояс, в котором находится сервер. Формат Time (RFC868) : целое число длиной 4 байта, означающее количество секунд, прошедшее с 0:0:0 01.01.1970 (1970/1/1 в 0:0:0). Формат NTP (RFC 1305) похож на Time (RFC 868).
Time Server Address	Введите IP-адрес или URL (до 20 знаков расширенного набора ASCII) сервера точного времени. Если вы не уверены в том, какие значения требуется ввести, обратитесь к провайдеру или администратору сети.
Time Zone Setup	
Time Zone	Выберите часовой пояс для данной местности. Это поле задает разницу во времени между местной временной зоной и гринвичским временем (GMT).
Enable Daylight Saving	Летнее время – это период между поздней весной и началом осени, когда во многих странах стрелки переводятся вперед на 1 час по отношению к обычному местному времени, чтобы продлить светлое время в конце дня. Выберите этот параметр, если в вашем часовом поясе действует переход на зимнее/летнее время.

Таблица 44 Экран System > Time Setting

ПОЛЕ	ОПИСАНИЕ
Start Date	<p>Укажите месяц и день перехода на летнее время, если был отмечен флажок Enable Daylight Saving. В поле o'clock используется 24-часовой формат. Примеры:</p> <p>На большей части территории США летнее время начинается во второе воскресенье марта. Для каждого часового пояса летнее время в США начинает действовать с 2:00 по местному времени. Поэтому для США необходимо выбрать Second, Sunday, March и 2:00.</p> <p>В Европейском союзе и в России летнее время начинается в последнее воскресенье марта. Во всех часовых поясах на территории Евросоюза летнее время начинается одновременно (в 1:00 по Гринвичу или UTC). Поэтому для Евросоюза необходимо выбрать Last, Sunday, March. Время, вводимое в поле o'clock, зависит от вашего часового пояса. Например, для Германии, где время на один час опережает гринвичское (GMT+1), следует ввести 2.</p>
End Date	<p>Укажите месяц и день перехода на зимнее время, если был отмечен флажок Enable Daylight Saving. В поле o'clock используется 24-часовой формат. Примеры:</p> <p>В США летнее время заканчивается в первое воскресенье ноября. Для каждого часового пояса летнее время в США заканчивает действовать в 2:00 по местному времени. Поэтому для США необходимо выбрать First, Sunday, November и 2:00.</p> <p>В Европейском союзе и в России летнее время заканчивается в последнее воскресенье октября. Во всех часовых поясах на территории Евросоюза летнее время заканчивается одновременно (в 1:00 по Гринвичу или UTC). Поэтому для Евросоюза необходимо выбрать Last, Sunday, October. Время, вводимое в поле o'clock, зависит от вашего часового пояса. Например, для Германии, где время на один час опережает гринвичское (GMT+1), следует ввести 2.</p>
Apply	Нажмите кнопку Apply , чтобы сохранить изменения в P-791R v2.
Cancel	Если нужно начать настройку заново, нажмите кнопку Cancel .

Журналы

В данной главе описывается настройка общих параметров ведения журналов и просмотр журналов P-791R v2. Пояснения по сообщениям, оставляемым в журналах, приведены в приложении.

14.1 Обзор средств ведения журналов

Веб-конфигуратор позволяет указать, какие категории событий и/или предупреждений должны отмечаться в журнале P-791R v2, и затем просмотреть журналы P-791R v2 или переслать их администратору (по электронной почте) или на SYSLOG-сервер.

14.1.1 Журналы и предупреждения

Предупреждение – это журнальное сообщение, требующее более серьёзного внимания. К предупреждениям относятся системные ошибки, атаки и попытки доступа к заблокированным веб-сайтам. Некоторые категории, такие как **системные ошибки**, состоят одновременно из простых журнальных сообщений и предупреждений. Их можно отличить по цвету на экране **View Log**. Предупреждения отображаются красным цветом, а журналы – чёрным.

14.2 Просмотр журналов

Чтобы перейти на экран **View Log**, выберите **Maintenance > Logs**. Экран **View Log** служит для просмотра журналов в категориях, выбранных на экране **Log Settings** (см. [разд. 14.3 на стр. 156](#)).

Сообщения, отмеченные красным цветом, являются предупреждениями. Журнал является кольцевым, т.е. при его заполнении происходит удаление старых записей. Щелкните заголовок столбца, чтобы отсортировать записи. Треугольник указывает на возрастающую или убывающую сортировку.

Рис. 78 Экран Logs > View Log

#	Time	Message	Source	Destination	Notes
1	01/01/2000 01:12:06	Router reply ICMP packet: ICMP(Host Unreachable)	192.168.1.1	192.168.1.34	ACCESS PERMITTED
2	01/01/2000 01:12:06	Firewall default policy: UDP (L to W)	192.168.1.34:1029172.17.2.5:161		ACCESS PERMITTED
3	01/01/2000 01:12:00	Router reply ICMP packet: ICMP(Host Unreachable)	192.168.1.1	192.168.1.34	ACCESS PERMITTED
4	01/01/2000 01:12:00	Firewall default policy: UDP (L to W)	192.168.1.34:1029172.17.2.5:161		ACCESS PERMITTED
5	01/01/2000 01:11:54	Router reply ICMP packet: ICMP(Host Unreachable)	192.168.1.1	192.168.1.34	ACCESS PERMITTED
6	01/01/2000 01:11:54	Firewall default policy: UDP (L to W)	192.168.1.34:1029172.17.2.5:161		ACCESS PERMITTED
7	01/01/2000 01:11:47	Router reply ICMP packet: ICMP(Host Unreachable)	192.168.1.1	192.168.1.34	ACCESS PERMITTED
8	01/01/2000 01:11:47	Firewall default policy: UDP (L to W)	192.168.1.34:1029172.17.2.5:161		ACCESS PERMITTED

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 45 Экран Logs > View Log

ПОЛЕ	ОПИСАНИЕ
Display	Категории, выбранные на странице Log Settings , отображаются в раскрывающемся списке. Выберите категорию журналов для просмотра; выберите пункт All Logs для просмотра журналов всех регистрационных категорий, выбранных на странице Log Settings .
Email Log Now	Нажмите кнопку Email Log Now , чтобы отправить экран журнала на адрес электронной почты, указанный на странице Log Settings (прежде убедитесь, что вы заполнили поля E-mail Log Settings на экране Log Settings).
Refresh	Нажмите кнопку Refresh для обновления экрана журнала.
Clear Log	Нажмите кнопку Clear Log для удаления всего содержимого журналов.
#	В этом поле отображается порядковый номер.
Time	В этом поле отображается время записи журнала.
Message	В этом поле указывается причина регистрации сообщения.
Source	В этом поле перечисляются исходные IP-адреса и номера портов поступающих пакетов.
Destination	В этом поле перечисляются IP-адреса места назначения и номера портов поступающих пакетов.
Notes	В этом поле отображается дополнительная информация о записи в журнале.

14.3 Настройка параметров ведения журналов

Дополнительные сведения см. в [разд. 14.1 на стр. 155](#). Экран **Log Settings** служит для настройки содержания журналов P-791R v2, графика отправки сообщений в журналы P-791R v2 и состава журнальных сообщений и экстренных предупреждений, регистрируемых P-791R v2. Дополнительные сведения см. в [разд. 14.1 на стр. 155](#).

Чтобы изменить параметры ведения журналов P-791R v2, выберите **Maintenance > Logs > Log Settings**. Появится изображенный ниже экран.

Предупреждения отправляются по электронной почте немедленно после их появления. Журналы могут отправляться по электронной почте, когда журнал заполняется. Если выбрано много типов предупреждений и/или категорий журналов (особенно в разделе **Access Control**), поток отправляемых по электронной почте сообщений может быть существенным.

Рис. 79 Экран Logs > Log Settings

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 46 Экран Logs > Log Settings

ПОЛЕ	ОПИСАНИЕ
E-mail Log Settings	
Mail Server	Введите имя сервера или IP-адрес почтового сервера для адресов электронной почты, указанных ниже. Если это поле оставить пустым, журналы и сообщения с предупреждениями не будут отправляться по электронной почте.
Mail Subject	Введите тему, которая будет указываться в заголовке журнальных сообщений, отправляемых P-791R v2 по электронной почте. Это поле имеется не у всех моделей P-791R v2.
Send Log To	P-791R v2 отправляет журналы по адресу электронной почты, указанному в данном поле. Если это поле оставить пустым, P-791R v2 не будет отправлять журналы по электронной почте.

Таблица 46 Экран Logs > Log Settings

ПОЛЕ	ОПИСАНИЕ
Send Alerts To	Оповещения - это уведомления, отправляемые в режиме реального времени, как только происходит событие, такое как атака DoS, ошибка системы или попытка доступа к запрещённому веб-узлу. Введите адрес электронной почты, по которому должны отправляться сообщения с предупреждениями. Оповещения содержат ошибки системы, атаки и попытки доступа к заблокированным веб-сайтам. Если это поле оставить пустым, сообщения с предупреждениями не будут отправляться по электронной почте.
Log Schedule	Это раскрывающееся меню используется для настройки периодичности отправки журнальных сообщений по электронной почте: Daily (ежедневно) Weekly (еженедельно) Hourly (ежечасно) When Log is Full (когда журнал полон) None (Нет). При выборе Weekly или Daily укажите время суток, когда должны отправляться сообщения по электронной почте. При выборе варианта Weekly укажите также день недели, когда должно отправляться сообщение. При выборе When Log is Full предупреждение отправляется, когда заполнен журнал. При выборе варианта None журнальные сообщения не отправляются.
Day for Sending Log	В раскрывающемся списке выберите день недели для отправки журналов.
Time for Sending Log	Введите время дня в 24-часовом формате (например, 23:00 соответствует 11:00 вечера) для отправки журналов.
Clear log after sending mail	Установите этот флажок, чтобы удалять все журналы после того, как P-791R v2 отправит их по электронной почте.
Syslog Logging	P-791R v2 отправляет журнальное сообщение на внешний сервер системного журнала (SYSLOG).
Active	Щёлкните на флажке Active для включения регистрации системных журналов.
Syslog Server IP Address	Введите имя или IP-адрес сервера SYSLOG, который будет принимать журнальные сообщения указанной категории.
Log Facility	Выберите местоположение из раскрывающегося списка. Распределение по журнальным объектам ("log facility") позволяет записывать сообщения на сервере в различные файлы. Обращайтесь к руководству сервера системных журналов для получения дополнительной информации.
Active Log and Alert	
Log	Выберите категории журналов, которые необходимо записать.
Send Immediate Alert	Выберите категории журналов, предупреждения по которым должны немедленно отправляться P-791R v2 по электронной почте.
Apply	Нажмите кнопку Apply для сохранения настроек и выхода из данного экрана.
Cancel	Чтобы вернуться к прежним настройкам, нажмите Cancel .

Системные инструменты

В этой главе описывается загрузка новой микропрограммы, управление настройками и перезагрузка P-791R v2.

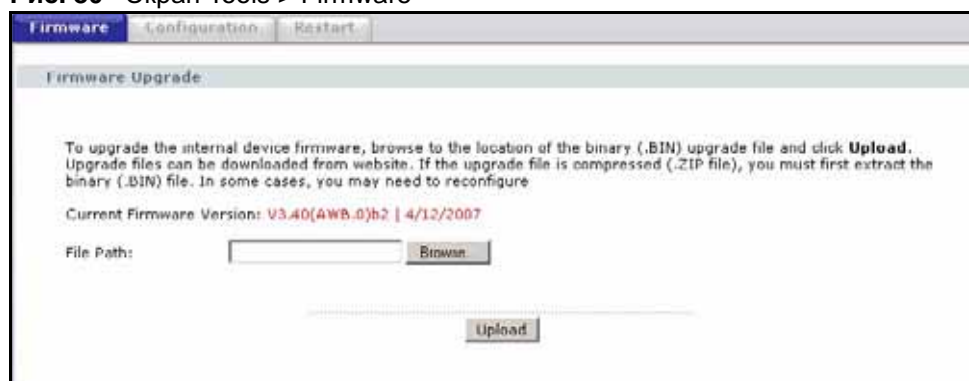
15.1 Обновление микропрограммы

Найдите файл с микропрограммой на сайте www.zyxel.ru. Обычно имя файла соответствует номеру модели с расширением “.bin” – например, “P-791R v2.bin”. В процессе загрузки, длящейся до двух минут, используется HTTP (Протокол передачи гипертекста). После успешной загрузки система перезапускается.

Используйте только микропрограмму, предназначенную для конкретной модели устройства. См. наклейку на нижней стороне корпуса устройства.

Чтобы перейти на экран **Firmware**, выберите **Maintenance > Tools**. Для загрузки микропрограммы в P-791R v2 следуйте указаниям на этом экране.

Рис. 80 Экран Tools > Firmware



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 47 Экран Tools > Firmware

ПОЛЕ	ОПИСАНИЕ
Current Firmware Version	В этом поле отображается версия и дата создания используемой микропрограммы.
File Path	Введите местоположение файла, который необходимо загрузить, в этом поле, или нажмите кнопку Browse ... (Обзор) для поиска этого файла.

Таблица 47 Экран Tools > Firmware (продолжение)

ПОЛЕ	ОПИСАНИЕ
Browse...	Нажмите кнопку Browse... (Найти) для поиска bin-файла, который необходимо загрузить. Помните о том, что необходимо распаковать сжатые файлы (.zip) перед их загрузкой в устройство.
Upload	Нажмите кнопку Upload , чтобы начать процесс загрузки. Этот процесс может занять до двух минут. Примечание. Не выключайте устройство во время загрузки в него микропрограммы.



НЕ выключайте P-791R v2, пока идет загрузка микропрограммы!

После того, как появится экран **Firmware Upload in Progress**, подождите две минуты, прежде чем снова обращаться к P-791R v2.

Рис. 81 Выполнение загрузки микропрограммы

По окончании загрузки микропрограммы P-791R v2 автоматически перезапускается, что приводит к временному отключению от сети. В некоторых операционных системах на рабочем столе может находиться следующий значок.

Рис. 82 Сеть временно недоступна

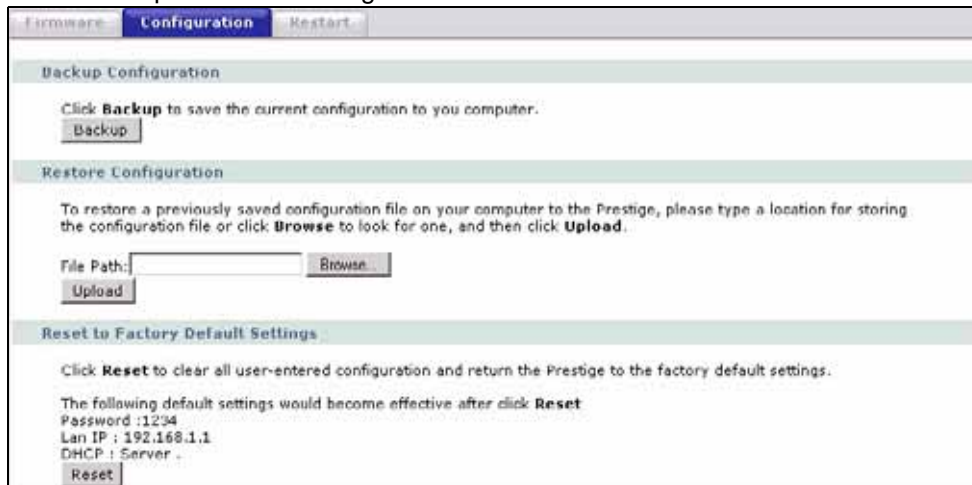
Через две минуты зарегистрируйтесь снова и проверьте новую версию микропрограммы на экране **Status**.

Если выгрузка была неудачной, появится следующее окно. Нажмите **Return**, если нужно вернуться к экрану **Firmware**.

Рис. 83 Сообщение об ошибке

15.2 Экран Configuration

Этот экран служит для резервного копирования или восстановления настроек P-791R v2. На нем также можно осуществить сброс P-791R v2 к заводским настройкам по умолчанию. Для перехода на этот экран выберите **Maintenance > Tools > Configuration**.

Рис. 84 Экран Tools > Configuration

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 48 Экран Tools > Configuration

ПОЛЕ	ОПИСАНИЕ
Backup Configuration	
Backup	Нажмите эту кнопку, чтобы сохранить текущие настройки P-791R v2 на вашем компьютере. После того, как устройство будет настроено и начнет работать в штатном режиме, рекомендуется перед любым изменением настроек делать резервную копию файла настроек. Резервный файл будет полезен в том случае, если потребуется вернуться к предыдущим настройкам.
Restore Configuration	
File Path	Введите местоположение файла для загрузки в устройство или нажмите Browse... , чтобы найти файл на диске.
Browse	Нажмите эту кнопку, чтобы найти файл, который требуется загрузить.

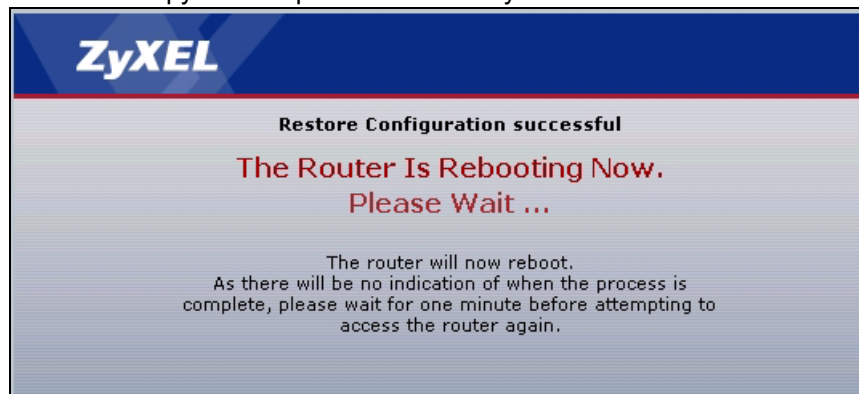
Таблица 48 Экран Tools > Configuration (продолжение)

ПОЛЕ	ОПИСАНИЕ
Upload	Нажмите эту кнопку для восстановления настроек из выбранного файла. Дополнительные сведения приведены ниже. Примечание. Не выключайте устройство во время загрузки в него файла настроек.
Reset to Factory Default Settings	
Reset	Нажмите эту кнопку, чтобы сбросить все пользовательские настройки и восстановить в P-791R v2 заводские настройки по умолчанию. Предупреждающий экран в этом случае не появится. Подробное описание процедуры сброса P-791R v2 см. в разд. 2.5 на стр. 46 .



Не выключайте устройство во время загрузки в него файла настроек!

Завершив восстановление настроек из выбранного файла, P-791R v2 выдаст следующий экран.

Рис. 85 Загрузка настроек выполнена успешно

После этого устройство автоматически перезагрузится. Соединение с сетью временно будет прервано. В некоторых операционных системах на рабочем столе может находиться следующий значок.

Рис. 86 Сеть временно недоступна

Если прежний IP-адрес P-791R v2 отличается от указанного в файле настроек, необходимо проверить, находится ли IP-адрес компьютера в одной подсети с P-791R v2. Указания по настройке IP-адреса компьютера см. в Руководстве по быстрому запуску.

Для повторного входа в настройки устройства может потребоваться открытие нового окна в браузере.

Если загрузку выполнить не удалось, появится экран **Configuration Upload Error** (Ошибка загрузки настроек).

Рис. 87 Ошибка при загрузке настроек



Нажмите ссылку **Return** (Назад), если нужно вернуться на предыдущий экран.

15.3 Restart

Функция перезагрузки системы позволяет перезагрузить P-791R v2, не выключая питание.

Выберите **Maintenance > Tools > Restart**. Чтобы перезагрузить P-791R v2, выберите **Restart**. Эта операция не влияет на настройки P-791R v2.

Рис. 88 Экран Tools > Restart



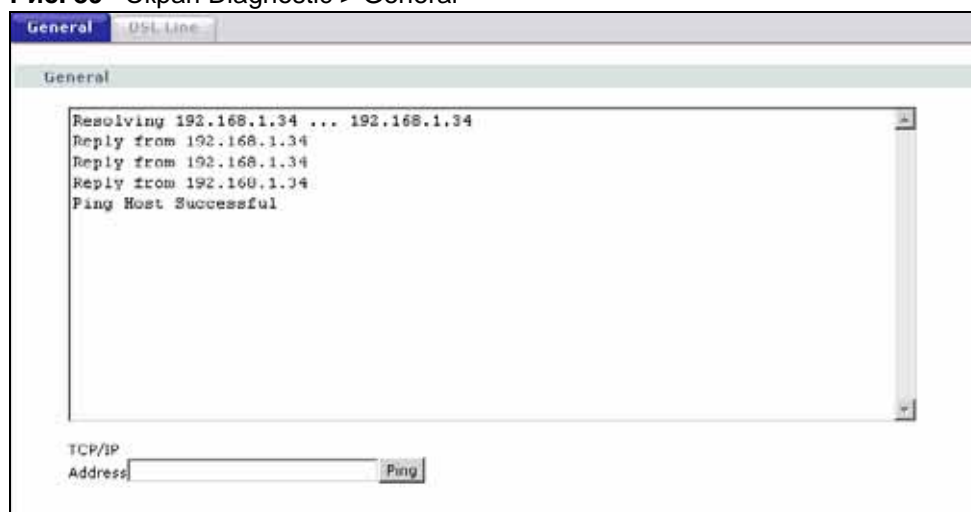
Диагностика

На этих экранах (доступных только для чтения) отображаются данные, которые могут помочь вам при диагностике проблем с P-791R v2.

16.1 Общая диагностика

Этот экран позволяет отправить эхозапрос на любой компьютер в сети. Чтобы перейти на показанный ниже экран, выберите **Maintenance > Diagnostic**.

Рис. 89 Экран Diagnostic > General



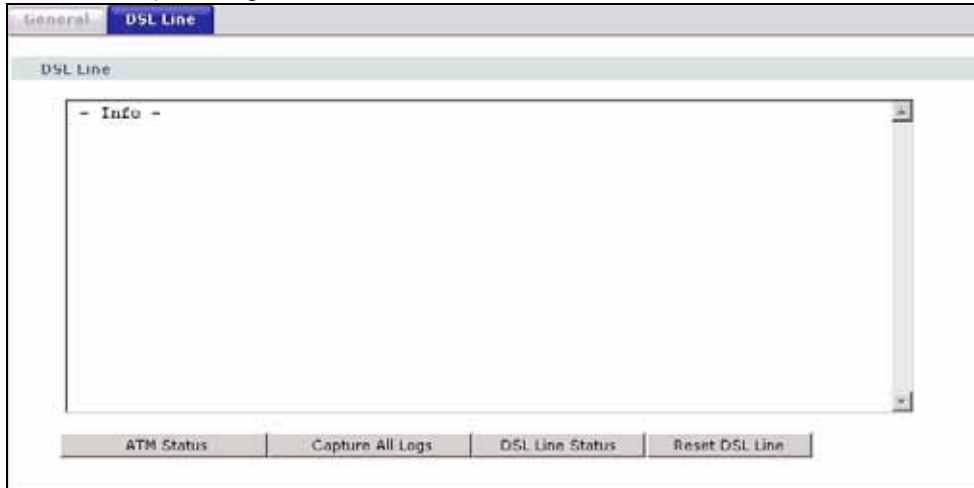
Поля изображённого выше экрана описаны в следующей таблице.

Таблица 49 Экран Diagnostic > General

ПОЛЕ	ОПИСАНИЕ
TCP/IP Address	Введите IP-адрес компьютера, соединение с которым требуется проверить посредством эхозапроса.
Ping	Чтобы проверить указанный IP-адрес с помощью эхозапроса, нажмите эту кнопку. Результаты будут отображены на экране.

16.2 Экран DSL Line Diagnostic

Этот экран служит для диагностики DSL-линии. Чтобы перейти на показанный ниже экран, выберите **Maintenance > Diagnostic > DSL Line**.

Рис. 90 Экран Diagnostic > DSL Line

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 50 Экран Diagnostic > DSL Line

ПОЛЕ	ОПИСАНИЕ
ATM Status	Нажмите эту кнопку, чтобы просмотреть состояние ATM.
Capture All Logs	Нажмите эту кнопку, чтобы просмотреть все сообщения в журналах, связанные с DSL-линией.
DSL Line Status	Нажмите эту кнопку, чтобы просмотреть рабочие параметры DSL-порта и распределение битовых полос.
Reset DSL Line	Нажмите эту кнопку, чтобы сбросить DSL-линию. После этого в крупном текстовом поле над этой кнопкой будет высвечиваться ход выполнения и результат операции, например: <pre>"Start to reset DSL Loading DSL modem F/W... Reset DSL Line Successfully!"</pre>

ЧАСТЬ VI

Использование SMT и устранение неполадок

- Введение в SMT (169)
- Общая настройка (175)
- Настройка WAN (179)
- Настройка LAN (185)
- Настройка доступа к Интернету (191)
- Настройка удаленного узла (195)
- Настройка статического маршрута (207)
- Настройка NAT (211)
- Настройка фильтра (227)
- Настройка SNMP (241)
- Системный пароль (243)
- Информация о системе и диагностика (245)
- Работа с файлами микропрограмм и настроек (255)
- Разделы меню с 24.8 по 24.11 (269)
- Настройка политик маршрутизации IP (277)
- Настройка расписания (285)
- Поиск и устранение неполадок (289)

Введение в SMT

Терминал управления системой (SMT) представляет собой текстовую консоль с системой меню для управления устройством P-791R v2. В этой главе описан вызов SMT и приведена краткая сводка имеющихся меню.

17.1 Получение доступа к SMT через порт консоли

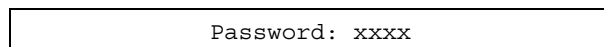
Порт CON/AUX используется для настройки P-791R v2 с помощью меню SMT. Установите переключатель CON/AUX в положение CON (Console), чтобы использовать порт CON/AUX для настройки и управления локальным устройством. Подключите разъем RJ-45 кабеля консоли к порту CON/AUX устройства ZyxEL, а другой конец кабеля — к последовательному порту (COM1, COM2 или другой порт COM) компьютера. На компьютере должна быть установлена программа эмуляции терминала (например, HyperTerminal), установленная в режим эмуляции VT100 без чётности с 8 битами данных, 1 стоповым битом, без сигналов квитирования, со скоростью порта 9600 бит/с.

17.2 Получение доступа к SMT через Telnet

SMT доступен по протоколу Telnet. Используйте желтый кабель Ethernet для подключения компьютера к порту ETHERNET устройства ZyxEL. Выполните следующие операции:

- 1 В Windows нажмите кнопку **Start** (Пуск) > **Run** (Выполнить).
- 2 Введите “telnet **w.x.y.z**” и нажмите **OK**.
Вместо **w.x.y.z** укажите IP-адрес устройства P-791R v2; адрес по умолчанию – 192.168.1.1.
P-791R v2 предложит ввести пароль.

Рис. 91 Экран входа



Password: xxxx

- 3 Введите пароль. Пароль по умолчанию – 1234. При вводе пароля на экране отображается звездочка “*” вместо вводимых символов.
- 4 После ввода пароля SMT откроет главное меню, как показано ниже.



Изменить пароль можно в меню 23.1.

Рис. 92 Главное меню SMT

```

Copyright (c) 1994 - 2007 ZyXEL Communications Corp.

P-791R v2 Main Menu

Getting Started
  1. General Setup
  2. WAN Setup
  3. LAN Setup
  4. Internet Access Setup

Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup
  15. NAT Setup

Advanced Management
  21. Filter Set Configuration
  22. SNMP Configuration
  23. System Password
  24. System Maintenance
  25. IP Routing Policy Setup
  26. Schedule Setup

99. Exit

Enter Menu Selection Number:

```



В системе предусмотрен таймер неактивности, по умолчанию настроенный на 10 минут. При отсутствии действий пользователя в течение этого времени P-791R v2 автоматически разрывает сеанс. В этом случае потребуется повторно войти в управление P-791R v2. Длительность периода неактивности можно настроить в веб-конфигураторе или посредством командной строки (КС) (меню 24.8).

17.3 Структура меню SMT

Каждый пункт меню кратко описан в следующей таблице.

Таблица 51 Краткий обзор главного меню

МЕНЮ	НАЗНАЧЕНИЕ
1 General Setup (общая настройка)	Это меню позволяет настроить режим работы устройства, службу DNS для динамических адресов и настроить параметры администрирования.
2 WAN Setup (настройка WAN)	Это меню служит для настройки параметров DSL-соединения, переадресации трафика и резервирования через коммутируемый доступ.

Таблица 51 Краткий обзор главного меню

МЕНЮ	НАЗНАЧЕНИЕ
3 LAN Setup (настройка локальной сети)	Этот раздел меню служит для применения фильтров LAN, настройки параметров DHCP и TCP/IP для сети LAN, а также для разрешения или блокирования обмена данными на 2-м уровне между отдельными парами портов.
4 Internet Access Setup (настройка доступа в Интернет)	Это меню служит для настройки подключения к Интернету.
11 Remote Node Setup (настройка удаленного узла)	Это меню используется для детальной настройки параметров удаленного узла (которым может являться ваш поставщик услуг Интернета), а также для применения фильтров.
12 Static Routing Setup	Это меню служит для настройки статических маршрутов IP и статических маршрутов моста (на уровне MAC).
15 NAT Setup (настройка NAT)	Этот экран позволяет настроить параметры трансляции сетевых адресов (NAT) в P-791R v2.
21 Filter Set Configuration (настройка набора фильтров)	Это меню служит для настройки фильтров.
22 SNMP Configuration (настройка SNMP)	Это меню служит для настройки SNMP.
23 System Password (системный пароль)	Это меню служит для изменения пароля.
24 System Maintenance (обслуживание системы)	Это меню служит для комплексной диагностики и обслуживания системы, от контроля состояния до загрузки микропрограммы. Из него также доступен интерфейс командной строки (КС).
25 IP Routing Policy Setup (настройка политик маршрутизации)	Это меню служит для настройки маршрутов в соответствии с политиками.
26 Schedule Setup (настройка расписания)	Это меню служит для настройки наборов расписаний.
99 Exit	Это меню служит для выхода из SMT.

Содержание отдельных меню SMT описано в следующей таблице.

Таблица 52 Общая структура меню SMT

МЕНЮ	ПОДМЕНЮ		
1 General Setup (общая настройка)	1.1 Configure Dynamic DNS (настройка DNS для динамических адресов)		
2 WAN Setup (настройка WAN)	2.1 Traffic Redirect Setup (настройка переадресации трафика)		
	2.2 Dial Backup Setup (настройка резервирования через коммутируемый доступ)	2.2.1 Advanced Dial Backup Setup (расширенная настройка резервирования)	

Таблица 52 Общая структура меню SMT (продолжение)

МЕНЮ	ПОДМЕНЮ		
3 LAN Setup (настройка локальной сети)	3.1 LAN Port Filter Setup (настройка фильтрации портов LAN)		
	3.2 TCP/IP and DHCP Setup (настройка TCP/IP и DHCP)	3.2.1 IP Alias Setup (настройка совмещения IP-адресов)	
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 параметры сетевого уровня для удаленного узла		
	11.5 фильтр удаленного узла		
	11.6 параметры уровня ATM для удаленного узла		
	11.8 специальные параметры настройки		
12 Static Route Setup (настройка статических маршрутов)	12.1 IP Static Route Setup (настройка статических маршрутов IP)	12.1.1 Edit IP Static Route (редактирование статических маршрутов IP)	
	12.3 Bridge Static Route Setup (настройка статических маршрутов в режиме моста)	12.3.1 Edit Bridge Static Route (редактирование статических маршрутов моста)	
15 NAT Setup (настройка NAT)	15.1 Address Mapping Sets (наборы привязки адресов)	15.1.x Address Mapping Rules (правила привязки адресов)	15.1.x.x Address Mapping Rule (правило привязки адресов)
	15.2 NAT Server Sets (наборы серверов для NAT)	15.2.x NAT Server Setup (настройка сервера, находящегося за NAT)	
21 Filter Set Configuration (настройка набора фильтров)	21.1 x Filter Rules Summary (сводка правил фильтра)	21.1.x.x TCP/IP Filter Rule (правило фильтра TCP/IP)	
22 SNMP Configuration (настройка SNMP)			
23 System Password (системный пароль)			

Таблица 52 Общая структура меню SMT (продолжение)

МЕНЮ	ПОДМЕНЮ		
24 System Maintenance (обслуживание системы)	24.1 System Maintenance - System Status (состояние системы)		
	24.2 System Information and Console Port Speed (сведения о системе и скорость консольного порта)	24.2.1 System Maintenance - Information (информационный экран)	
		24.2.2 System Maintenance - Change Console Port Speed (изменение скорости консольного порта)	
	24.3 System Maintenance - Log and Trace (журналы и трассировка)	24.3.1 View Error Log (просмотр журнала ошибок)	
		24.3.2 System Maintenance - UNIX Syslog (системный журнал UNIX)	
	24.4 System Maintenance - Diagnostic (диагностика)		
	24.5 Backup Configuration (резервное копирование настроек)		
	24.6 Restore Configuration (восстановление настроек)		
	24.7 System Maintenance - Upload Firmware (загрузка микропрограмм)	24.7.1 System Maintenance - Upload System Firmware (загрузка системной микропрограммы)	
		24.7.2 System Maintenance - Upload System Configuration File (загрузка файла настроек)	
	24.8 Command Interpreter Mode (режим интерпретатора команд)		
	24.9 System Maintenance - Call Control (управление вызовами)	24.9.1 Budget Management (управление бюджетом)	
	24.10 System Maintenance - Time and Date Setting (настройка времени и даты)		
24.11 Remote Management Control (настройка удаленного управления)			
25 IP Routing Policy Summary (сводка политик маршрутизации)	25.1 IP Routing Policy Setup (настройка политик маршрутизации)	25.1.1 IP Routing Policy (политика маршрутизации IP)	
26 Schedule Setup (настройка расписания)	26.1 Schedule Set Setup (настройка набора расписаний)		

17.4 Использование интерфейса SMT

Прежде чем приступить к настройке устройства посредством SMT, необходимо ознакомиться со следующими приемами работы в меню.

Таблица 53 Команды главного меню

ОПЕРАЦИЯ	КЛАВИШИ И ЗНАЧКИ	ОПИСАНИЕ
Перемещение к следующему меню	[ENTER]	Для перехода к подменю введите номер нужного подменю и нажмите клавишу [ENTER].
Возврат к предыдущему меню	[ESC]	Нажмите [ESC] ([ВЫХОД]) для перемещения к предыдущему меню.
Перемещение к "скрытому" меню	Нажмите пробел, чтобы изменить значение No на Yes , затем нажмите [ENTER].	Поля, начинающиеся со слова "Edit" ("Редактировать"), ведут к скрытым меню, которые по умолчанию содержат значение No (Нет). Чтобы изменить значение No (Нет) на Yes (Да), нажмите один раз пробел. Затем, чтобы войти в "скрытое" меню, нажмите [ENTER].
Перемещение курсора	Клавиша [ENTER] ("ввод") или стрелки вверх/вниз.	Перейдя к меню, нажмите [ENTER] для перемещения к следующему полю. Можно также использовать клавиши со стрелками [UP]/[DOWN] ([ВВЕРХ]/[ВНИЗ]) для перемещения к предыдущему и следующему полю соответственно.
Ввод информации	Введите символ или нажмите пробел, затем нажмите [ENTER].	Необходимо заполнить 2 типа полей. В первом требуется ввести соответствующую информацию. Во втором можно циклически пройти по доступным вариантам выбора, нажимая пробел.
Обязательные поля	<?> или ChangeMe	Необходимо заполнить все поля символом <?>, чтобы иметь возможность сохранения новой конфигурации. Нельзя оставлять пустыми поля со значением ChangeMe , чтобы иметь возможность сохранения новой конфигурации.
Неприменимые поля	<N/A>	В некоторых полях в SMT отображается значение <N/A> (Неприменимо). Этот символ относится к опции, являющейся Not Applicable (Неприменимой).
Save your configuration (Сохранение конфигурации)	[ENTER]	Сохраните конфигурацию, нажав [ENTER] ([ВВОД]) при появлении сообщения "Нажмите [ENTER] ([ВВОД]) для подтверждения или [ESC] ([ВЫХОД]) для отмены". Сохранение данных на отображаемом экране приведет в большинстве случаев к предыдущему меню.
Выход из SMT	Введите число 99, затем нажмите [ENTER].	Введите число 99 в окне приглашения главного меню и нажмите [ENTER] для выхода из интерфейса SMT.

Общая настройка

Это меню позволяет настроить режим работы устройства, службу DNS для динамических адресов и настроить параметры администрирования.

18.1 Задание общих настроек

- 1 В главном меню введите 1, чтобы перейти в раздел **Menu 1 - General Setup** (Общая настройка).
- 2 Появится экран **Menu 1 - General Setup**, показанный ниже. Заполните нужные поля.

Рис. 93 Меню 1: общая настройка

```

Menu 1 - General Setup

System Name= P-791Rv2
Location=
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No

Route IP= Yes
Bridge= No
  
```

Поля изображённого выше меню описаны в следующей таблице.

Таблица 54 Меню 1: экран General Setup

ПОЛЕ	ОПИСАНИЕ
System Name	Выберите описательное название, позволяющее идентифицировать оборудование. Рекомендуется ввести "Computer name" ("Имя компьютера") в данном поле. Это имя может быть длиной до 30 буквенно-цифровых символов. Пробелы недопустимы, но тире "-" и символ подчеркивания "_" приемлемы.
Location	Введите описание места размещения P-791R v2. В этом поле можно ввести до 31 символов или оставить его пустым.
Contact Person's Name	Укажите ФИО лица, которому могут быть направлены вопросы, касающиеся P-791R v2. В этом поле можно ввести до 30 символов или оставить его пустым.

Таблица 54 Меню 1: экран General Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Domain Name	Введите здесь имя домена (если оно известно). Если оставить это поле пустым, ISP может назначить имя домена через DHCP. Можно перейти к меню 24.8 и ввести "sys domain name" ("имя домена системы"), чтобы увидеть текущее имя домена, используемое интернет-центром. Имя домена, введенное пользователем, получает приоритет над назначенным ISP именем домена. Если нужно очистить это поле, просто нажмите пробел, а затем [ENTER].
Edit Dynamic DNS	Нажмите пробел и [ENTER], чтобы выбрать значение Yes или No (по умолчанию). Выберите Yes для настройки раздела Menu 1.1: Configure Dynamic DNS , описанного ниже.
Route IP	Выберите Yes , чтобы включить в P-791R v2 IP-маршрутизацию. Этот параметр начинает действовать для данного удаленного узла только после того, как на удаленном узле также будет выбрана IP-маршрутизация. См. Меню 11.1: профиль удаленного узла (узлы 1 – 7) в разд. 22.3 на стр. 195 . На этом экране необходимо включить Route IP , Bridge или оба режима. Если режимы Route IP и Bridge отключены, устройство не будет пересылать трафик между портами LAN и удаленным узлом.
Bridge	Если для параметра Route IP выбрано значение Yes , выберите в этом поле Yes , чтобы разрешить режим моста в P-791R v2 для протоколов, не поддерживаемых IP-маршрутизацией (например, SNA). Если для параметра Route IP выбрано значение No , выберите Yes , чтобы установить мост через P-791R v2 для всех протоколов. Во всех случаях этот параметр становится действителен только после того, как на соответствующем удаленном узле также будет активирован мост. См. Меню 11.1: профиль удаленного узла (узлы 1 – 7) в разд. 22.3 на стр. 195 . На этом экране необходимо включить Route IP , Bridge или оба режима. Если режимы Route IP и Bridge отключены, устройство не будет пересылать трафик между портами LAN и удаленным узлом.
После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в приглашении "Press ENTER to Confirm..." ("Нажмите ВВОД для подтверждения...") для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции в любой момент.	

18.1.1 Настройка динамической DNS

Чтобы настроить DNS для динамических адресов, установите P-791R v2 в режим маршрутизатора в меню 1 или на экране **MAINTENANCE Device Mode**, перейдите в раздел **Menu 1 - General Setup**, затем нажмите пробел, чтобы выбрать **Yes** в поле **Edit Dynamic DNS**. Нажмите [ENTER], чтобы вызвать раздел **Menu 1.1 - Configure Dynamic DNS** (показанный ниже).

Рис. 94 Меню 1.1: настройка DNS для динамических адресов

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= No
DDNSType= DynamicDNS
Host 1=
Host 2=
Host 3=
Username=
Password= *****
Enable Wildcard Option= No
Enable Off Line Option= N/A
IP Address Update Policy:
  DDNS Server Auto Detect IP Address= No
  Use Specified IP Address= No
  Use IP Address= N/A

```

Выполните инструкции, указанные в таблице ниже, для настройки параметров динамической DNS.

Таблица 55 Меню 1.1: настройка DNS для динамических адресов

ПОЛЕ	ОПИСАНИЕ
Service Provider	Это название поставщика услуг динамической DNS.
Active	Нажмите пробел, чтобы выбрать значение Yes , а затем нажмите [ENTER], чтобы активировать DNS для динамических адресов.
DDNSType	Если вы используете службу DNS для динамических адресов, нажмите пробел и [ENTER], чтобы выбрать DynamicDNS . Выберите StaticDNS , если используется DNS для статических адресов. Выберите CustomDNS , если используется специализированная служба DNS.
Host 1-3	Введите в этих полях имена хостов (не более трех).
Username	Введите свое имя пользователя.
Password	Введите присвоенный вам пароль.
Enable Wildcard Option	P-791R v2 поддерживает шаблоны DYNDNS. Нажмите пробел и [ENTER] для выбора значения Yes или No . Это поле не учитывается (N/A), если в качестве поставщика услуг используется клиент DDNS.
Enable Off Line Option	Это поле доступно только в том случае, когда в поле DDNS Type выбрано значение CustomDNS . Нажмите пробел и [ENTER] для выбора значения Yes . Когда выбрано значение Yes (Да) , трафик http://www.dyndns.org/ перенаправляется на адрес, указанный ранее (обращайтесь по адресу www.dyndns.org для получения дополнительных сведений).
IP Address Update Policy	Можно выбрать значение Yes в любом из полей: DDNS Server Auto Detect IP Address (рекомендуемое) или Use Specified IP Address , но не в обоих полях. Если поля DDNS Server Auto Detect IP Address и Use Specified IP Address оба имеют значение No , сервер DDNS будет автоматически обновлять IP-адрес для имен хоста P-791R v2, руководствуясь его IP-адресом в сети WAN. DDNS не работает с частным IP-адресом. Если значения обоих полей – No , то для работы с DDNS устройство P-791R v2 должно иметь глобальный IP-адрес в сети WAN.

Таблица 55 Меню 1.1: настройка DNS для динамических адресов

ПОЛЕ	ОПИСАНИЕ
DDNS Server Auto Detect IP Address	<p>Этот параметр следует выбирать только в том случае, если между P-791R v2 и сервером DDNS присутствуют один или несколько маршрутизаторов с поддержкой NAT. Нажмите пробел, чтобы выбрать Yes, затем нажмите [ENTER], чтобы сервер DDNS автоматически определил и запомнил IP-адрес маршрутизатора NAT, которому присвоен глобальный IP-адрес.</p> <p>Примечание. DDNS-сервер может неверно определить IP-адрес, если между P-791R v2 и DDNS-сервером присутствует прокси-сервер HTTP.</p>
Use Specified IP Address	<p>Нажмите пробел для выбора значения Yes, а затем нажмите [ENTER] для обновления IP-адреса имени (имен) хоста, чтобы установить значение IP-адреса, указанное ниже.</p> <p>Значение Yes следует выбирать только в том случае, если P-791R v2 использует статический глобальный IP-адрес или находится за другим устройством, использующим такой адрес.</p>
Use IP Address	<p>Если в поле Use Specified IP Address было выбрано значение Yes, введите статический глобальный IP-адрес.</p>
<p>После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в приглашении "Press ENTER to Confirm..." ("Нажмите ВВОД для подтверждения...") для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции в любой момент.</p>	

Настройка WAN

Это меню служит для настройки параметров DSL-соединения, переадресации трафика и резервирования через коммутируемый доступ.

19.1 Настройка WAN

В главном меню введите 2 для открытия меню 2.

Рис. 95 Меню 2: настройка WAN

```

Меню 2 - настройка WAN

Service Mode= 2-wire
Service Type= Server
Rate Adaption= Disable
Transfer Max Rate(Kbps)= 5696
Transfer Min Rate(Kbps)= 192
Standard Mode= ETSI(ANNEX_B)
Wan Backup Setup:
Check Mechanism = ICMP
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 = 31
  Recovery Interval(sec) = 3
  ICMP Timeout(sec) = 9677
Traffic Redirect = No
Dial Backup = No
  
```

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 56 Меню 2: настройка WAN

ПОЛЕ	ОПИСАНИЕ
Service Mode	В этом поле указывается, что P-791R v2 использует 2-проводной режим для подключения к линии DSL. Выбираемый режим зависит от параметров имеющейся телефонной линии и влияет на максимальную скорость соединения. В 2-проводном режиме максимальная скорость передачи данных не превышает 5,69 Мбит/с.
Service Type	Нажмите пробел, чтобы указать, на какой из сторон DSL-соединения (клиентской или серверной) находится P-791R v2. Выберите Server , если данное устройство P-791R v2 является сервером в соединении по схеме "точка-точка". (См. гл. 4 на стр. 57.) В противном случае выберите Client .

Таблица 56 Меню 2: настройка WAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Rate Adaption	Это поле доступно для настройки, если в поле Service Type указано значение Server . Нажмите пробел, чтобы разрешить устройству P-791R v2 согласовывать скорость соединения с другим устройством.
Transfer Max Rate(Kbps)	Это поле активно, если в поле Service Type выбрано значение Server . Нажмите пробел, чтобы указать максимальную скорость отправки и приема данных для P-791R v2. Если активирован режим Rate Adaption , P-791R v2 будет подстраиваться под скорость удаленного устройства и может превысить указанную скорость.
Transfer Min Rate(Kbps)	Это поле активно, если в поле Service Type выбрано значение Server . Нажмите пробел, чтобы указать минимальную скорость отправки и приема данных для P-791R v2. Если активирован режим Rate Adaption , P-791R v2 будет подстраиваться под скорость удаленного устройства и может передавать информацию на меньшей скорости.
Standard Mode	Это поле активно, если в поле Service Type выбрано значение Server . Нажмите пробел, чтобы выбрать режим, используемый P-791R v2 для организации DSL-соединения.
Wan Backup Setup	
Check Mechanism	Выберите метод, которым P-791R v2 будет проверять наличие DSL-соединения. Выберите DSL Link , чтобы устройство P-791R v2 проверяло наличие физического соединения с DSLAM. Выберите ICMP , чтобы периодически отправлять эхозапросы с P-791R v2 на IP-адреса, заданные в полях Check WAN IP Address .
Check WAN IP Address1 Check WAN IP Address2 Check WAN IP Address3	Это поле задает адреса, с помощью которых P-791R v2 будет проверять доступность WAN. Введите IP-адреса от одного до трех близкорасположенных надежных хостов (например, адрес DNS-сервера поставщика услуг). Примечание. Если вы активируете переадресацию трафика или резервирование через коммутируемый доступ, здесь необходимо указать по крайней мере один IP-адрес. При использовании резервирования WAN P-791R v2 периодически отправляет эхозапросы на указанные здесь адреса и при неполучении ответа переключается на резервное соединение с WAN (если оно настроено).
KeepAlive Fail Tolerance	Укажите число раз (рекомендуемое значение – 2), которое P-791R v2 может отправить эхозапросы на указанные в поле Check WAN IP Address IP-адреса без получения отклика, прежде чем переключится на резервное соединение с WAN (или на другой вид резервного соединения с WAN).
Recovery Interval(sec)	Когда P-791R v2 использует соединение с меньшим приоритетом (обычно – резервное соединение с WAN), устройство периодически проверяет возможность перехода на более приоритетное соединение. Введите длительность интервала в секундах (рекомендуется 30), выдерживаемого P-791R v2 между проверками доступности сети. Увеличьте интервал, если целевой IP-адрес обрабатывает много трафика.
ICMP Timeout(sec)	Введите число секунд (рекомендуется 3), в течение которого P-791R v2 будет ожидать отклика на один из эхозапросов, отправленных по указанным в поле Check WAN IP Address адресам, прежде чем запрос будет сочтен превысившим время ожидания. Соединение с WAN будет признано недоступным после того, как P-791R v2 обнаружит истечение времени ожидания указанное в поле Fail Tolerance число раз. Если ваша сеть занята или переполнена, введите в этом поле более высокое значение.

Таблица 56 Меню 2: настройка WAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Traffic Redirect	Выберите Yes , нажав пробел, затем нажмите [ENTER], чтобы активировать перенаправление трафика и отредактировать ее параметры.
Dial Backup	Выберите Yes , нажав пробел, затем нажмите [ENTER], чтобы активировать интерфейс резервирования через коммутируемый доступ и отредактировать его параметры.
После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в приглашении "Press ENTER to Confirm..." ("Нажмите ВВОД для подтверждения...") для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции в любой момент.	

19.2 Настройка перенаправления трафика

Находясь в главном меню, перейдите в меню 2 и выберите **Yes** в поле **Traffic Redirect**, затем нажмите [ENTER].

Рис. 96 Меню 2.1: настройка перенаправления трафика

<pre> Menu 2.1 - Traffic Redirect Setup Active= No Configuration: Backup Gateway IP Address= 0.0.0.0 Metric= 15 </pre>

Поля изображённого выше меню описаны в следующей таблице.

Таблица 57 Меню 2.1: настройка перенаправления трафика

ПОЛЕ	ОПИСАНИЕ
Active	Это поле включает (Yes) или отключает (No) функцию перенаправления трафика.
Configuration	
Backup Gateway IP Address	Введите IP-адрес резервного межсетевых шлюза в десятичном виде через точку. P-791R v2 автоматически переадресует трафик на этот IP-адрес, если разрывается соединение P-791R v2 с Интернетом.
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-791R v2. Метрика обозначает "стоимость" передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой "стоимостью". Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключённым сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже "стоимость".
После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в приглашении "Press ENTER to Confirm..." ("Нажмите ВВОД для подтверждения...") для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции в любой момент.	

19.3 Интерфейс резервирования через коммутируемый доступ

Перед использованием вспомогательного порта убедитесь, что переключатель установлен правильно, а порт подключен. Затем выполните настройку в следующих меню.

- 1 Меню 2 - настройка WAN
- 2 Меню 2.2 - настройка резервирования через коммутируемый доступ
- 3 Меню 2.2.1 - расширенная настройка резервирования через коммутируемый доступ
- 4 Меню 11.1 - профиль удаленного узла (узел 8, резервный поставщик услуг Интернета)

19.4 Настройка резервирования через коммутируемый доступ в меню 2

В главном меню введите 2 для открытия меню 2.

Рис. 97 Меню 2.2: настройка резервирования через коммутируемый доступ

```

2.2 - Dial Backup Setup

Dial-Backup:
  Active= No
  Port Speed= 115200

AT Command String:
  Init= at&fs0=0

Edit Advanced Setup= No

```

Поля изображённого выше меню описаны в следующей таблице.

Таблица 58 Меню 2.2: настройка резервирования через коммутируемый доступ

ПОЛЕ	ОПИСАНИЕ
Dial-Backup:	
Active	Это поле включает (Yes) или отключает (No) функцию резервирования через коммутируемый доступ.
Port Speed	Нажмите пробел и [ENTER], чтобы выбрать скорость соединения между портом резервирования через коммутируемый доступ и внешним устройством. Доступны следующие скорости: 9600, 19200, 38400, 57600, 115200 или 230400 бит/с.
AT Command String:	
Init	Введите AT-строку инициализации устройства, используемого для доступа в WAN. Описание конкретных AT-команд см. в документации на устройство, подключаемое к порту резервирования.

Таблица 58 Меню 2.2: настройка резервирования через коммутируемый доступ

ПОЛЕ	ОПИСАНИЕ
Edit Advanced Setup	Чтобы отредактировать расширенные параметры порта резервирования через коммутируемый доступ, подведите курсор к этому полю, нажмите пробел, чтобы выбрать Yes , затем нажмите [ENTER] для входа в раздел Menu 2.1 - Advanced Setup .
После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в приглашении "Press ENTER to Confirm..." ("Нажмите ВВОД для подтверждения...") для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции в любой момент.	

19.5 Расширенная настройка резервирования через коммутируемый доступ



Описание AT-команд устройства, подключаемого к порту резервирования, см. в документации на устройство.

Чтобы отредактировать расширенные параметры порта резервирования, подведите курсор к полю **Edit Advanced Setup** в разделе меню **Menu 2.2 - Dial Backup Setup**, нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER].

Рис. 98 Меню 2.2.1: расширенная настройка резервирования через коммутируемый доступ

Menu 2.2.1 - Advanced Dial Backup Setup	
AT Command Strings:	Call Control:
Dial= atd	Dial Timeout(sec)= 60
Drop= ~~~~~ath	Retry Count= 0
Answer= ata	Retry Interval(sec)= N/A
	Drop Timeout(sec)= 20
Drop DTR When Hang Up= No	Call Back Delay(sec)= 15
AT Response Strings:	
CLID= NMBR =	
Called Id=	
Speed= CONNECT	

Поля изображённого выше меню описаны в следующей таблице.

Таблица 59 Меню 2.2.1: расширенная настройка резервирования через коммутируемый доступ

ПОЛЕ	ОПИСАНИЕ
AT Command Strings:	
Dial	Введите AT-команду для осуществления вызова.

Таблица 59 Меню 2.2.1: расширенная настройка резервирования через коммутируемый доступ (продолжение)

ПОЛЕ	ОПИСАНИЕ
Drop	Введите AT-команду для завершения вызова. Символ “~” кодирует 1-секундную задержку. Например, для модемов с медленным откликом можно использовать строку “~~~+++~ath”.
Answer	Введите AT-команду для ответа на входящий вызов.
Drop DTR When Hang Up	Нажмите пробел, чтобы выбрать значение Yes (да) или No (нет). Когда выбрано значение Yes (действующее по умолчанию), после отправки строки “AT Command String: Drop” осуществляется сброс сигнала DTR.
AT Response Strings:	
CLID (идентификация вызывающей линии)	Введите ключевое слово, после которого в AT-строке отклика приводится CLID (идентификация вызывающей линии). Это позволяет P-791R v2 извлекать CLID из AT-строки доступа, полученной от устройства, через которое осуществляется доступ в WAN. Идентификатор CLID применяется для CLID-аутентификации.
Called Id	Введите ключевое слово, которое предшествует набираемому номеру.
Speed	Введите ключевое слово, которое предшествует скорости соединения.
Call Control	
Dial Timeout (sec)	Укажите число секунд, в течение которых P-791R v2 будет ожидать установления исходящего соединения перед прекращением операции. P-791R v2 сообщает об истечении времени ожидания и прекращает попытку установления исходящего соединения, если его не удалось установить за указанное время.
Retry Count	Укажите число повторных попыток набора номера, которые P-791R v2 будет предпринимать при обнаружении сигнала “занято” или при отсутствии ответа удаленной стороны, прежде чем номер будет занесен в черный список.
Retry Interval (sec)	Укажите продолжительность паузы (в секундах), которую P-791R v2 будет выдерживать между попытками повторного набора номера. Эта пауза действует до занесения номера в черный список.
Drop Timeout (sec)	Введите число секунд, по истечении которых P-791R v2 сбросит линию DTR, если не будет получено явное подтверждение разъединения.
Call Back Delay (sec)	Укажите длительность паузы (в секундах), которую P-791R v2 будет выдерживать между завершением запроса встречного вызова (callback) и началом соответствующего встречного вызова.

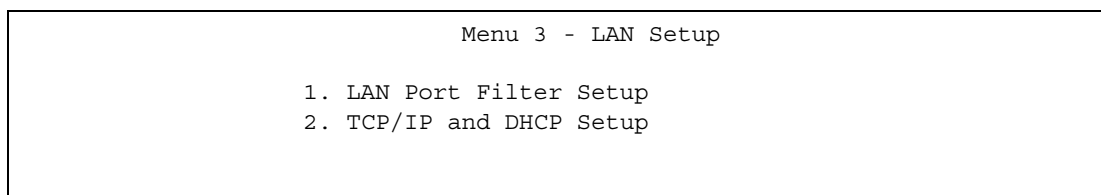
Настройка LAN

Этот раздел меню служит для применения фильтров LAN, настройки параметров DHCP и TCP/IP для сети LAN.

20.1 Вход в меню LAN

В главном меню введите цифру 3 для открытия **Menu 3 - LAN Setup**.

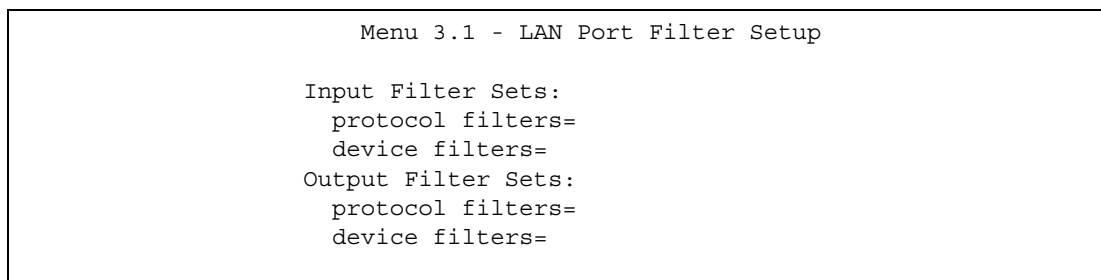
Рис. 99 Меню 3: настройка LAN



20.2 Меню LAN Port Filter Setup

Это меню позволяет указать наборы фильтров, применяемые к трафику в локальной сети. Необходимость фильтрации трафика в LAN возникает редко; однако наборы фильтров могут быть полезными для блокирования определенных пакетов, уменьшения объема трафика и укрепления системы безопасности.

Рис. 100 Меню 3.1: настройка фильтров для порта LAN



20.3 Меню TCP/IP and DHCP Setup

Находясь в основном меню, наберите цифру 3, чтобы войти в меню **Menu 3 - LAN Setup** для настройки параметров TCP/IP (RFC 1155) и DHCP. В меню 3 выберите подменю **TCP/IP and DHCP Setup** и нажмите [ENTER]. Появится экран **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**, показанный ниже. Доступные поля будут зависеть от модели устройства.

Рис. 101 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-2B
Multicast= IGMP-v2
IP Policies=
Edit IP Alias= No

```

Для настройки этих полей руководствуйтесь следующей таблицей.

Таблица 60 Меню 3.2: настройка TCP/IP и DHCP для Ethernet

ПОЛЕ	ОПИСАНИЕ
DHCP Setup	
DHCP	<p>Это поле позволяет включить/выключить DHCP-сервер.</p> <p>Если выбрано значение Server, P-791R v2 будет работать в режиме DHCP-сервера. Потребуется настроить остальные поля в этом разделе, за исключением Remote DHCP Server.</p> <p>При выборе значения Relay P-791R v2 действует как заменитель DHCP-сервера и выполняет обмен запросами и откликами между удаленным сервером и клиентами. В этом случае необходимо указать удаленный DHCP-сервер (Remote DHCP Server).</p> <p>При выборе значения None сервер будет выключен.</p>
Client IP Pool Starting Address	В этом поле указывается первый адрес в непрерывном пуле IP-адресов.
Size of Client IP Pool	В этом поле указывается размер или общая численность пула IP-адресов.

Таблица 60 Меню 3.2: настройка TCP/IP и DHCP для Ethernet (продолжение)

ПОЛЕ	ОПИСАНИЕ
Primary DNS Server Secondary DNS Server	<p>P-791R v2 сообщает IP-адреса DNS-серверов в указанном порядке DHCP-клиентам.</p> <p>Выберите From ISP, если поставщик услуг Интернета динамически назначает параметры DNS-сервера (а также IP-адрес P-791R v2 в сети WAN). В поле IP Address (IP-адрес) внизу отображается IP-адрес DNS-сервера (только для чтения), назначаемый оператором.</p> <p>Выберите User-Defined, если вам известен IP-адрес DNS-сервера. Введите IP-адрес DNS-сервера в поле IP Address внизу. Если выбрано значение User-Defined (Определяется пользователем), но значение IP-адреса остается равным 0.0.0.0, User-Defined (Определяется пользователем) заменяется значением None (Нет) после сохранения изменений. Если во втором случае выбрана опция User-Defined (Определяется пользователем) и введен тот же IP-адрес, вторая опция User-Defined (Определяется пользователем) приобретает значение None (Нет) после сохранения изменений.</p> <p>Выберите DNS Relay, чтобы использовать P-791R v2 в режиме прокси-сервера для DNS. IP-адрес P-791R v2 в сети LAN отображается в расположенном ниже поле IP Address (это поле недоступно для редактирования). P-791R v2 сообщает DHCP-клиентам в локальной сети, что само устройство P-791R v2 является DNS-сервером. Когда компьютер в локальной сети отправляет запрос DNS на P-791R v2, P-791R v2 переадресует запрос DNS-серверу, настроенному для P-791R v2 в меню 1, и возвращает отклик компьютеру. Режим DNS Relay можно выбрать только для одного из трех серверов; режим DNS Relay, выбранный для второго или третьего сервера, изменяется на None после сохранения изменений.</p> <p>Выберите None, если DNS-серверы настраивать не требуется. Если настройка DNS-сервера не выполняется, для получения доступа к машине необходимо знать ее IP-адрес.</p>
Remote DHCP Server	Если в поле DHCP выбран режим Relay , введите здесь IP-адрес фактического удаленного DHCP-сервера.
TCP/IP Setup:	
IP Address	Введите IP-адрес P-791R v2 в сети LAN в десятичном виде через точку.
IP Subnet Mask	P-791R v2 автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. Если вам не требуется деление на подсети, используйте маску подсети, рассчитанную P-791R v2.
RIP Direction	Нажмите пробел и [ENTER] для выбора направления RIP. Возможны следующие значения: Both (оба), In Only (только вход), Out Only (только выход) или None (нет).
Version	Нажмите пробел и [ENTER] для выбора версии RIP. Возможны следующие значения: RIP-1 , RIP-2B или RIP-2M .
Multicast	IGMP (Широковещательный протокол взаимодействия групп в Интернете) – протокол уровня сессии, используемый для установки членства в группе многоадресной рассылки. P-791R v2 поддерживает протокол IGMP версии 1 (IGMP-v1) и версии 2 (IGMP-v2). Нажмите пробел и [ENTER] для включения многоадресной IP-рассылки или выберите None (по умолчанию) для ее отключения.
IP Policies	Для данного удаленного узла могут применяться до четырех политик маршрутизации. Политики должны быть предварительно настроены в меню 25. Подробное описание политик маршрутизации см. в гл. 31 на стр. 277 .

Таблица 60 Меню 3.2: настройка TCP/IP и DHCP для Ethernet (продолжение)

ПОЛЕ	ОПИСАНИЕ
Edit IP Alias	P-791R v2 поддерживает до трех логических интерфейсов LAN на одном физическом интерфейсе Ethernet, при этом P-791R v2 будет выступать в качестве межсетевого шлюза для каждой сети LAN. Чтобы войти в меню 3.2.1, выберите Yes , нажав пробел, а затем нажмите [ENTER].
После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в приглашении [Press ENTER to Confirm...] ([Нажмите ВВОД для подтверждения...]) для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции в любой момент.	

20.4 Совмещение IP-адресов в локальной сети

Для настройки первой сети используется меню 3.2, настройка двух других сетей осуществляется в меню 3.2.1. Переместите курсор в поле **Edit IP Alias**, нажмите пробел для выбора значения **Yes** и клавишу [ENTER] для настройки второй и третьей сетей.

Рис. 102 Меню 3.2.1: настройка совмещения IP-адресов

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

Используйте инструкции в приведенной ниже таблице для настройки совмещения IP-адресов.

Таблица 61 Меню 3.2.1: настройка совмещения IP-адресов

ПОЛЕ	ОПИСАНИЕ
IP Alias 1, 2	Выберите Yes , чтобы настроить сеть LAN для P-791R v2.
IP Address	Введите IP-адрес вашего P-791R v2 в десятичном виде через точку.
IP Subnet Mask	P-791R v2 автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. Если вам не требуется деление на подсети, используйте маску подсети, рассчитанную P-791R v2.
RIP Direction	Нажмите пробел и [ENTER] для выбора направления RIP. Возможны следующие значения: Both (оба), In Only (только вход), Out Only (только выход) или None (нет).

Таблица 61 Меню 3.2.1: настройка совмещения IP-адресов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Version	Нажмите пробел и [ENTER] для выбора версии RIP. Возможны следующие значения: RIP-1, RIP-2B или RIP-2M .
Incoming protocol filters	Укажите наборы фильтров, применяемые ко входящему трафику между данным узлом и P-791R v2.
Outgoing protocol filters	Укажите наборы фильтров, применяемые к исходящему трафику между данным узлом и P-791R v2.
После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в приглашении [Press ENTER to Confirm...] ([Нажмите ВВОД для подтверждения...]) для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции в любой момент.	

Настройка доступа к Интернету

Это меню служит для настройки подключения к Интернету. Чтобы настроить доступ к Интернету в P-791R v2, используйте информацию, полученную от поставщика услуг Интернета, а также указания, приведенные в этой главе. Обращайтесь к своему оператору, чтобы определить, какой тип инкапсуляции следует использовать.

21.1 Настройка доступа к Интернету

Введите 4 в главном меню.

Рис. 103 Меню 4: настройка доступа к Интернету

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 0
VCI #= 33
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= 0.0.0.0
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

```

Поля изображённого выше меню описаны в следующей таблице.

Таблица 62 Меню 4: настройка доступа к Интернету

ПОЛЕ	ОПИСАНИЕ
ISPfs Name	Введите описательное название поставщика услуг Интернета, позволяющее его идентифицировать.
Encapsulation	Нажмите пробел и [ENTER], чтобы выбрать тип инкапсуляции, используемый поставщиком услуг Интернета.

Таблица 62 Меню 4: настройка доступа к Интернету (продолжение)

ПОЛЕ	ОПИСАНИЕ
Multiplexing	Нажмите пробел, чтобы выбрать метод мультиплексирования, используемый поставщиком услуг Интернета. Возможны два варианта: мультиплексирование на основе виртуальных каналов (VC-based) или на основе логического канала связи (LLC-based).
VPI	Совокупность VPI (идентификатора виртуального пути) и VCI (идентификатора виртуального канала) определяет виртуальную цепь. Допустимый диапазон значений VPI – от 0 до 255. Введите присвоенный вам VPI.
VCI	Допустимый диапазон значений VCI – от 32 до 65535 (диапазон от 0 до 31 зарезервирован для локального управления трафиком ATM). Введите присвоенный вам VCI.
ATM QoS Type	Выберите CBR (постоянная битовая скорость), если нужно задать фиксированную полосу пропускания для передачи голоса или данных. Выберите UBR (незаданная скорость передачи), если изменение скорости передачи со временем не имеет большого значения, например, в случае электронной почты. Для пульсирующего трафика с совместным использованием полосы пропускания другими приложениями выберите VBR (переменная битовая скорость).
Peak Cell Rate (PCR)	Разделите скорость DSL-линии (бит/с) на 424 (размер ATM-ячейки). Получится пиковая скорость передачи ячеек (PCR). Полученное значение будет соответствовать максимальной скорости отправки ячеек отправителем. Введите значение PCR в этом поле.
Sustain Cell Rate (SCR)	Средняя скорость передачи ячеек (Sustained Cell Rate, SCR) – средняя скорость передачи ячеек (усреднение выполняется на большом промежутке времени). Введите SCR (значение SCR должно быть меньше PCR). Необходимо помнить, что по умолчанию система использует значение 0 ячеек в секунду.
Maximum Burst Size (MBS)	Максимальный размер пульсации (Maximum Burst Size, MBS) – это максимальное число ячеек, при отправке которого будет соблюдаться PCR. Введите MBS (меньше 65535).
My Login	(Только для PPPoE и PPPoA) Введите имя пользователя, полученное от поставщика услуг Интернета.
My Password	(Только для PPPoE и PPPoA) Введите свой пароль, полученный от поставщика услуг Интернета.
ENET ENCAP Gateway	(Только для инкапсуляции ENET ENCAP) Введите IP-адрес шлюза, предоставленный поставщиком услуг Интернета.
Idle Timeout (sec)	(Только для PPPoE и PPPoA) Укажите период неактивности соединения. Значение по умолчанию – 0, при котором сеанс соединения с Интернетом не завершается никогда.
IP Address Assignment	Если оператор не назначил фиксированный IP-адрес, нажмите пробел и [ENTER] для выбора значения Dynamic (динамический), в противном случае выберите значение Static (статический) и введите IP-адрес и маску подсети в следующих полях.
IP Address	Это поле доступно в том случае, если в поле IP Address Assignment выбрано значение Static . Введите (фиксированный) IP-адрес, назначенный оператором (назначение статического IP-адреса выбирается в предыдущем поле).

Таблица 62 Меню 4: настройка доступа к Интернету (продолжение)

ПОЛЕ	ОПИСАНИЕ
Network Address Translation	<p>Трансляция сетевых адресов (NAT) обеспечивает преобразование IP-адреса, используемого в пределах одной сети (например, частного IP-адреса, используемого в локальной сети) в другой IP-адрес, известный в пределах другой сети (например, открытый IP-адрес, используемый в Интернете). Выберите None (Нет), чтобы отключить NAT.</p> <p>Выберите SUA Only (Только SUA), если существует 1 общедоступный IP-адрес. SUA (Учетная запись одного пользователя) является подмножеством NAT, поддерживающим 2 типа привязки: Many-to-One (Множество – один) и Server (Сервер).</p> <p>Выберите Full Feature (Полный набор возможностей), если существует несколько общедоступных IP-адресов. Типы привязки Full Feature (Полный набор возможностей) включают: One-to-One (Один – один), Many-to-One (Множество – один) (SUA/PAT), Many-to-Many Overload (Перегрузка множество – множество), Many- One-to-One (Множество – один – один) и Server (Сервер). При выборе опции Full Feature необходимо настроить как минимум один набор привязки адресов.</p> <p>Подробное описание функции трансляции сетевых адресов см. в гл. 7 на стр. 99.</p>
Address Mapping Set	<p>Это поле доступно в том случае, если в поле Network Address Translation выбрано значение Full Feature.</p> <p>Введите номер набора привязки адресов, который требуется использовать для данного соединения с Интернетом.</p>
<p>После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в приглашении "Press ENTER to Confirm..." ("Нажмите ВВОД для подтверждения...") для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции в любой момент.</p>	

Настройка удаленного узла

Это меню используется для детальной настройки параметров удаленного узла (которым может являться ваш поставщик услуг Интернета), а также для применения фильтров.

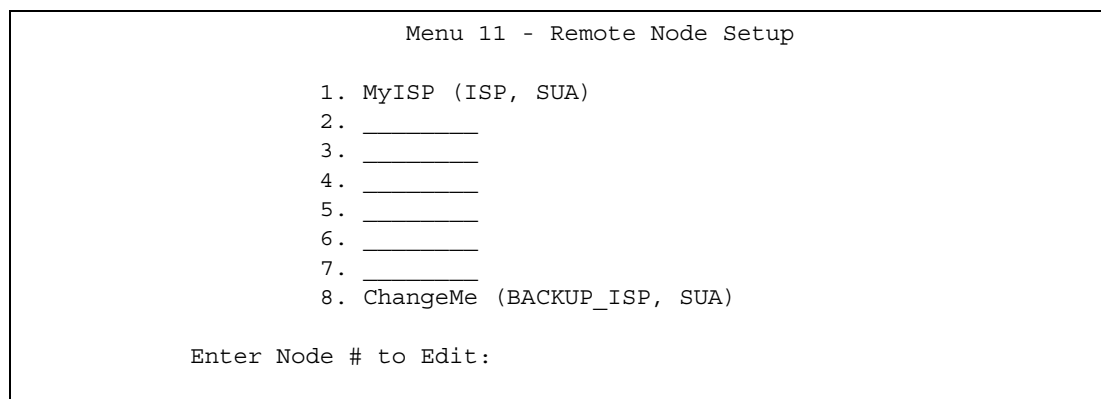
22.1 Введение в настройку удаленного узла

Удаленный узел требуется для размещения вызовов на удаленном межсетевом шлюзе. Удаленный узел представляет собой как удаленный межсетевой шлюз, так и сеть, находящуюся за ним в соединении WAN. Обратите внимание на то, что при использовании меню 4 для настройки доступа к Интернету фактически выполняется настройка удаленного узла.

22.2 Настройка удаленного узла

В главном меню выберите пункт 11, чтобы перейти в раздел **Menu 11 - Remote Node Setup** (как показано ниже).

Рис. 104 Меню 11: Remote Node Setup



Введите номер правила, которое вы хотите настроить, и нажмите [ENTER].

22.3 Профиль удаленного узла

Настройка удаленных узлов 1 – 7 описана ниже.

Рис. 105 Меню 11.1: профиль удаленного узла (узлы 1 – 7)

```

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= No
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
    
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 63 Меню 11.1: профиль удаленного узла (узлы 1 – 7)

ПОЛЕ	ОПИСАНИЕ
Rem Node Name	Введите название поставщика услуг Интернета.
Active	Укажите, используется ли данное соединение с Интернетом.
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета.
Multiplexing	Выберите тип мультиплексирования, используемый поставщиком услуг Интернета, из раскрывающегося списка. Варианты выбора: VC или LLC .
Service Name	(Только для инкапсуляции PPPoE) Введите название службы, предоставленное поставщиком услуг Интернета. Если поставщик услуг Интернета не предоставил соответствующей информации, оставьте это поле пустым.
входящих вызовов	Этот раздел доступен только для инкапсуляции PPPoA / PPPoE.
Rem Login	Введите имя пользователя, которое будет использоваться дистанционным узлом при вызове вашего устройства P-791R v2. Для аутентификации узла будут использоваться указанное имя пользователя и пароль из поля Rem Password .
Rem Password	Введите пароль, который будет использоваться дистанционным узлом при вызове вашего устройства P-791R v2.
исходящих вызовов	Этот раздел доступен только для инкапсуляции PPPoA / PPPoE.
My Login	Введите имя пользователя, предоставленное поставщиком услуг Интернета.
My Password	Введите пароль, предоставленный поставщиком услуг Интернета.
Retype to Confirm	Введите пароль повторно.
Authen	Это поле доступно в том случае, если в поле Encapsulation выбран режим инкапсуляции PPPoE . Выберите тип аутентификации, используемый поставщиком услуг Интернета. Чтобы разрешить P-791R v2 использовать оба варианта аутентификации, выберите CHAP/PAP .

Таблица 63 Меню 11.1: профиль удаленного узла (узлы 1 – 7) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Route	<p>Нажмите пробел и [ENTER], чтобы выбрать параметр IP, разрешающий IP-маршрутизацию через данный удаленный узел. Этот параметр становится действителен только после того, как в устройстве P-791R v2 также будет активирована IP-маршрутизация. См. Меню 1: общая настройка в разд. 18.1 на стр. 175.</p> <p>На этом экране необходимо включить Route IP, Bridge или оба режима. Если режимы Route IP и Bridge отключены, устройство не будет пересылать трафик между портами LAN и удаленным узлом.</p>
Bridge	<p>Если для параметра Route выбрано значение IP, выберите в этом поле Yes, чтобы установить мост с этим удаленным узлом для протоколов, не поддерживаемых IP-маршрутизацией (например, SNA).</p> <p>Если для параметра Route выбрано значение None, выберите в этом поле Yes, чтобы установить мост с этим удаленным узлом для всех протоколов.</p> <p>Во всех случаях этот параметр становится действителен только после того, как в устройстве P-791R v2 также будет активирован мост. См. Меню 1: общая настройка в разд. 18.1 на стр. 175.</p> <p>На этом экране необходимо включить Route IP, Bridge или оба режима. Если режимы Route IP и Bridge отключены, устройство не будет пересылать трафик между портами LAN и удаленным узлом.</p>
Edit IP/Bridge	<p>Это поле доступно в том случае, если параметр Route установлен в значение IP. Для задания IP-адреса в сети WAN и дополнительных параметров порта WAN нажмите пробел, чтобы выбрать Yes, затем нажмите [ENTER]. Появится меню 11,3.</p>
Edit ATM Options	<p>Это поле доступно в том случае, если параметр Route установлен в значение IP. Для редактирования параметров виртуального канала и ATM QoS нажмите пробел, чтобы выбрать Yes, затем нажмите [ENTER]. Появится меню 11,6.</p>
Edit Advance Options	<p>Это поле отображается при редактировании удаленного узла 1 и доступно только для соединений PPPoE. Для задания дополнительных параметров подключения к Интернету нажмите пробел, чтобы выбрать Yes, затем нажмите [ENTER]. Появится меню 11,8.</p>
Telco Option	<p>Этот раздел доступен только для инкапсуляции PPPoA / PPPoE.</p>
Allocated Budget(min)	<p>Введите максимальную продолжительность каждого вызова (в минутах). Чтобы снять ограничение на продолжительность вызова, введите 0. Поле Period позволяет ограничить суммарную продолжительность исходящего вызова с P-791R v2. Если общее время исходящих вызовов превышает лимит, текущий вызов отбрасывается, и все последующие исходящие вызовы блокируются.</p>
Period(hr)	<p>Введите количество часов, по истечении которого параметр Allocated Budget будет сбрасываться. Например, если в течение каждого часа под исходящие вызовы выделяется 30 минут, установите параметр Allocated Budget равным 30, а в этом поле введите 1.</p>
Schedule Sets	<p>Введите наборы расписаний, действующие для данного соединения.</p>
Nailed-Up Connection	<p>Выберите этот флажок, чтобы автоматически соединять P-791R v2 с поставщиком услуг Интернета при включении питания и никогда не разрывать соединение. Не рекомендуется использовать этот режим, если у поставщика услуг Интернета действует повременная оплата.</p>
Session Options	

Таблица 63 Меню 11.1: профиль удаленного узла (узлы 1 – 7) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Edit Filter Sets	Для задания дополнительных наборов входных и выходных фильтров на порту WAN нажмите пробел, чтобы выбрать Yes , затем нажмите [ENTER]. Появится меню 11,5.
Idle Timeout (sec)	Введите число секунд, по истечении которых P-791R v2 отключается от поставщика услуг Интернета, если за это время трафик отсутствовал. Допустимые интервалы – от 10 до 9999 секунд.

Ниже описана настройка удаленного узла 8 для резервирования соединения по коммутируемой линии.

Рис. 106 Меню 11.1: профиль удаленного узла (узел 8)

Menu 11.1 - Remote Node Profile (Backup ISP)	
Rem Node Name= ?	Edit PPP Options= No
Active= Yes	Rem IP Addr= ?
	Edit IP= No
Outgoing:	Edit Script Options= No
My Login=	
My Password= *****	Telco Option:
Authen= CHAP/PAP	Allocated Budget (min)= 0
Pri Phone #= ?	Period(hr)= 0
Sec Phone #=	Nailed-Up Connection= No
	Session Options:
	Edit Filter Sets= No
	Idle Timeout(sec)= 100

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 64 Меню 11.1: профиль удаленного узла (узел 8)

ПОЛЕ	ОПИСАНИЕ
Rem Node Name	Введите название поставщика услуг Интернета.
Active	Укажите, используется ли данное соединение с Интернетом.
Outgoing	Этот раздел доступен только для инкапсуляции PPPoA / PPPoE.
My Login	Введите имя пользователя, предоставленное поставщиком услуг Интернета.
My Password	Введите пароль, предоставленный поставщиком услуг Интернета.
Retype to Confirm	Введите пароль повторно.
Authen	Это поле доступно в том случае, если в поле Encapsulation выбран режим инкапсуляции PPPoE . Выберите тип аутентификации, используемый поставщиком услуг Интернета. Чтобы разрешить P-791R v2 использовать оба варианта аутентификации, выберите CHAP/PAP .
Pri Phone # Sec Phone #	Введите один или два телефонных номера удаленного узла. В тех случаях, когда основной номер (Primary Phone) занят или не отвечает, P-791R v2 набирает запасной номер (Secondary Phone), если он указан. В некоторых телефонных сетях для вызова местных номеров перед ними необходимо набирать решетку (#). В этом случае перед номером нужно указать знак #.

Таблица 64 Меню 11.1: профиль удаленного узла (узел 8) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Edit PPP Options	Для редактирования параметров PPP резервного поставщика услуг Интернета нажмите пробел, чтобы выбрать Yes , затем нажмите [ENTER]. Появится меню 11,2.
Rem IP Addr	В этом поле отображается тип маршрутизации, используемый устройством P-791R v2.
Edit IP/Bridge	Это поле доступно в том случае, если параметр Route установлен в значение IP . Для задания IP-адреса в сети WAN и дополнительных параметров порта WAN нажмите пробел, чтобы выбрать Yes , затем нажмите [ENTER]. Появится меню 11,3.
Edit ATM Options	Это поле доступно в том случае, если параметр Route установлен в значение IP . Для редактирования параметров виртуального канала и ATM QoS нажмите пробел, чтобы выбрать Yes , затем нажмите [ENTER]. Появится меню 11,6.
Edit Advance Options	Это поле отображается при редактировании удаленного узла 1 и доступно только для соединений PPPoE. Для задания дополнительных параметров подключения к Интернету нажмите пробел, чтобы выбрать Yes , затем нажмите [ENTER]. Появится меню 11,8.
Telco Option	Этот раздел доступен только для инкапсуляции PPPoA / PPPoE.
Allocated Budget(min)	Введите максимальную продолжительность каждого вызова (в минутах). Чтобы снять ограничение на продолжительность вызова, введите 0. Поле Period позволяет ограничить суммарную продолжительность исходящего вызова с P-791R v2. Если общее время исходящих вызовов превышает лимит, текущий вызов отбрасывается, и все последующие исходящие вызовы блокируются.
Period(hr)	Введите количество часов, по истечении которого параметр Allocated Budget будет сбрасываться. Например, если в течение каждого часа под исходящие вызовы выделяется 30 минут, установите параметр Allocated Budget равным 30, а в этом поле введите 1.
Schedule Sets	Введите наборы расписаний, действующие для данного соединения.
Nailed-Up Connection	Выберите этот флажок, чтобы автоматически соединять P-791R v2 с поставщиком услуг Интернета при включении питания и никогда не разрывать соединение. Не рекомендуется использовать этот режим, если у поставщика услуг Интернета действует повременная оплата.
Session Options	
Edit Filter Sets	Для задания дополнительных наборов входных и выходных фильтров на порту WAN нажмите пробел, чтобы выбрать Yes , затем нажмите [ENTER]. Появится меню 11,5.
Idle Timeout (sec)	Введите число секунд, по истечении которых P-791R v2 отключается от поставщика услуг Интернета, если за это время трафик отсутствовал. Допустимые интервалы – от 10 до 9999 секунд.

22.4 Опции сетевого уровня удаленного узла

Переместите курсор в поле **Edit IP (Редактировать IP)** в меню 11.1, затем нажмите клавишу [SPACE BAR] ([ПРОБЕЛ]) для выбора значения **Yes (Да)**. Нажмите клавишу [ENTER] для открытия раздела **Menu 11.3 - Remote Node Network Layer Options**.

Рис. 107 Меню 11.3: опции сетевого уровня удаленного узла

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:
  IP Address Assignment = Static
  Rem IP Addr = 192.168.2.2
  Rem Subnet Mask= 255.255.255.0
  My WAN Addr= 192.168.2.1
  NAT= SUA Only
  Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= None
  Version= RIP-1
  Multicast= None
  IP Policies=

Bridge Options:
  Ethernet Addr Timeout (min)= N/A

```

Поля изображённого выше меню описаны в следующей таблице.

Таблица 65 Меню 11.3: параметры сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ
IP Address Assignment	Если поставщик услуг Интернета не присвоил вам фиксированный (статический) IP-адрес, выберите Dynamic . Если поставщик услуг Интернета выделил вам фиксированный (статический) IP-адрес, выберите Static . Следующие три поля недоступны, если был выбран динамический адрес (Dynamic).
	Эти поля появляются, если в меню 11 для параметра Encapsulation выбрано значение Ethernet .
Rem IP Address	Если оператором назначен статический IP-адрес, введите его.
Rem IP Subnet Mask	Если назначен статический IP-адрес, введите назначенную маску подсети.
My WAN Addr	Введите фиксированный (статический) IP-адрес, предоставленный поставщиком услуг Интернета.
NAT	Если не предполагается использовать переадресацию портов, триггерные порты или NAT, выберите None . Если вы планируете использовать некоторые из этих функций, но для P-791R v2 выделен только один глобальный IP-адрес в сети WAN, выберите SUA Only . Если вы планируете использовать некоторые из этих функций, и для P-791R v2 выделено несколько глобальных IP-адресов в сети WAN, выберите Full Feature .
Address Mapping Set	Это поле доступно в том случае, если параметр NAT установлен в значение Full Feature . Укажите набор привязки адресов, который должен использоваться для этого удаленного узла.
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-791R v2. Метрика обозначает "стоимость" передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой "стоимостью". Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключённым сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже "стоимость".

Таблица 65 Меню 11.3: параметры сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ
Private	Это поле используется протоколом RIP. Это поле указывает, будет ли P-791R v2 включать данный маршрут к конкретному удаленному узлу в широковещательную рассылку RIP. Если выбрано Yes , маршрут не включается в широковещательную рассылку RIP. Если выбрано No , маршрут к данному удаленному узлу сообщается другим хостам в широковещательных рассылках RIP. Обычно для этого поля будет приемлемым значение по умолчанию.
RIP Direction	Это поле определяет состав сведений о маршрутизации, принимаемых и отправляемых P-791R v2 по данному соединению. None - P-791R v2 не отправляет и не принимает сведения о маршрутизации по данному соединению. Both - P-791R v2 отправляет и принимает сведения о маршрутизации по данному соединению. In Only - P-791R v2 использует данное соединение только для приема сведений о маршрутизации. Out Only - P-791R v2 использует данное соединение только для отправки сведений о маршрутизации.
Version	Выберите версию протокола RIP, используемую P-791R v2 при отправке или приеме сведений о подсети. RIP-1 - P-791R v2 для обмена сведениями о маршрутизации использует RIPv1. RIP-2B - P-791R v2 для обмена сведениями о маршрутизации использует широковещательные сообщения RIPv2. RIP-2M - P-791R v2 для обмена сведениями о маршрутизации использует многоадресные сообщения RIPv2.
Multicast	Для использования RIP-2M включить многоадресную рассылку не требуется. (См. описание параметра RIP Version .) Выберите версию протокола IGMP, используемую P-791R v2 для реализации многоадресной рассылки на данном порту. При многоадресной рассылке пакеты отправляются только определенной группе компьютеров, что отличает этот способ от одноадресной (отправка пакетов на один компьютер) и широковещательной (отправка пакетов всем компьютерам) рассылки. None - P-791R v2 не поддерживает многоадресную рассылку. IGMP-v1 - P-791R v2 поддерживает IGMP версии 1. IGMP-v2 - P-791R v2 поддерживает IGMP версии 2. Многоадресная рассылка может улучшить общую производительность сети ценой большей вычислительной нагрузки и повышенного объема трафика. Кроме того, используемая версия IGMP должна поддерживаться всеми компьютерами в сети.
IP Policies	Для данного удаленного узла могут применяться до четырех политик маршрутизации. Политики должны быть предварительно настроены в меню 25. Подробное описание политик маршрутизации см. в гл. 31 на стр. 277 .
Bridge Options	

Таблица 65 Меню 11.3: параметры сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ
Ethernet Addr Timeout(min)	Это поле доступно в том случае, если в SMT (Меню 11.1: профиль удаленного узла (узлы 1 – 7)) параметр Bridge установлен в значение Yes . Введите интервал времени (в минутах), в течение которого P-791R v2 будет сохранять информацию об Ethernet-адресах в собственных внутренних таблицах после разъединения линии. Наличие этой информации поможет избежать необходимости повторного составления таблиц в P-791R v2 после восстановления соединения.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm...", чтобы сохранить настройки и вернуться в меню 11.1, либо нажмите клавишу [ESC] для отмены операции в любой момент.	

22.5 Фильтр удаленного узла.

В меню 11.1 переместите курсор в поле **Edit Filter Sets** и нажмите пробел, чтобы установить значение **Yes**. Нажмите клавишу [ENTER] ([BВОД]) для открытия **Menu 11.5 - Remote Node Filter (Меню 11.5 – Фильтр удаленного узла)**.

Это меню позволяет задать набор(ы) фильтров, применяемых к входящему и исходящему трафику между данным удаленным узлом и P-791R v2 для предотвращения исходящих вызовов при поступлении определенных типов пакетов. Можно указать до 4 наборов фильтров, отделенных запятыми, например, 1, 5, 9, 12, в каждом поле фильтра. Обратите внимание на то, что в этом поле применяются пробелы. [Гл. 25 на стр. 227](#) содержит подробное описание настройки фильтров. Для выполнения инкапсуляции PPPoE или PPTP существует дополнительная опция указания наборов фильтров для вызовов удаленных узлов.

Рис. 108 Меню 11.5: фильтр удаленного узла.

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=

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 66 Меню 11.5: фильтр удаленного узла

ПОЛЕ	ОПИСАНИЕ
Input Filter Sets (фильтры входящих пакетов)	
Protocol filters	Введите наборы фильтров (не более четырех). Чтобы ввести несколько наборов, перечислите их через запятую (,).

Таблица 66 Меню 11.5: фильтр удаленного узла (продолжение)

ПОЛЕ	ОПИСАНИЕ
Device filters	Введите наборы фильтров (не более четырех). Чтобы ввести несколько наборов, перечислите их через запятую (,).
Output Filter Sets (фильтры исходящих пакетов)	
Protocol filters	Введите наборы фильтров (не более четырех). Чтобы ввести несколько наборов, перечислите их через запятую (,).
Device filters	Введите наборы фильтров (не более четырех). Чтобы ввести несколько наборов, перечислите их через запятую (,).
Call Filter Sets (фильтры пакетов, инициирующих вызов)	Эти поля появляются, если в меню 11.1 для параметра Encapsulation выбрано значение PPPoA или PPPoE .
Protocol filters	Введите наборы фильтров (не более четырех). Чтобы ввести несколько наборов, перечислите их через запятую (,).
Device filters	Введите наборы фильтров (не более четырех). Чтобы ввести несколько наборов, перечислите их через запятую (,).

22.6 Параметры уровня ATM для удаленного узла

Переместите курсор в поле **Edit ATM Options** в меню 11.1 и нажмите пробел, чтобы выбрать **Yes**. Нажмите [ENTER] для входа в меню. Содержание меню зависит от параметров мультиплексирования и инкапсуляции, выбранных в меню 11.1.

Рис. 109 Меню 11.6: параметры уровня ATM для удаленного узла

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

Поля изображённого выше меню описаны в следующей таблице.

Таблица 67 Меню 11.6: параметры уровня ATM для удаленного узла

ПОЛЕ	ОПИСАНИЕ
VPI	Допустимый диапазон значений VPI – от 0 до 255. Введите присвоенный вам VPI.
VCI	Допустимый диапазон значений VCI – от 32 до 65535 (диапазон от 0 до 31 зарезервирован для локального управления трафиком ATM). Введите присвоенный вам VCI.

Таблица 67 Меню 11.6: параметры уровня ATM для удаленного узла (продолжение)

ПОЛЕ	ОПИСАНИЕ
ATM QoS Type	Выберите CBR (постоянная битовая скорость), если нужно задать фиксированную полосу пропускания для передачи голоса или данных. Выберите UBR (незаданная скорость передачи), если изменение скорости передачи со временем не имеет большого значения, например, в случае электронной почты. Для пульсирующего трафика с совместным использованием полосы пропускания другими приложениями выберите VBR (переменная битовая скорость).
Peak Cell Rate (PCR)	Разделите скорость DSL-линии (бит/с) на 424 (размер ATM-ячейки). Получится пиковая скорость передачи ячеек (PCR). Полученное значение будет соответствовать максимальной скорости передачи ячеек отправителем. Введите значение PCR в этом поле.
Sustain Cell Rate (SCR)	Средняя скорость передачи ячеек (Sustained Cell Rate, SCR) – средняя скорость передачи ячеек (усреднение выполняется на большом промежутке времени). Введите SCR (значение SCR должно быть меньше PCR). Необходимо помнить, что по умолчанию система использует значение 0 ячеек в секунду.
Maximum Burst Size (MBS)	Максимальный размер пульсации (Maximum Burst Size, MBS) – это максимальное число ячеек, при отправке которого будет соблюдаться PCR. Введите MBS (меньше 65535).
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm...", чтобы сохранить настройки и вернуться в меню 11.1, либо нажмите клавишу [ESC] для отмены операции в любой момент.	

22.7 Специальные параметры настройки

В меню 11.1 (только для удаленного узла 1) подведите курсор к полю **Edit Advance Options** и нажмите пробел, чтобы выбрать **Yes**. Нажмите [ENTER] для входа в раздел **Menu 11.8 - Advanced Setup Options** (специальные параметры настройки).

Рис. 110 Меню 11.8: специальные параметры настройки

Menu 11.8 - Advance Setup Options
PPPoE pass-through= No

Поля изображённого выше меню описаны в следующей таблице.

Таблица 68 Меню 11.8: специальные параметры настройки

ПОЛЕ	ОПИСАНИЕ
PPPoE pass-through	<p>В дополнение к встроенному в устройство ZyXEL PPPoE-клиенту можно включить режим сквозного прохождения PPPoE, чтобы разрешить использование PPPoE-клиентов на хостах в локальной сети для соединения с поставщиком услуг Интернета через устройство ZyXEL. Каждый хост может иметь отдельную учетную запись и глобальный IP-адрес на стороне WAN.</p> <p>Сквозной режим PPPoE – альтернатива NAT для тех применений, где использование NAT невозможно.</p> <p>Отключите сквозной режим PPPoE, чтобы запретить хостам в локальной сети с помощью программных клиентов PPPoE соединяться с поставщиком услуг Интернета.</p>
<p>После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm...", чтобы сохранить настройки и вернуться в меню 11.1, либо нажмите клавишу [ESC] для отмены операции в любой момент.</p>	

Настройка статического маршрута

Это меню служит для настройки статических маршрутов IP и статических маршрутов моста (на уровне MAC).

23.1 Настройка статического IP-маршрута

Находясь в меню 12, введите 1. Для настройки статических маршрутов IP в меню 12.1 выберите один из статических маршрутов, перечисленных ниже.

Рис. 111 Меню 12.1: настройка статического IP-маршрута

```
Menu 12.1 - IP Static Route Setup

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
```

Введите номер статического маршрута, который необходимо настроить.

Рис. 112 Меню 12.1.1: редактирование статического IP-маршрута

```

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

```

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 69 Меню 12.1.1: редактирование статического маршрута IP

ПОЛЕ	ОПИСАНИЕ
Route #	Это – порядковый номер статического маршрута, выбранного в меню 12.
Route Name	Введите описательное имя для данного маршрута. Оно служит только для идентификации.
Active	Это поле позволяет активировать/деактивировать данный статический маршрут.
Destination IP Address	Этот параметр указывает IP-адрес конечной точки маршрута. Маршрутизация всегда подразумевает диапазон сетевых адресов. Если требуется указать маршрут до отдельного хоста, в поле "IP Subnet Mask" введите маску подсети 255.255.255.255 – при этом диапазон сетевых адресов будет ограничен до адреса хоста.
IP Subnet Mask	Введите маску подсети для места назначения данного маршрута.
Gateway IP Address	Введите IP-адрес интернет-центра. Шлюз – это непосредственно соседствующая с P-791R v2 система, которая направляет пакет к месту назначения. В сети LAN шлюз должен быть маршрутизатором, находящимся в одном сегменте с P-791R v2; в WAN шлюз должен иметь IP-адрес одного из удаленных узлов.
Metric	Введите число от 1 до 15, определяющее приоритет данного маршрута в наборе маршрутов P-791R v2 (см. разд. 5.2 на стр. 66). Чем выше число, тем выше приоритет маршрута.
Private	Этот параметр определяет, будет ли P-791R v2 включать данный маршрут к удаленному узлу в свою широковещательную рассылку RIP. При установке значения Yes (Да) этот маршрут является частным и не включается в широковещательную рассылку RIP. При выборе значения No (Нет) маршрут к данному удаленному узлу распространяется на другие хосты через широковещательную рассылку RIP.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel", чтобы сохранить настройки, либо клавишу [ESC] для отмены.	

23.2 Настройка статического маршрута в режиме моста

Находясь в меню 12.3, введите 3. Для настройки статических маршрутов в меню 12.3 выберите один из маршрутов, перечисленных ниже.

Рис. 113 Меню 12.3: настройка статического маршрута в режиме моста

```

Menu 12.3 - Bridge Static Route Setup

1. _____
2. _____
3. _____
4. _____

```

Введите номер статического маршрута, который необходимо настроить.

Рис. 114 Меню 12.3.1: редактирование статического маршрута моста

```

Menu 12.3.1 - Edit Bridge Static Route

Route #: 1
Route Name= ?
Active= No
Ether Address= ?
IP Address=
Gateway Node= 1

```

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 70 Меню 12.3.1: редактирование статического маршрута моста

ПОЛЕ	ОПИСАНИЕ
Route #	Это – порядковый номер статического маршрута, выбранного в меню 12.
Route Name	Введите описательное имя для данного маршрута. Оно служит только для идентификации.
Active	Это поле позволяет активировать/деактивировать данный статический маршрут.
Ether Address	Этот параметр указывает MAC-адрес конечной точки маршрута.
IP Address	Введите IP-адрес интернет-центра. Шлюз – это непосредственно соседствующая с P-791R v2 система, которая направляет пакет к месту назначения. В сети LAN шлюз должен быть маршрутизатором, находящимся в одном сегменте с P-791R v2; в WAN шлюз должен иметь IP-адрес одного из удаленных узлов.
Gateway Node	Нажмите пробел и [ENTER], чтобы выбрать номер удаленного узла, являющегося шлюзом для данного статического маршрута.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel", чтобы сохранить настройки, либо клавишу [ESC] для отмены.	

Настройка NAT

Этот экран позволяет настроить параметры трансляции сетевых адресов (NAT) в P-791R v2.

24.1 Использование NAT

24.1.1 Сравнение SUA и других режимов NAT

SUA (Учетная запись отдельного пользователя) является подмножеством ZyNOS NAT и поддерживает два типа привязки - **Many-to-One ("Множество-один")** и **Server (Сервер)**. Подробное описание настройки NAT для SUA см. в [разд. 24.2.1 на стр. 213](#). P-791R v2 также поддерживает полноценный режим NAT (**Full Feature**), в котором несколько глобальных IP-адресов привязываются к нескольким IP-адресам клиентов или серверов в частных сетях LAN одним из нескольких способов.



Если для P-791R v2 выделен только один глобальный IP-адрес в сети WAN, выберите **SUA Only**.



Если для P-791R v2 выделено несколько глобальных IP-адресов в сети WAN, выберите **Full Feature**.

24.1.2 Применение NAT

NAT применяется через меню 4 или 11.3, как показано ниже. На рисунке внизу показано, как применять NAT для доступа к Интернету в меню 4. Введите 4 в главном меню для перехода в раздел **Menu 4 - Internet Access Setup**.

Рис. 115 Меню 4: применение NAT для доступа к Интернету

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 0
VCI #= 33
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= 0.0.0.0
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

```

На следующем рисунке показано, как применять NAT к удаленному узлу в меню 11.3.

- 1 Введите 11 в главном меню.
- 2 Введите 1, чтобы войти в раздел **Menu 11.1 - Remote Node Profile**.
- 3 Подведите курсор к полю **Edit IP/Bridge**, нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER] для входа в раздел **Menu 11.3 - Remote Node Network Layer Options**.

Рис. 116 Меню 11.3: применение NAT к удаленному узлу

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:
  IP Address Assignment = Static
  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=

Bridge Options:
  Ethernet Addr Timeout (min)= N/A

```

Поля изображённого выше меню описаны в следующей таблице.

Таблица 71 Применение NAT в меню 4 и 11.3.

ПОЛЕ	ОПИСАНИЕ	ЗНАЧЕНИЯ
Network Address Translation	Если выбрано это значение, SMT будет использовать указанный набор привязки адресов (меню 15.1 – подробности см. в разд. 24.2.1 на стр. 213). Можно настроить любой из перечисленных типов привязки (гл. 7 на стр. 99). Выберите Full Feature , если для P-791R v2 выделено несколько глобальных IP-адресов в сети WAN. При выборе опции Full Feature необходимо настроить как минимум один набор привязки адресов.	Full Feature
	Это значение параметра отключает NAT.	Нет
	Если выбран этот параметр, SMT использует набор привязки адресов 255 (меню 15.1 – см. разд. 24.2.1 на стр. 213). Если для P-791R v2 выделен только один глобальный IP-адрес в сети WAN, выберите SUA Only .	SUA Only

24.2 Настройка NAT

Меню и подменю наборов привязки адресов используются для создания таблицы привязки, по которой присваиваются глобальные адреса компьютерам в LAN и DMZ.

Набор 255 используется для SUA. Если в меню 4 или меню 11.3 выбран режим **Full Feature**, SMT будет использовать указанный набор привязки адресов. При выборе **SUA Only** SMT использует предварительно заданный набор **255** (только для чтения).

Набор серверов – это список серверов в локальной сети, которым поставлены в соответствие внешние порты. Для использования этого набора правило сервера должно устанавливаться внутри набора привязки адресов NAT. Подробнее об этих меню см. в описании переадресации портов в [разд. 7.4 на стр. 104](#). Для настройки NAT введите 15 в главном меню для отображения следующего экрана.

Рис. 117 Меню 15: NAT Setup

Menu 15 - NAT Setup
<ol style="list-style-type: none"> 1. наборы привязки адресов 2. наборы серверов NAT

24.2.1 Наборы привязки адресов

Нажмите 1, чтобы войти в раздел **Menu 15.1.1 - Address Mapping Sets** (Наборы привязки адресов).

Рис. 118 Меню 15.1: наборы привязки адресов

```

Menu 15.1 - Address Mapping Sets

1. ACL Default Set
2.
3.
4.
5.
6.
7.
8.
255. SUA (read only)

```

Выберите набор привязки адресов, который требуется изменить. Поля в адресе 255 используются для SUA и не могут быть изменены.

24.2.1.1 Определяемые пользователем наборы привязки адресов



Чтобы удалить весь набор, оставьте поле **Set Name** пустым и нажмите [ENTER] внизу экрана.

Рис. 119 Меню 15.1.1: правила привязки адресов

```

Menu 15.1.1 - Address Mapping Rules

Set Name= ACL Default Set

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
-----
1.           0.0.0.0           Server+
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= None          Select Rule= N/A

```



Тип, локальный и глобальный начальный / конечный IP-адреса задаются в меню 15.1.1.1 (описано ниже), а соответствующие значения отображаются здесь.

Таблица 72 Меню 15.1.1: правила привязки адресов

ПОЛЕ	ОПИСАНИЕ
Set Name	Это – имя набора, выбранного в меню 15.1. Или введите имя нового набора, который нужно создать.
Нумерация	Это – номер правила.
Local Start IP	Local Start IP – начальный локальный IP-адрес (ILA).
Local End IP	Local End IP – конечный локальный IP-адрес (ILA). Если данное правило применяется для всех локальных IP, в этом случае начальный адрес – 0.0.0.0, а конечный адрес – 255.255.255.255.
Global Start IP	Это начальный глобальный IP-адрес (IGA). При наличии динамического IP-адреса введите 0.0.0.0 в качестве Global Start IP (Глобального начального IP-адреса) .
Global End IP	Это конечный глобальный IP-адрес (IGA).
Type	В этой графе перечисляются типы привязок, описанные выше. Режим Server позволяет указывать несколько серверов различных типов за NAT для подключения к данной машине. Некоторые примеры смотрите ниже.
Завершив настройку правила в этом меню, нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel", чтобы сохранить настройки, либо клавишу [ESC] для отмены.	

Порядок следования правил имеет важное значение, поскольку P-791R v2 применяет правила в том порядке, в котором они определены. Когда правило соответствует текущему пакету, P-791R v2 выполняет соответствующее действие, и остальные правила игнорируются. Если перед настроенным правилом есть пустые правила, это созданное правило передвинется вверх на определенное число пустых правил.

Например, если правила 1 – 6 уже заданы в текущем наборе и выполняется настройка правила номер 9, на экране с обзором набора новое правило получает номер 7, а не 9.

Если удалить правило 4, правила 5 – 7 поднимаются на 1 правило, так что старое правило 5 становится правилом 4, старое правило 6 – правилом 5, а старое правило 7 – правилом 6.



Для сохранения всего набора нажмите клавишу [ENTER] в нижней части экрана. Это нужно сделать снова, если производятся какие-либо изменения с набором – включая удаление правила. Изменения не вносятся в набор до тех пор, пока не будет выполнено это действие.

Выбор значения **Edit** в поле **Action** с последующим выбором правила приводит к появлению следующего меню, **Menu 15.1.1.1 - Address Mapping Rule**, в котором можно редактировать отдельные правила и настроить поля **Type** (Тип), **Local** (Локальный) и **Global Start/End IPs** (Глобальный начальный / конечный IP-адреса).



Конечный IP-адрес должен быть больше в числовом выражении, чем соответствующий начальный IP-адрес.

Рис. 120 Меню 15.1.1.1: правило привязки адресов

Menu 15.1.1.1 Address Mapping Rule
Type= Server
Local IP:
Start= N/A
End = N/A
Global IP:
Start= 0.0.0.0
End = N/A
Server Mapping Set= 2

Поля изображённого выше меню описаны в следующей таблице.

Таблица 73 Меню 15.1.1.1: правило привязки адресов

ПОЛЕ	ОПИСАНИЕ
Type	Нажмите пробел и [ENTER], чтобы выбрать один из пяти типов. В этой графе перечисляются типы привязок, описанные ранее (гл. 7 на стр. 99). Server позволяет указать несколько серверов различных типов, расположенных на данном компьютере за различными типами NAT. Пример см. в разд. 24.4.3 на стр. 220.
Local IP	Доступность отдельных полей зависит от содержимого поля Type .
Start	Введите начальный локальный IP-адрес (ILA).
End	Введите конечный локальный IP-адрес (ILA). Если данное правило применяется для всех локальных IP, в этом случае установите значение 0.0.0.0 для начального IP-адреса и 255.255.255.255 – для конечного. Это поле N/A (недоступно) для типов One-to-One и Server.
Global IP	Доступность отдельных полей зависит от содержимого поля Type .
Start	Введите начальный глобальный IP-адрес (IGA). При наличии динамического IP-адреса введите 0.0.0.0 в качестве Global Start IP (Глобального начального IP-адреса) . Обратите внимание на то, что для Global IP Start (Глобального начального адреса) можно установить значение 0.0.0.0 только в том случае, если выбраны типы Many-to-One (Множество – один) или Server (Сервер) .
End	Введите конечный глобальный IP-адрес (IGA). Это поле не действует (N/A) для привязок One-to-One, Many-to-One и Server .

Таблица 73 Меню 15.1.1.1: правило привязки адресов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Server Mapping Set	Это поле доступно только в том случае, если в поле Type выбран режим Server . Выберите набор привязок сервера, используемый для данного правила.
Завершив настройку правила в этом меню, нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel", чтобы сохранить настройки, либо клавишу [ESC] для отмены.	

24.3 Настройка сервера, находящегося за NAT



Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-791R v2 будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.

Для настройки сервера, находящегося за NAT, выполните следующие действия:

- 1 Введите 15 в главном меню для перехода к **Menu 15 - NAT Setup**.
- 2 Введите 2, чтобы войти в меню 15.2 (для настройки правил привязки адресов на порту WAN устройства P-791R v2, снабженного одним портом WAN).

Рис. 121 Меню 15.2: наборы серверов 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

- 3 Введите 1, чтобы настроить набор сервера, используемый в режиме SUA, или введите номер набора сервера, который требуется изменить для полноценного режима NAT. В разделе **Menu 15.2 - NAT Server Setup** настройте правила переадресации портов.

Рис. 122 Меню 15.2: настройка NAT в режиме сервера

Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	80	80	192.168.1.10
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

Первая запись описывает сервер по умолчанию (**Default**). Поля изображенного выше экрана описаны в следующей таблице.

Таблица 74 Меню 15.2: настройка NAT в режиме сервера

ПОЛЕ	ОПИСАНИЕ
Rule	Это поле содержит порядковый номер и не связано с каким-либо правилом. Однако сам порядок также имеет значение. P-791R v2 последовательно проверяет каждое активное правило и применяет только первое найденное правило, для которого выполняются условия.
Start Port	В этом поле отображается начало диапазона номеров портов, переадресуемых данным правилом.
End Port	В этом поле отображается конец диапазона номеров портов, переадресуемых данным правилом. Если указан только один номер порта, значение этого поля будет совпадать со значением поля Start Port .
IP Address	В этом поле отображается IP-адрес сервера, на который переадресуются пакеты для указанных портов.

24.4 Общие примеры NAT

Ниже приведены некоторые примеры конфигурации NAT.

24.4.1 Пример 1: только доступ к Интернету

Следующий пример доступа к Интернету показывает, что для связывания всех внутренних локальных адресов (ILA) с одним внутренним глобальным адресом (IGA), назначаемым поставщиком услуг Интернета, достаточно одного правила.

Рис. 123 NAT: пример 1

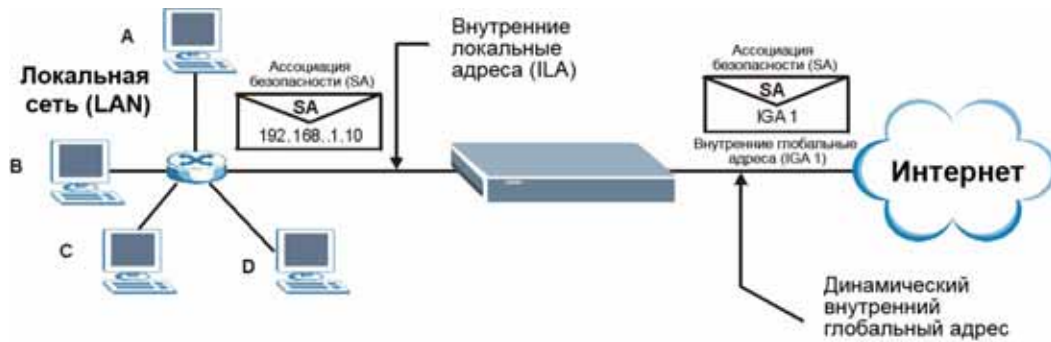


Рис. 124 Меню 4: пример применения NAT для доступа в Интернет

```

Menu 4 - Internet Access Setup

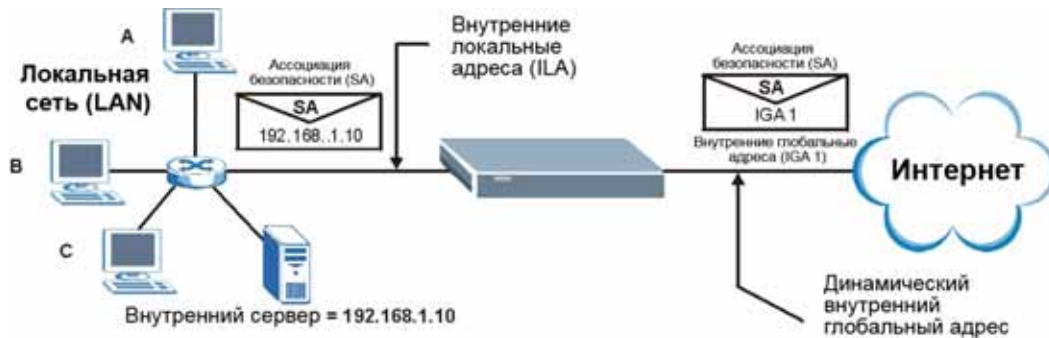
ISP's Name= MyISP
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #- 0
VCI #- 33
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= 0.0.0.0
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

```

В показанном выше меню 4 выберите параметр **SUA Only** из поля **Network Address Translation**. При этом активируется режим привязки “многие к одному”, описанный в [разд. 24.4 на стр. 218](#). Недоступный для редактирования параметр **SUA Only** в поле **Network Address Translation** меню 4 и 11.3 изначально настроен на этот случай.

24.4.2 Пример 2: доступ к Интернету с использованием внутреннего сервера по умолчанию

Рис. 125 NAT: пример 2



В этом случае порядок действий соответствует описанному выше (используется удобный предопределенный набор **SUA Only**), но дополнительно потребуется войти в меню 15.2.1 и указать режим **Default Server** для сервера, находящегося за NAT, как показано на следующем рисунке.

Рис. 126 Меню 15.2: указание внутреннего сервера

Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	192.168.1.10
2.	21	25	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

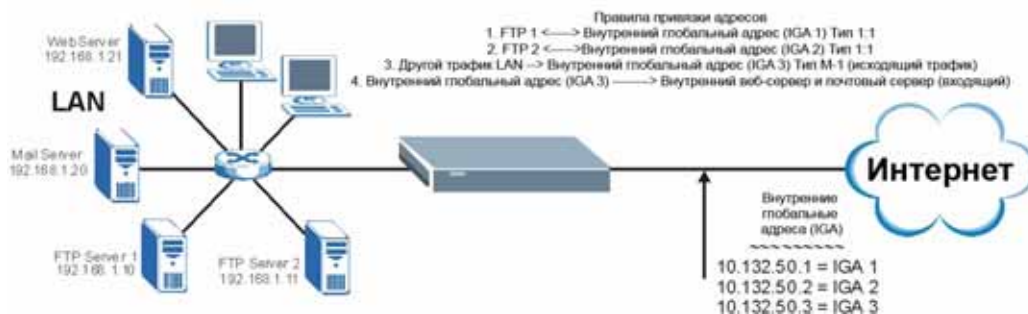
24.4.3 Пример 3: несколько общедоступных IP-адресов с использованием внутренних серверов

В данном примере показано три IGA, предоставленных оператором. Существует много отделов, но два из них имеют собственный FTP-сервер. Все отделы совместно пользуются одним и тем же маршрутизатором. На данном примере показано резервирование одного IGA для каждого отдела с FTP-сервером, и все отделы используют другой IGA. Установите соответствие FTP-серверов с первыми двумя IGA, а остальной трафик LAN - с оставшимися IGA. Установите соответствие между третьим IGA и внутренним веб-сервером и почтовым сервером. Необходимо настроить четыре правила, два двунаправленных и два однонаправленных, как показано ниже.

- 1 Установите соответствие первого IGA с первым внутренним FTP-сервером для FTP-трафика в обоих направлениях (**1:1** привязка, дающая как локальные, так и глобальные IP-адреса).
- 2 Установите соответствие второго IGA со вторым внутренним FTP-сервером для FTP-трафика в обоих направлениях (**1:1** привязка, дающая как локальные, так и глобальные IP-адреса).
- 3 Установите соответствие другого исходящего трафика LAN с IGA3 (**несколько: 1** привязка).
- 4 Кроме того, производится установка соответствия третьего IGA с веб-сервером и почтовым сервером в сети LAN. Тип **Server (Сервер)** позволяет указать несколько серверов различных типов для других компьютеров за NAT в LAN.

Можно привести следующий пример:

Рис. 127 NAT: пример 3



- 1 В этом случае следует настроить набор привязки адресов 1 в разделе **Menu 15.1 - Address Mapping Sets**. Для этого в поле **Network Address Translation** (меню 4 или меню 11.3) необходимо выбрать режим **Full Feature**, как показано на [рис. 128 на стр. 222](#).
- 2 Затем введите 15 в главном меню.
- 3 Введите 1 для настройки наборов привязки адресов.
- 4 Введите 1, чтобы начать настройку этого нового набора. Введите имя набора, выберите значение **Edit Action** (Редактировать действие) и затем введите 1 в поле **Select Rule** (Выбрать правило). Нажмите [ENTER] для подтверждения.
- 5 В поле **Type** выберите **One-to-One** (непосредственная привязка для пакетов, пересылаемых в обоих направлениях) и в качестве локального начального IP-адреса (**Start IP**) введите 192.168.1.10 (IP-адрес FTP-сервера 1), а в качестве глобального начального IP-адреса (**Start IP**) введите 10.132.50.1. Этот адрес будет первым IGA. (См. [рис. 129 на стр. 222](#)).
- 6 Повторите предыдущее действие для выполнения правил 2 – 4, как указано выше.
- 7 После выполнения этих настроек меню 15.1.1 должно принять вид, показанный на [рис. 130 на стр. 223](#).

Рис. 128 Пример 3: меню 11.3

```
Menu 11.3 - Remote Node Network Layer Options

IP Options:
IP Address Assignment = Dynamic
Rem IP Addr = 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= N/A
NAT= SUA Only
  Address Mapping Set= N/A
Metric= 2
Private= No
RIP Direction= None
  Version= RIP-1
Multicast= None
IP Policies=

Bridge Options:
Ethernet Addr Timeout (min)= N/A
```

Следующий рисунок иллюстрирует настройку первого правила.

Рис. 129 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
```

Рис. 130 Пример 3: заключительное 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	10.32.50.3		M-1
4.			10.132.50.3		Server+
5.					
6.					
7.					
8.					
9.					
10.					
Action= None			Select Rule= N/A		

Теперь настройте IGA3 для привязки к веб-серверу и почтовому серверу в сети LAN.

- 1** Введите 15 в главном меню.
- 2** Введите 2, чтобы перейти в меню 15.2.
- 3** (Для P-791R v2 с несколькими портами WAN в меню 15.2 введите 1 или 2).
Настройте меню, как показано на [рис. 131](#) на [стр. 223](#).

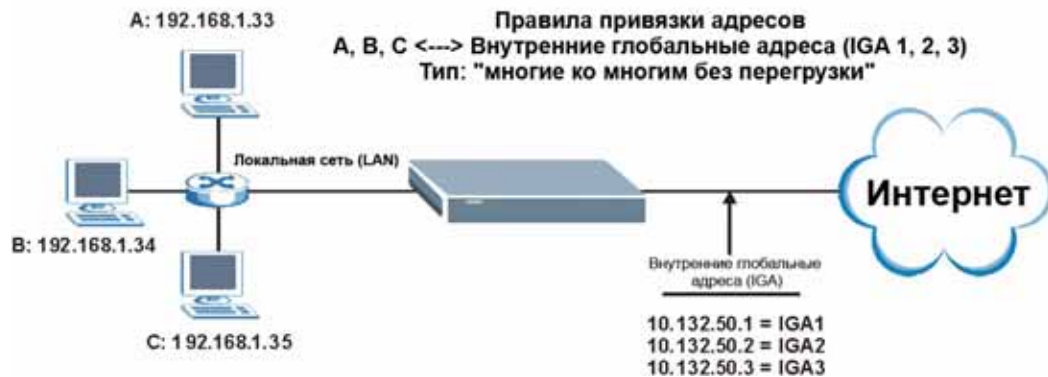
Рис. 131 Пример 3: меню 15.2

Menu 15.2 - 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

24.4.4 Пример 4: программы, несовместимые с NAT

Некоторые приложения не поддерживают привязку NAT с использованием трансляции адресов портов TCP и UDP. В этом случае лучше использовать привязку **Many-One-to-One**, поскольку в режимах NAT **Many-One-to-One** (а также **One-to-One**) номера портов *не* изменяются. Это проиллюстрировано на следующем рисунке.

Рис. 132 NAT: пример 4



Другие приложения, такие как игровые программы, являются не дружественными к NAT, потому что они вставляют информацию об адресах в поток передачи данных. Эти приложения не работают через NAT даже при использовании привязок **One-to-One** и **Many-One-to-One**.

Выполните действия, описанные в примере 3, чтобы настроить эти два меню следующим образом.

Рис. 133 Пример 4: меню 15.1.1.1: правило привязки 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
```

После завершения настройки правила следует проверить настройки в меню 15.1.1, как показано ниже.

Рис. 134 Пример 4: меню 15.1.1: правила привязки 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 N+
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= None          Select Rule= N/A
```


Настройка фильтра

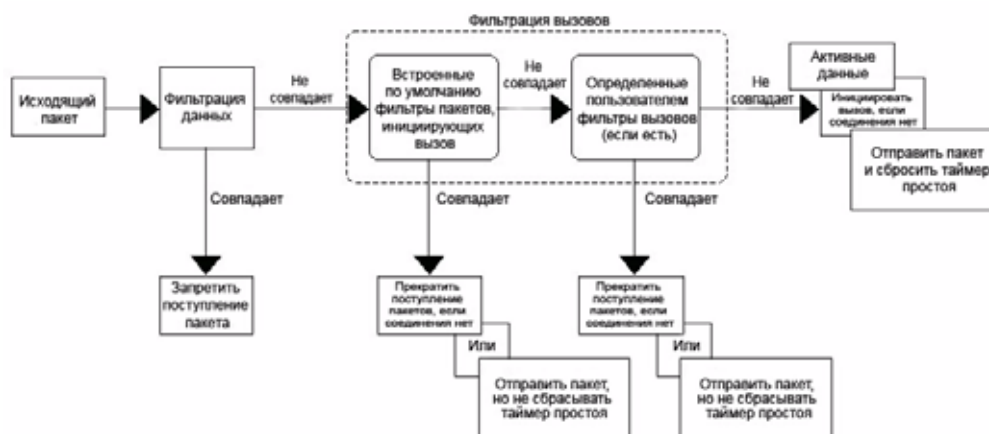
В этой главе дается описание того, как создавать и применять фильтры.

25.1 Основы применения фильтров

P-791R v2 использует фильтры для принятия решений о прохождении или запрете пакета, а также об осуществлении исходящего вызова. Существует два типа применения фильтров: фильтрация данных и фильтрация вызовов. Фильтры данных подразделяются на фильтры устройств и протоколов, описание которых даётся ниже.

Фильтрация данных позволяет просматривать данные для принятия решения о том, следует ли передавать пакет. Фильтры данных делятся на фильтры входящие и исходящие, в зависимости от направления пакета относительно порта. Фильтрация данных может применяться как в WAN, так и в LAN. Фильтрация вызовов используется для принятия решения о том, должен ли пакет приводить к запуску вызова. Фильтрация вызовов удалённого узла применяется только при использовании инкапсуляции PPPoE. Исходящие пакеты должны проходить фильтрацию данных, прежде чем будет выполняться фильтрация вызовов, как показано на рисунке ниже.

Рис. 135 Процесс фильтрации исходящих пакетов



К исходящим пакетам P-791R v2 применяет только фильтры данных. Пакеты обрабатываются в зависимости от того, найдено ли соответствие. В следующих разделах описана настройка наборов фильтров.

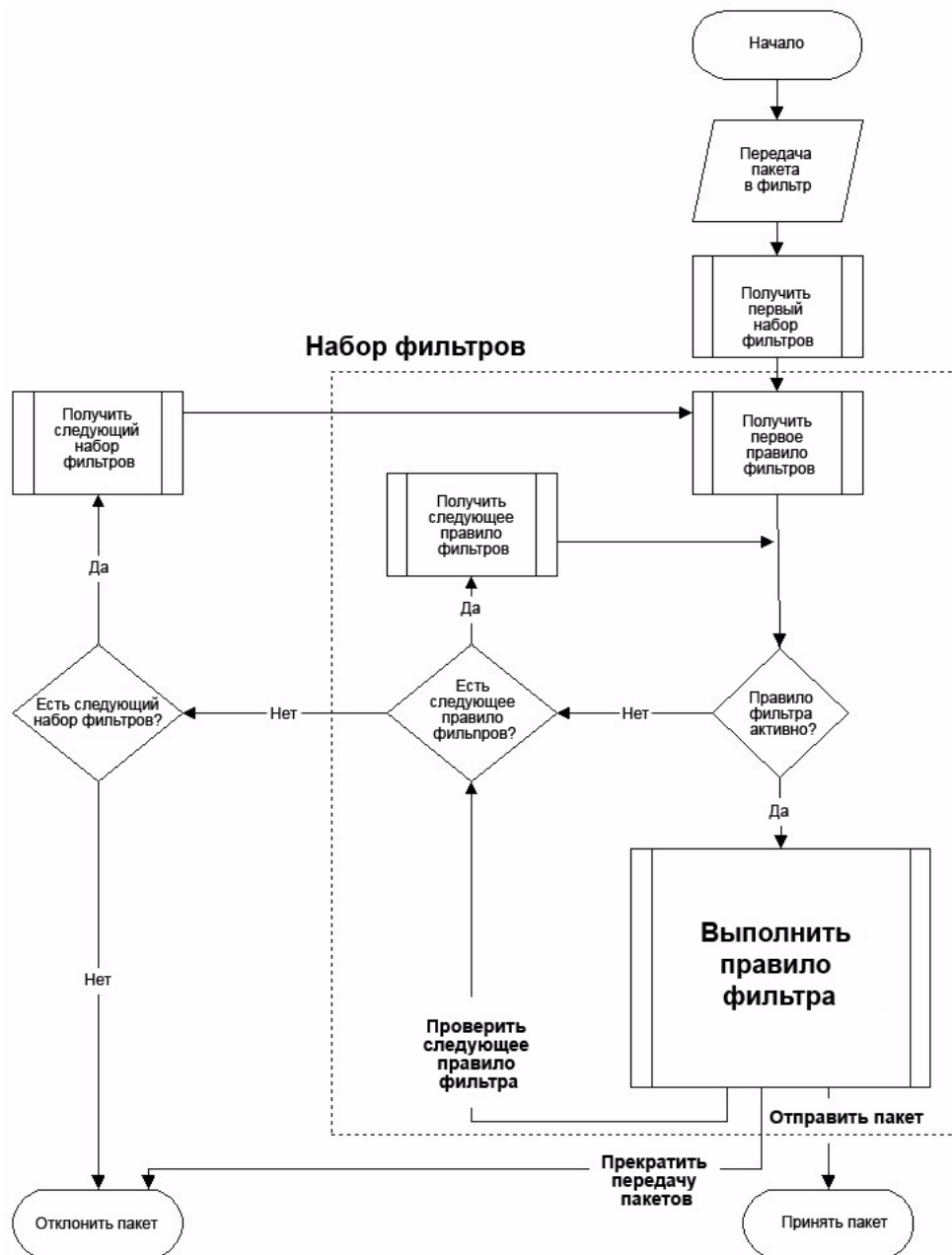
25.1.1 Структура фильтров устройства P-791R v2

Набор фильтров состоит из одного или нескольких правил фильтров. Обычно группы объединяют соответствующие правила, например, все правила для NetBIOS, в набор с общим именем. P-791R v2 позволяет настроить до двенадцати наборов фильтров, содержащих 6 правил в каждом наборе, что всего составляет 72 правила фильтров в системе. В одном наборе нельзя смешивать правила фильтров устройств и правила фильтров протоколов. Можно применить до четырёх наборов фильтров для конкретного порта с целью блокирования нескольких типов пакетов. При том, что каждый набор фильтров содержит до шести правил, можно иметь максимум 24 правила, действующих для одного порта.

Наборы правил фильтров с заводскими настройками в меню 21 по умолчанию препятствуют запуску вызовов трафиком NetBIOS и открытию входящих сеансов. Обзор правил фильтров показан на рисунках внизу.

На следующем рисунке проиллюстрирован логический поток при выполнении правила фильтра. Смотрите также [рис. 140 на стр. 234](#), где изображён логический поток при выполнении IP-фильтра.

Рис. 136 Процесс выполнения правил фильтра



Можно применить до четырёх наборов фильтров для конкретного порта с целью блокирования нескольких типов пакетов. При том, что каждый набор фильтров содержит до шести правил, можно иметь максимум 24 правила, задействованных для одного порта.

25.2 Настройка набора фильтров

P-791R v2 осуществляет фильтрацию пакетов протокола NetBIOS поверх TCP/IP по умолчанию. Для настройки другого набора фильтров выполните указанные ниже действия.

- 1 Введите 21 в главном меню для открытия меню 21.

Рис. 137 Меню 21: настройка набора фильтров

```

Menu 21 - Filter Set Configuration

Filter                               Filter
Set #   Comments                     Set #   Comments
-----  -----
  1     NetBIOS_WAN                    7
  2     NetBIOS_LAN                    8
  3     TELNET_WAN                     9
  4     PPPoE                          10
  5     FTP_WAN                        11
  6     _____                    12     _____

Enter Filter Set Number to Configure= 0

Edit Comments= N/A

```

- 2 Выберите набор фильтров, которые необходимо настроить (1-12), и нажмите [ENTER].
- 3 Введите описательное имя или комментарий в поле **Edit Comments** и нажмите [ENTER].
- 4 Нажмите [ENTER] в сообщении [Press ENTER to confirm] для открытия **Menu 21.x - Filter Rules Summary**.

На этом экране отображается сводка правил, имеющихся в наборе фильтров.

Рис. 138 Меню 21.1: сводка правил фильтра

```

Menu 21.1. - Filter Rules Summary

# A Type ( A тип)                    Filter Rules (Правила фильтра)
M m n
-----
 1 N
 2 N
 3 N
 4 N
 5 N
 6 N

```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 75 Аббревиатуры, используемые в меню сводки правил фильтров

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер.
A	Активность: "Y" означает, что правило активно. "N" означает, что правило неактивно.
Type	Тип правила фильтра: "GEN" – универсальный, "IP" – TCP/IP.
Filter Rules	Эти параметры отображаются здесь.
C	Дополнительно. "Y" означает, что существуют и другие правила проверки, формирующие цепочку правил вместе с текущим правилом. Действие невозможно выполнять до тех пор, пока цепочка правил не будет завершена. "N" означает, что больше нет правил, подлежащих проверке. Можно указать действие, которое следует выполнить, т.е. переадресовать пакет, отбросить пакет или проверить следующее правило. Следующее правило не зависит от только что проверенного.
m	Действие при совпадении. "F" означает немедленную переадресацию пакета и пропуск проверки остальных правил. "D" означает отбрасывание пакета. "N" означает проверку следующего правила.
n	Действие при несовпадении. "F" означает немедленную переадресацию пакета и пропуск проверки остальных правил. "D" означает отбрасывание пакета. "N" означает проверку следующего правила.

В следующей таблице содержится краткое описание аббревиатур, используемых в предыдущих меню. Аббревиатуры правил фильтров, зависящие от протокола, перечислены ниже.

Таблица 76 Используемые аббревиатуры правил

СОКРАЩЕНИЯ	ОПИСАНИЕ
IP	
Pr	Протокол
SA	Адрес источника
SP	Номер порта источника
DA	Адрес получателя
DP	Номер порта получателя
GEN	
Off	Смещение
Len	Длина

Настройка правил фильтров описана в следующем разделе.

25.2.1 Настройка правила фильтра

Чтобы настроить правило фильтра, введите его номер в разделе **Menu 21.x - Filter Rules Summary** и нажмите [ENTER]. Откроется меню 21.x.x для редактирования правила.

Для ускорения фильтрации все правила в наборе фильтров должны относиться к одному и тому же классу, т.е. быть фильтрами протоколов или универсальными фильтрами. Класс набора фильтров определяется по первому правилу, создаваемому пользователем. При применении наборов фильтров к порту отдельные поля меню предоставляются для наборов фильтров протоколов и устройств. При попытке указать набор фильтров протокола в поле фильтров устройства или наоборот P-791R v2 отображает предупреждение и не позволяет выполнить сохранение.

25.2.2 Настройка правила фильтра TCP/IP

В данном разделе иллюстрируется порядок настройки правил фильтров TCP/IP. Правила TCP/IP позволяют основывать правило на полях в IP и протоколе верхнего уровня, например, заголовках UDP и TCP.

Для настройки правил TCP/IP выберите **TCP/IP Filter Rule** в поле **Filter Type** и нажмите [ENTER], чтобы открыть раздел **Menu 21.x.x - TCP/IP Filter Rule**. Ниже в качестве примера приведено меню 122.1.1.

Рис. 139 Меню 21.1.1: правила фильтров TCP/IP

```

Menu 21.1.1. - 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

```

Настройка правила фильтра TCP/IP описана в следующей таблице.

Таблица 77 Меню 21.1.1: правила фильтров TCP/IP

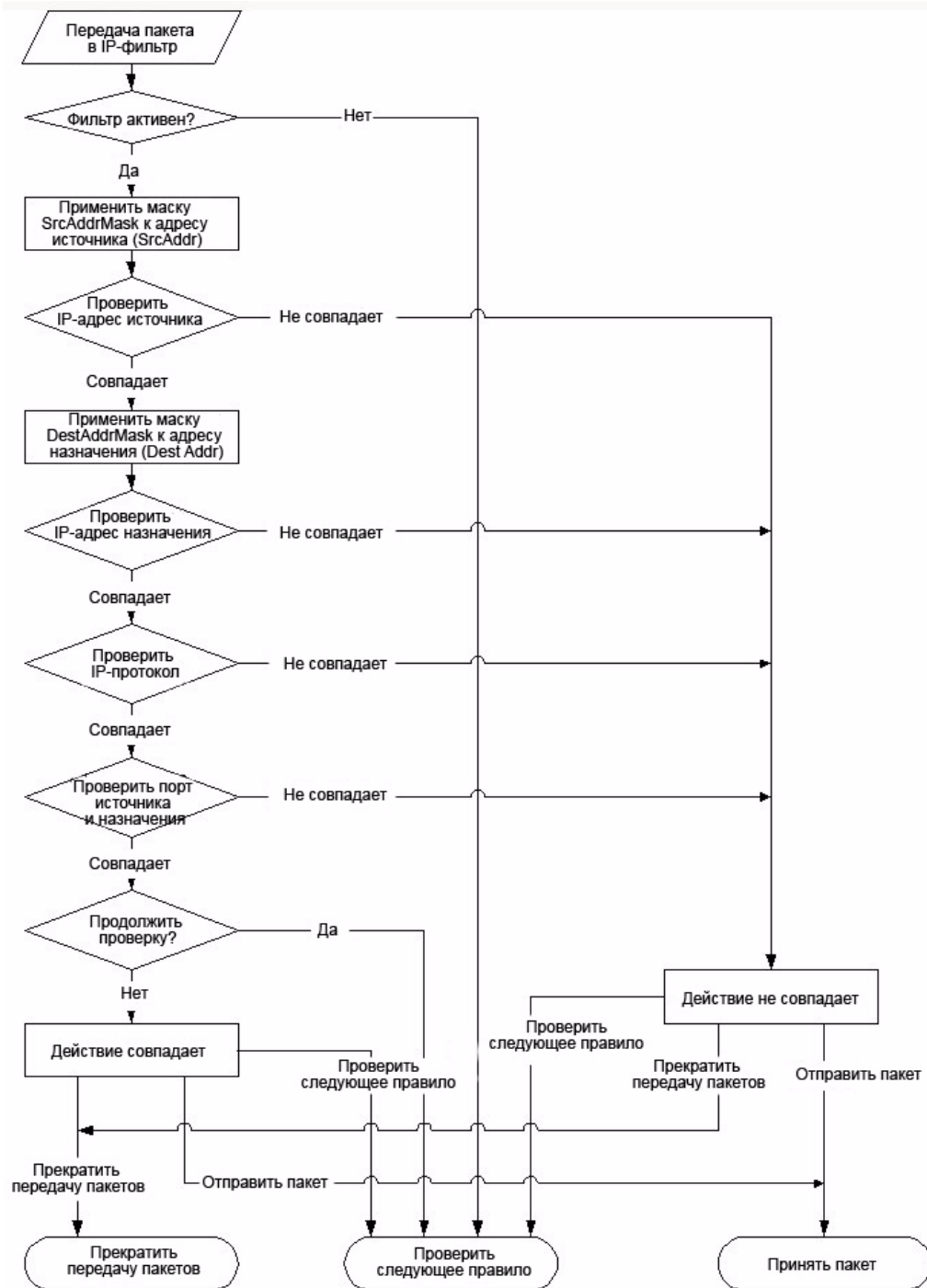
ПОЛЕ	ОПИСАНИЕ
Active	Нажмите пробел, затем [ENTER], чтобы выбрать Yes и активировать правило фильтра, или No для деактивации правила.
IP Protocol	Укажите протокол верхнего уровня, например, TCP – 6, UDP – 17, ICMP – 1. Введите значение от 0 до 255. Значение 0 соответствует ЛЮБОМУ протоколу.
IP Source Route	Нажмите пробел и [ENTER], чтобы выбрать значение Yes для применения правила к пакетам с опцией исходного маршрута IP. В противном случае пакеты не должны иметь опцию исходного маршрута. Большинство пакетов IP не содержат исходный маршрут.
Destination	

Таблица 77 Меню 21.1.1: правила фильтров TCP/IP

ПОЛЕ	ОПИСАНИЕ
IP Addr	Введите IP-адрес места получателя пакета, который необходимо фильтровать. Поле игнорируется, если его значение – 0.0.0.0.
IP Mask	Введите маску IP, применяемую к полю Destination: IP Addr .
Port #	Введите порт получателя пакетов, подлежащих фильтрации. Диапазон данного поля – 0 - 65535. Это поле игнорируется, если его значение 0.
Port # Comp	Нажмите [SPACE BAR], затем [ENTER] для выбора сравнения с целью применения к порту места назначения в пакете и значения, заданного в поле Destination: Port # . Возможны следующие значения: None (нет), Equal (равно), Not Equal (не равно), Less (меньше) и Greater (больше).
Source	
IP Addr	Введите IP-адрес источника пакета, который необходимо фильтровать. Поле игнорируется, если его значение – 0.0.0.0.
IP Mask	Введите маску IP для применения к Source (Источнику): IP Addr .
Port #	Введите порт источника пакетов, которые необходимо фильтровать. Диапазон данного поля – 0 - 65535. Это поле игнорируется, если его значение 0.
Port # Comp	Нажмите пробел, затем [ENTER] для выбора сравнения, применяемого к порту источника в пакете, и значения, заданного в поле Source: Port # . Возможны следующие значения: None (нет), Equal (равно), Not Equal (не равно), Less (меньше) и Greater (больше).
TCP Estab	Это поле действует только в том случае, когда значение поля IP Protocol (Протокол IP) – 6, TCP. Нажмите пробел и [ENTER], чтобы выбрать значение Yes и применять правило к пакетам, устанавливающим соединение TCP (SYN=1 и ACK=0); если значение – No , правило игнорируется.
More	Нажмите пробел и [ENTER] для выбора значения Yes или No . Если значение – Yes (Да) , соответствующий пакет передается следующему правилу фильтров перед выполнением действия; если No (Нет) , пакет отбрасывается в соответствии с полями действия. Если значение поля More – Yes (Да) , в таком случае Action Matched и Action Not Matched будут N/A .
Log	Нажмите пробел, затем [ENTER] для выбора опции регистрации из следующих вариантов: None (Нет) – No packets will be logged (пакеты не регистрируются). Action Matched - регистрируются только пакеты, соответствующие параметрам правила. Action Not Matched - регистрируются только пакеты, не соответствующие параметрам правила. Both (Оба) – регистрируются все пакеты.
Action Matched	Нажмите пробел и [ENTER], чтобы выбрать действие для пакетов, соответствующих условиям. Возможны следующие значения: Check Next Rule (проверить следующее правило), Forward (переслать) и Drop (отбросить).
Action Not Matched	Нажмите пробел и [ENTER] для выбора действия для пакета, не соответствующего условиям правила. Возможны следующие значения: Check Next Rule (проверить следующее правило), Forward (переслать) и Drop (отбросить).
По завершении настроек в меню Menu 21.1.1 - TCP/IP Filter Rule нажмите [ENTER] в сообщении "Press ENTER to Confirm" или [ESC] для отмены. Эти данные теперь должны отображаться в Menu 21.1. - Filter Rules Summary (Меню 21.1.1 – Сводка правил фильтра) .	

На следующем рисунке проиллюстрирован логический поток фильтра IP.

Рис. 140 Выполнение фильтра IP



25.2.3 Настройка универсального правила фильтра

В данном разделе описан порядок настройки универсального правила фильтра. Цель универсальных правил – предоставить возможность фильтрации пакетов, не относящихся к IP. Обычно для IP лучше использовать правила IP непосредственно.

При обработке универсальных правил P-791R v2 рассматривает пакет как поток байтов, а не как структурированный пакет IP или IPX. Следует указать часть пакета, подлежащую проверке с использованием полей **Offset** (от 0) и **Length**, выраженных в байтах. P-791R v2 применяет к блоку данных маску (с использованием побитового “И”), после чего сравнивает результат со значением для определения соответствия. Поля **Mask** и **Value** указываются в виде шестнадцатеричных чисел. Обратите внимание на то, что для представления байта требуется две шестнадцатеричных цифры, поэтому если длина – 4, для ввода значения в каждом поле требуется 8 цифр, например, FFFFFFFF.

Для настройки универсального правила выберите **Generic Filter Rule** в поле **Filter Type** в меню 21.1.1 и нажмите [ENTER], чтобы открыть универсальное правило фильтра, как показано ниже. Ниже в качестве примера приведено меню 21.1.1 .

Рис. 141 Меню 21.1.1: универсальное правило фильтра

```

Menu 21.1.1 - Generic Filter Rule

Filter #: 1,1
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

```

Поля меню **Generic Filter Rule** описаны в следующей таблице.

Таблица 78 Меню 21.1.1: универсальное правило фильтра

ПОЛЕ	ОПИСАНИЕ
Filter #	В этом поле указываются координаты правила. Например, 2,3 означает второй набор фильтров и третье правило этого набора.
Filter Type	Нажмите пробел и [ENTER] для выбора типа правила. Параметры, отображаемые под каждым типом, различны. Правила фильтров TCP/IP используются для фильтрации пакетов IP, тогда как универсальные правила фильтров допускают фильтрацию пакетов, не относящихся к IP. Возможны следующие значения: Generic Filter Rule (универсальное правило фильтра) и TCP/IP Filter Rule (правило фильтра TCP/IP).
Active	Выберите Yes (Да) для включения правила фильтров или No (Нет) для его выключения.
Offset	Введите начальный байт блока данных в пакете, который необходимо сравнить. Диапазон этого поля – от 0 до 255.
Length	Введите сумму байтов блока данных в пакете, который необходимо сравнить. Диапазон этого поля – от 0 до 8.
Mask	Введите маску (в шестнадцатеричном формате) для применения к блоку данных перед сравнением.
Value	Введите значение (в шестнадцатеричном формате) для сравнения с блоком данных.

Таблица 78 Меню 21.1.1: универсальное правило фильтра (продолжение)

ПОЛЕ	ОПИСАНИЕ
More	Если значение – Yes (Да) , соответствующий пакет передаётся следующему правилу фильтров перед выполнением действия; в противном случае пакет отбрасывается в соответствии с полями действия. Если в поле More значение Yes , то поля Action Matched и Action Not Matched будут содержать значение No .
Log	Выберите опцию регистрации из числа следующих вариантов: None – пакеты не регистрируются. Action Matched - регистрируются только пакеты, соответствующие параметрам правила. Action Not Matched - регистрируются только пакеты, не соответствующие параметрам правила. Both (Оба) – регистрируются все пакеты.
Action Matched	Выберите действие для пакета, соответствующему правилу. Возможны следующие значения: Check Next Rule (проверить следующее правило), Forward (переслать) и Drop (отбросить).
Action Not Matched	Выберите действие для пакетов, не соответствующих правилу. Возможны следующие значения: Check Next Rule (проверить следующее правило), Forward (переслать) и Drop (отбросить).
При заполненном меню Menu 21.1.1 - TCP/IP Filter Rule (Меню 21.4.1.1 Универсальное правило фильтра) нажмите [ENTER] ([ВВОД]) в сообщении "Press ENTER to Confirm" (Нажмите Ввод для подтверждения) для сохранения конфигурации или [ESC] ([ВЫХОД]) для отмены действий. Эти данные теперь должны отображаться в Menu 21.1. - Filter Rules Summary (Меню 21.1.1 – Сводка правил фильтра) .	

25.3 Пример фильтра

Рассмотрим пример блокирования доступа внешних пользователей к устройству P-791R v2 через Telnet. Другие примеры фильтров можно найти на компакт-диске в комплекте с устройством.

Рис. 142 Пример фильтра для Telnet

- 1 Перейдите в раздел **Menu 21 - Filter and Firewall Setup**, введя **21 Настройка набора фильтров** в главном меню.
- 2 Выберите номер набора фильтров, который необходимо настроить (например, 3), и нажмите [ENTER].

- 3 Введите описательное имя или комментарий в поле **Edit Comments** и нажмите [ENTER].
- 4 Чтобы открыть раздел **Menu 21.1 - Filter Rules Summary**, в сообщении [Press ENTER to confirm] нажмите [ENTER].
- 5 Введите 1 для настройки первого правила фильтров (единственное правило фильтров в данном наборе). Внесите записи в это меню, как показано на следующем рисунке.

Рис. 143 Пример фильтра: меню 21.1.1

```

Menu 21.1.1. - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0 (Адрес IP= 0.0.0.0)
              IP Mask= 0.0.0.0 (Маска IP= 0.0.0.0)
              Port # = 23
              Port # Comp= Equal
Source: IP Addr= 0.0.0.0 (Адрес IP= 0.0.0.0)
        IP Mask= 0.0.0.0 (Маска IP= 0.0.0.0)
        Port # =
        Port # Comp= None
TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule

```

Номер порта для службы Telnet (по протоколу TCP) – **23**. Номера портов распространенных сетевых служб см. в документе *RFC 1060*.

После нажатия клавиши [ENTER] для подтверждения отображается следующий экран. Обратите внимание на то, что в этом наборе имеется только одно правило фильтров.

Рис. 144 Пример сводки правил фильтров: меню 21.1.

```

Menu 21.1. - Filter Rules Summary

# A Type ( A тип)                Filter Rules (Правила фильтра)
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

```

Он показывает, что выполнена настройка и активация (**A = Y**) правила фильтров TCP/IP (**Type = IP, Pr = 6**) для портов telnet получателя (**DP = 23**).

M = N означает, что действие можно выполнять немедленно. Действие заключается в отбрасывании пакета (**m = D**), если оно соответствующее, и в немедленной переадресации пакета (**n = F**), если действие несоответствующее, независимо от того, есть ли другие правила, которые необходимо проверить (в этом примере их нет).

После создания набора фильтров необходимо применить его.

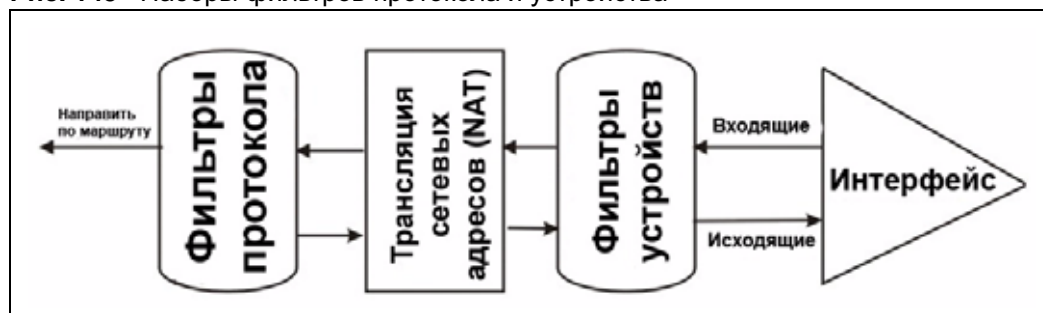
- 1 Введите 11 в главном меню для перехода к меню 11.
- 2 Введите 1 или 2 для входа в раздел **Menu 11.x - Remote Node Profile**.
- 3 Перейдите в поле **Edit Filter Sets**, нажмите пробел для выбора значения **Yes**, а затем – [ENTER].
- 4 Откроется меню 11.1.4. Активируйте набор фильтров (в данном примере – набор 3), как показано на [рис. 108 на стр. 202](#).
- 5 Указав номера наборов и покинув меню 11.1.4, нажмите [ENTER] для подтверждения.

25.4 Типы фильтров и NAT

Существует два класса правил фильтров: универсальные правила устройства (**Generic Filter**) и правила фильтра протоколов (**TCP/IP**). Правила универсального фильтра действуют по отношению к необработанным данным, пересылаемым в / из LAN и WAN. Правила фильтра протокола воздействуют на пакеты IP. Более подробно правила универсального фильтра и фильтра TCP/IP рассматриваются в следующем разделе. При включении NAT (трансляции сетевых адресов) внутренний адрес IP и номер порта заменяются на основе последовательных соединений, что делает возможным выяснение точного адреса и порта в сети. Поэтому P-791R v2 применяет фильтры протоколов к “известному” IP-адресу и номеру порта перед прохождением NAT для исходящих пакетов и после NAT – для входящих пакетов.

С другой стороны, универсальные фильтры или фильтры устройств применяются к необработанным пакетам, появляющимся в сети. Фильтры на P-791R v2 применяются в момент приема и отправки пакетов, т.е. на интерфейсе. Интерфейсом может служить порт Ethernet или любой другой аппаратный порт. Это проиллюстрировано на следующей диаграмме.

Рис. 145 Наборы фильтров протокола и устройства



25.5 Применение фильтра

В этом разделе показано, где применять фильтр(-ы) после его (их) создания. В устройстве P-791R v2 предусмотрены стандартные фильтры для предотвращения исходящих вызовов в результате трафика NetBIOS, а также блокирования входящих соединений по Telnet, FTP и HTTP.

25.5.1 Применение фильтров LAN

Наборы фильтров трафика LAN могут быть полезны для блокировки определённых пакетов, сокращения объема трафика и предотвращения возникновения брешей в системе безопасности. Перейдите в меню 3.1 (показано ниже) и введите номер(-а) набора(-ов) фильтров, которые необходимо применить соответствующим образом. Можно выбрать до четырёх наборов фильтров (из 12), введя их номера через запятую, например, 3, 4, 6, 11. Наборы входных фильтров фильтруют входящий в P-791R v2 трафик, а наборы выходных фильтров – трафик, исходящий из P-791R v2.

Рис. 146 Фильтрация трафика LAN

```

Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

```

25.5.2 Применение фильтров удаленного узла

Перейдите в показанное ниже меню 11.5 (необходимо учесть, что наборы фильтров вызовов предусмотрены только для инкапсуляции PPPoA или PPPoE) и введите соответствующие номера наборов фильтров. Можно последовательно ввести до четырёх наборов фильтров, вводя их номера, разделённые запятыми. В устройстве P-791R v2 предусмотрены стандартные фильтры для предотвращения исходящих вызовов в результате трафика NetBIOS, а также блокирования входящих соединений по Telnet, FTP и HTTP.

Рис. 147 Фильтрация трафика удалённого узла

```

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=

```


Настройка SNMP

Это меню служит для настройки SNMP. Дополнительные сведения о протоколе SNMP см. в [разд. 11.6 на стр. 129](#).

26.1 Настройка SNMP

Для настройки SNMP введите 22 в основном меню, чтобы перейти на показанный ниже экран **Menu 22 - SNMP Configuration**. Под “сообществом” для запросов **Get**, **Set** и **Trap** в терминологии SNMP понимается аналог пароля.

Рис. 148 Меню 22: SNMP Configuration

```

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

```

В следующей таблице описаны параметры конфигурации SNMP.

Таблица 79 Меню 22: настройка SNMP

ПОЛЕ	ОПИСАНИЕ
Get Community	Введите сообщество для запроса Get, которое будет выступать в качестве пароля для всех входящих запросов Get и GetNext от диспетчерской станции.
Set Community	Введите сообщество для запроса Set, которое будет выступать в качестве пароля для всех входящих запросов Set от диспетчерской станции.
Trusted Host	Если указан доверенный хост, P-791R v2 будет отвечать на SNMP-сообщения, исходящие только с этого адреса. Пустое (по умолчанию) поле означает, что P-791R v2 будет отвечать на все сообщения SNMP, получаемые им, независимо от источника.
Trap	
Community	Введите сообщество для прерываний, которое будет выступать в качестве пароля при отправке прерываний диспетчеру SNMP.
Destination	Введите IP-адрес станции, которой следует направлять прерывания SNMP.
Заполнив поля в этом меню, нажмите [ENTER] в приглашении “Press [ENTER] to confirm or [ESC] to cancel”, чтобы сохранить настройки, или [ESC] для отмены и возврата на предыдущий экран.	

Системный пароль

Это меню служит для изменения пароля. Этот же пароль используется для входа в веб-конфигуратор. Чтобы открыть это меню, в основном меню введите 23.

Рис. 149 Меню 23: системный пароль

Menu 23 - System Password Old Password= ? New Password= ? Retype to confirm= ?

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 80 Меню 23: системный пароль

ПОЛЕ	ОПИСАНИЕ
Old Password	Введите текущий пароль администратора для P-791R v2.
New Password	Введите новый пароль администратора для P-791R v2.
Retype to confirm	Повторно введите новый пароль администратора.

Информация о системе и диагностика

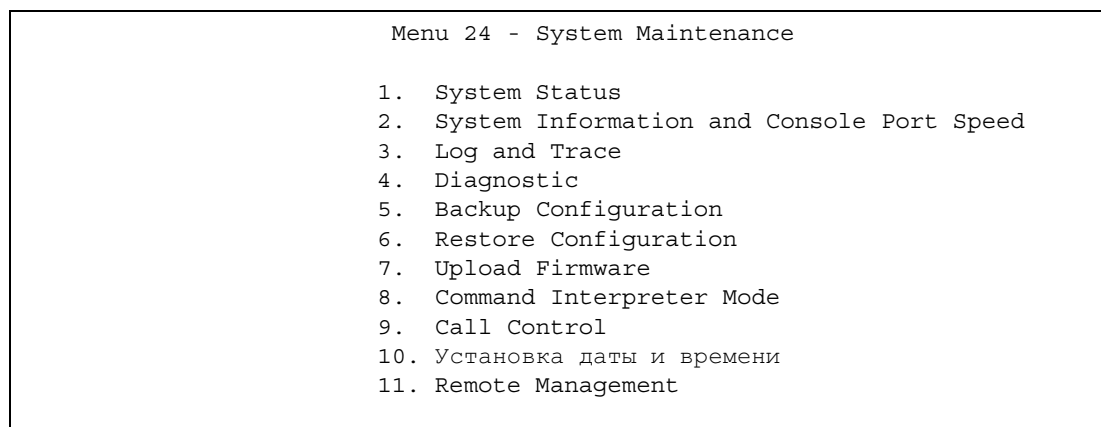
В этой главе рассматриваются меню SMT с 24.1 по 24.4.

28.1 Обзор средств наблюдения за состоянием системы

В этой главе описываются диагностические средства, которые могут использоваться для обслуживания P-791R v2. Эти инструменты сообщают текущее состояние системы и портов, обеспечивают ведение журналов и трассировку.

В главном меню выберите 24, чтобы открыть показанный ниже раздел **Menu 24 - System Maintenance**.

Рис. 150 Меню 24: обслуживание системы



28.2 Меню System Status

Первый пункт – System Status (состояние системы) – содержит сведения о версии микропрограммы и состоянии портов, а также статистику по портам, как показано на следующем рисунке. Экран System Status можно использовать для наблюдения за состоянием P-791R v2. В частности, этот экран предоставляет информацию о версии микропрограммы и числе отправленных и полученных пакетов.

Для входа в раздел System Status:

- 1 Введите 24, чтобы перейти в меню 24 - System Maintenance (обслуживание системы).
- 2 В этом меню введите 1, чтобы перейти в раздел System Maintenance - Status.
- 3 В разделе **Menu 24.1 - System Maintenance - Status** доступны три команды: Ввод цифры 1 разрывает соединение с сетью WAN, 9 сбрасывает счетчики, а нажатие клавиши [ESC] возвращает вас на предыдущий экран.

Рис. 151 Меню 24.1: состояние системы

```

Menu 24.1 - System Maintenance - Status                                06:28:45
                                                                    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: 4210   Line Status: Down
  Collisions: 0                          Rx Pkts: 4466   Transfer Rate: 0 кбит/с
CPU Load = 1.27%

Press Command:
COMMANDS: 1-Reset Counters  ESC-Exit
    
```

Поля экрана **Menu 24.1 - System Maintenance - Status** описаны в следующей таблице. Эти поля предназначены для диагностики и доступны только для чтения. В правом верхнем углу экрана отображаются текущие время и дата.

Таблица 81 Меню 24.1: состояние системы

ПОЛЕ	ОПИСАНИЕ
Node-Lnk	В этом поле отображается порядковый номер и тип соединения с удаленным узлом (тип инкапсуляции).
Status	В этом поле отображается состояние: Down (канал разъединен), Up (канал соединен), если используется инкапсуляция Ethernet, и Down (канал разъединен), Up (канал соединен), Idle (соединение (ppp-сеанс) неактивно), Dial (начало вызова) и Drop (прерывание вызова), если используется инкапсуляция PPPoE. Отсутствие соединения на порту обозначается N/A .
TxPkts	В этом поле отображается количество пакетов, отправленных P-791R v2 на удаленный узел.
RxPkts	В этом поле отображается количество пакетов, принятых P-791R v2 с удаленного узла.
Errors	В этом поле отображается количество пакетов, полученных через данное соединение с ошибкой.
Tx B/s	В этом поле отображается скорость передачи данных в байтах в секунду через данный порт.

Таблица 81 Меню 24.1: состояние системы (продолжение)

ПОЛЕ	ОПИСАНИЕ
Rx B/s	В этом поле отображается скорость приема данных в байтах в секунду через данный порт.
Up Time	В этом поле отображается общая продолжительность соединения с удаленным узлом по данному каналу.
My WAN IP (from ISP)	В этом поле отображается IP-адрес, присвоенный поставщиком услуг Интернета, или адрес, заданный в меню 4.
Ethernet:	В этом разделе отображаются сведения о портах LAN.
Status	В этом поле отображаются параметры скорости и дуплекса для портов LAN.
Collisions	Это – количество коллизий на данный порт.
TxPkts	Это – количество пакетов, отправленных через данный порт.
RxPkts	Это – количество пакетов, полученных через данный порт.
WAN	В этом разделе отображаются сведения, касающиеся порта WAN. Примечание. При соединении по схеме “точка – две точки” в этом поле отображается только состояние линии 1.
Line Status	В этом поле отображаются параметры скорости порта и дуплекса, если используется инкапсуляция Ethernet, либо одно из следующих значений: Down (линия разъединена или не подключена), Idle (неактивность PPP), Dial (начало вызова) и Drop (завершение вызова), если используется инкапсуляция PPPoE.
Transfer Rate	В этом поле отображается скорость передачи данных в килобитах в секунду через данный порт.
CPU Load	В этом поле отображается загрузка ЦП (в процентах).
Чтобы сбросить счетчики, введите 1. Для возврата в меню 24 нажмите [ESC].	

28.3 System Information and Console Port Speed

В этом разделе описываются параметры системы и выбирается скорость консольного порта. Чтобы перейти к экранам System Information (информация о системе) и Console Port Speed (скорость консольного порта):

- 1 Введите 24 для входа в меню **Menu 24 - System Maintenance**.
- 2 Введите 2 для перехода в раздел **Menu 24.2 - System Information and Console Port Speed**.
- 3 В этом меню имеется 2 варианта выбора, как показано на следующем рисунке:

Рис. 152 Меню 24.2: System Information and Console Port Speed

<p>Menu 24.2 - System Information and Console Port Speed</p> <ol style="list-style-type: none"> 1. Экран сведений о системе 2. Настройка скорости консольного порта

28.3.1 Информация о системе

Экран System Information содержит сведения о системе, показанные ниже. В частности, он сообщает протокол маршрутизации, Ethernet-адрес, IP-адрес и т.п.

Рис. 153 Меню 24.2.1: обслуживание системы – информация

Menu 24.2.1 - System Maintenance - Information	
Name: P-791Rv2	
Routing: IP	
ZyNOS F/W Version (Версия ZyNOS F/W): V3.40 (AWB.0)b2 4/ 12/2007	
SHDSL Chipset Vendor: IFX Soc2U 1.1-1.5.2__001	
Standard: ANSI (ANNEX_A)	
LAN	
Ethernet Address: 00:13:49:65:43:21	
IP Address: 192.168.1.1	
IP Mask: 255.255.255.0	
DHCP: Server	

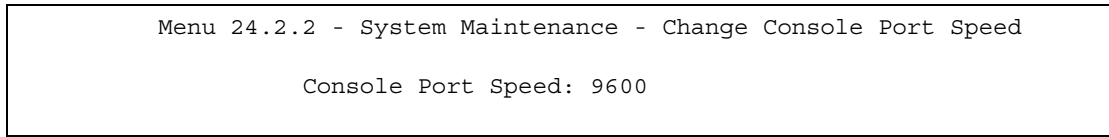
Поля изображённого выше экрана описаны в следующей таблице.

Таблица 82 Меню 24.2.1: обслуживание системы – информация

ПОЛЕ	ОПИСАНИЕ
Name	В этом поле отображается имя системы P-791R v2 и имя домена, назначенное в меню 1. Пример: System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Указывает на используемый протокол маршрутизации.
ZyNOS F/W Version	Отображает версию сетевой операционной системы ZyXEL.
SHDSL Chipset Vendor	Отображает тип чипсета SHDSL в устройстве P-791R v2.
Standard	Отображает протокол, используемый P-791R v2 и DSLAM (мультиплексором цифровых абонентских каналов).
LAN	
Ethernet Address	Отображает MAC-адрес устройства P-791R v2.
IP Address	В этом поле отображается IP-адрес P-791R v2 в десятичном виде через точку.
IP Mask	В этом поле отображается маска IP-подсети P-791R v2.
DHCP	В этом поле отображается режим DHCP, используемый P-791R v2.
Просмотрев настройки, нажмите [ESC] или [ENTER] для выхода.	

28.3.2 Настройка скорости консольного порта

Экран **Menu 24.2.2 – System Maintenance - Change Console Port Speed** позволяет изменить скорость консольного порта. Консольный порт P-791R v2 поддерживает следующие скорости передачи: 9600 (по умолчанию), 19200, 38400, 57600 и 115200 бит/с. Чтобы выбрать требуемую скорость, в меню 24.2.2 нажмите пробел и [ENTER].

Рис. 154 Меню 24.2.2: обслуживание системы: изменение скорости консольного порта

28.4 Регистрация и трассировка

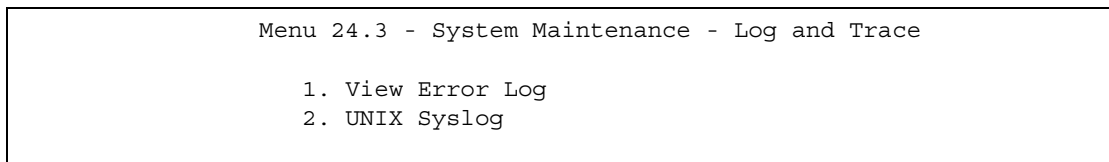
Устройство P-791R v2 реализует две функции ведения журналов. Первая – журналы ошибок и записи трассировки (отслеживания), сохраняемые локально. Вторая – регистрация сообщений на UNIX SYSLOG-сервере.

28.4.1 Просмотр журнала ошибок

При обнаружении любых неполадок следует в первую очередь сверяться с журналом ошибок/трассировки. Для просмотра локального журнала ошибок/трассировки необходимы следующие действия:

- 1 В главном меню введите 24, чтобы перейти в меню **Menu 24 - System Maintenance**.
- 2 В меню 24 введите 3, чтобы открыть раздел **Menu 24.3 - System Maintenance - Log and Trace**.
- 3 В разделе **Menu 24.3 - System Maintenance - Log and Trace** выберите первый пункт, чтобы просмотреть системный журнал ошибок.

После того, как P-791R v2 выведет журнал полностью, устройство предложит очистить журнал.

Рис. 155 Меню 24.3: обслуживание системы – журналы и трассировка

На следующем рисунке представлен типичный пример журнала с ошибками и информационными сообщениями.

Рис. 156 Примеры ошибок и информационных сообщений

```

34 Sat Jan 1 00:00:02 2000 PP05 -WARN SNMP TRAP 3: link up
35 Sat Jan 1 00:00:04 2000 PP00 INFO Channel 0 ok
36 Sat Jan 1 00:00:06 2000 PP0c INFO LAN promiscuous mode <0>
37 Sat Jan 1 00:00:06 2000 PP00 -WARN SNMP TRAP 0: cold start
38 Sat Jan 1 00:00:06 2000 PP00 INFO main: init completed
39 Sat Jan 1 00:00:06 2000 PP00 INFO Starting Connectivity Monitor
40 Sat Jan 1 00:00:06 2000 PP18 INFO adjtime task pause 1 day
41 Sat Jan 1 00:00:06 2000 PP19 INFO monitoring WAN connectivity
42 Sat Jan 1 00:00:06 2000 PP06 WARN MPOA Link Down
43 Sat Jan 1 04:10:22 2000 PP0c WARN netMakeChannDial: err=-3001
44 Sat Jan 1 04:10:42 2000 PP10 WARN Last errorlog repeat 18 Times
45 Sat Jan 1 04:10:42 2000 PP10 INFO SMT Password pass
46 Sat Jan 1 04:10:42 2000 PP00 INFO SMT Session Begin
47 Sat Jan 1 04:10:44 2000 PP0c WARN netMakeChannDial: err=-3001
48 Sat Jan 1 04:46:08 2000 PP00 WARN Last errorlog repeat 216 Times
49 Sat Jan 1 04:46:08 2000 PP00 INFO SMT Session End
51 Sat Jan 1 04:46:59 2000 PP0c WARN netMakeChannDial: err=-3001
52 Sat Jan 1 04:58:00 2000 PP10 WARN Last errorlog repeat 65 Times
53 Sat Jan 1 04:58:00 2000 PP10 INFO SMT Password pass
Clear Error Log (y/n):

```

28.4.2 Ведение журнала на SYSLOG-сервере

По протоколу SYSLOG P-791R v2 передает на сервер SYSLOG записи CDR (детализацию вызовов) и системные сообщения. Параметры SYSLOG и учета настраиваются на экране **Menu 24.3.2 - System Maintenance - Syslog Logging**, показанном ниже.

Рис. 157 Меню 24.3.2: обслуживание системы – UNIX SYSLOG

```

Menu 24.3.2 - System Maintenance - UNIX Syslog

UNIX Syslog:
Active= No
Syslog IP Address= 0.0.0.0
Log Facility= Local 1

```

Для активации системного журнала необходимо настроить параметры системного журнала, описанные в следующей таблице, затем следует выбрать, что нужно регистрировать.

Таблица 83 Меню 24.3.2: обслуживание системы - UNIX Syslog

ПОЛЕ	ОПИСАНИЕ
UNIX Syslog:	
Active	Чтобы включить или выключить ведение системного журнала, нажмите пробел и [ENTER].
Syslog IP Address	Введите имя или IP-адрес сервера SYSLOG, который будет принимать журнальные сообщения указанной категории.

Таблица 83 Меню 24.3.2: обслуживание системы - UNIX Syslog (продолжение)

ПОЛЕ	ОПИСАНИЕ
Log Facility	Нажмите пробел и [ENTER], чтобы выбрать журнальный объект. Распределение по журнальным объектам ("log facility") позволяет записывать сообщения на сервере в различные файлы. Подробности см. в документации на используемую программу ведения системного журнала.
Завершив настройку на этом экране, нажмите [ENTER] для подтверждения или [ESC] для отмены.	

P-791R v2 направляет в SYSLOG пять различных типов сообщений. Ниже показаны некоторые примеры сообщений (не все из них относятся строго к P-791R v2) и описан их формат:

1 CDR

Формат сообщения CDR
<pre>SdcmSyslogSend(SYSLOG_CDR, SYSLOG_INFO, строка); строка = board xx line xx channel xx, call xx, str board = идентификатор платы line = идентификатор платы в сети WAN channel = идентификатор канала в сети WAN call = код вызова, который начинается с 1 и увеличивается на 1 для каждого нового вызова str = C01 - исходящий вызов, dev xx, ch xx (dev: номер устройства, ch: номер канала) L02 - соединение туннеля (L2TP) C02 - соединение исходящего вызова xxxx (скорость соединения) xxxxx (номер вызова удаленной стороны) L02 - завершение вызова C02 - завершение вызова 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</pre>

2 Триггерный пакет

Формат сообщения о триггерном пакете
<pre>SdcmSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, строка); строка = Packet trigger: Protocol=xx Data=xxxxxxxxx.....x (Протокол=xx Данные=xxxxxxxxx.....x) Protocol: номер протокола (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: 48 шестнадцатеричных символов, отправляемых на сервер Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c02000100616263646566676869 6a6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008c d40000020405b4 Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d143013500400007 7600000</pre>

3 Журнал фильтра

<p>Формат сообщения в журнале фильтра</p> <pre>SdcmSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, строка); строка = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD IP[...] расшифровывает заголовок пакета, а S04>R01mD означает набор фильтров 4 (S), правило 1 (R), совпадение (m) и отбрасывание (D). Src: адрес источника Dst: адрес получателя prot: протокол ("TCP", "UDP", "ICMP") spo: исходный порт dpo: порт на удаленной стороне. Mar 03 10:39:43 202.132.155.97 ZyXEL: GEN[ffffffffnordff0080] }S05>R01mF Mar 03 10:41:29 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 10:41:34 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF Mar 03 11:59:20 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 12:00:52 202.132.155.97 ZyXEL: GEN[ffffffff0080] }S05>R01mF Mar 03 12:00:57 202.132.155.97 ZyXEL: GEN[00a0c5f502010080] }S05>R01mF Mar 03 12:01:06 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF</pre>
--

4 Журнал PPP

<p>PPP Log Message Format (Формат сообщения о журнале PPP)</p> <pre>SdcmSyslogSend(SYSLOG_PPLOG, SYSLOG_NOTICE, String) (SdcmSyslogSend(SYSLOG_PPLOG, SYSLOG_NOTICE, строка)); строка = ppp:prot Starting (запуск) / ppp:prot Opening (открытие) / ppp:prot Closing (закрытие) / ppp:prot Shutdown (завершение) prot = 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</pre>
--

28.5 Диагностика

Средства диагностики позволяют тестировать различные компоненты P-791R v2 для проверки их работоспособности. Меню 24.4 позволяет выбрать один из нескольких диагностических тестов для контроля состояния системы, как показано ниже. Доступные поля будут зависеть от модели устройства.

Для перехода в раздел **Menu 24.4 - System Maintenance - Diagnostic** следуйте приведенным ниже указаниям.

- 1 В главном меню введите 24, чтобы перейти в меню **Menu 24 - System Maintenance**.

2 В этом меню выберите пункт 4. Diagnostic. Откроется раздел **Menu 24.4 - System Maintenance - Diagnostic**.

Рис. 158 Меню 24.4: обслуживание системы - 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

```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 84 Меню 24.4: обслуживание системы – диагностика

ПОЛЕ	ОПИСАНИЕ
Reset xDSL	Введите 1, чтобы сбросить DSL-соединение на порту WAN.
Ping Host	Введите 12 для выполнения эхозапроса любой машины (с IP-адресом) в сети LAN или WAN. Введите IP-адрес в поле Адрес IP-хоста внизу.
Reboot System	Введите 11, чтобы перезагрузить P-791R v2.
Command Mode	Введите 22 для перехода в интерпретатор командной строки (КС) для углубленной диагностики. Войти в интерпретатор команд можно также через меню 24.8.
Host IP Address	Если в поле Enter Menu Selection Number был выбран пункт 1, укажите в этом поле IP-адрес компьютера для отправки эхозапроса.
Введите номер пункта или нажмите [ESC] для отмены.	

Работа с файлами микропрограмм и настроек

В этой главе описывается порядок резервного копирования и восстановления файла настроек, а также загрузка новых микропрограмм и файлов настроек.

29.1 Введение

Для изменения файла настроек и обновления микропрограммы P-791R v2 следуйте указаниям в этой главе. Завершив настройку P-791R v2, можно сохранить на компьютере резервную копию файла настроек. Это позволяет впоследствии, если настройки P-791R v2 будут ошибочно изменены, восстановить сохраненные значения из резервной копии файла настроек. Можно также загрузить файл с заводскими настройками, если требуется вернуть P-791R v2 к заводским настройкам. Все функции и возможности P-791R v2 реализуются микропрограммой. Обновления микропрограмм для улучшения работы P-791R v2 можно загрузить с сайта www.zyxel.ru.

29.2 Принятая схема именования файлов

Файл настроек (часто называемый romfile или rom-0) содержит заводские настройки по умолчанию в меню, такие как пароль, настройка DHCP, настройка TCP/IP и т.д. Файл настроек поставляется компанией ZyXEL с расширением в имени файла “rom”. После настройки параметров устройства P-791R v2 их можно сохранить на своем компьютере, присвоив имя файла по своему усмотрению.

Сетевая операционная система ZyNOS (ZyXEL Network Operating System, иногда называется файлом “ras”) – это микропрограмма, файл которой имеет расширение “bin”. Во многих FTP и TFTP-клиентах имена файлов указываются аналогично приведенным ниже примерам.

```
ftp> put firmware.bin ras
```

Это примерный фрагмент FTP-сеанса для передачи файла "firmware.bin" с компьютера в P-791R v2.

```
ftp> get rom-0 config.cfg
```

Это примерный фрагмент FTP-сеанса для сохранения текущих настроек в файле “config.cfg” .

Если ваш (Т)FTP-клиент не позволяет указать целевое имя файла, отличное от исходного, то файлы потребуется переименовать, поскольку P-791R v2 принимает только файлы с именами “rom-0” и “ras”. Для использования в дальнейшем сохраните неизменённые копии обоих файлов.

Общее описание файлов дано в следующей таблице. Внутренним именем файла называется имя файла в P-791R v2, а внешним именем файла называется имя файла вне P-791R v2, например, на диске компьютера, в локальной сети или на FTP-сервере, где оно может быть другим (не изменяется только расширение файла). Загрузив новую микропрограмму, проверьте версию микропрограммы в поле **ZyNOS F/W Version** на экране **Menu 24.2.1 - System Maintenance - Information**. Команда AT – та команда, которая вводится пользователем после нажатия “у” при появлении приглашения в меню SMT для перехода в режим отладки.

Таблица 85 Принятая схема именования файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл настроек	Rom-0	Это имя файла настроек в P-791R v2. При загрузке файла rom-0 замещается вся файловая система в ПЗУ устройства, включая настройки P-791R v2, системные данные (в т.ч. пароль по умолчанию), журнал ошибок и журнал трассировки.	*.rom
Firmware	Ras	Это имя файла микропрограммы ZyNOS в P-791R v2.	*.bin

29.3 Backup Configuration



В меню 24.5, 24.6, 24.7.1 и 24.7.2 устройство P-791R v2 объясняет различные способы резервного копирования, восстановления и загрузки файлов, в зависимости от того, осуществляется ли управление через консольный порт или по Telnet.

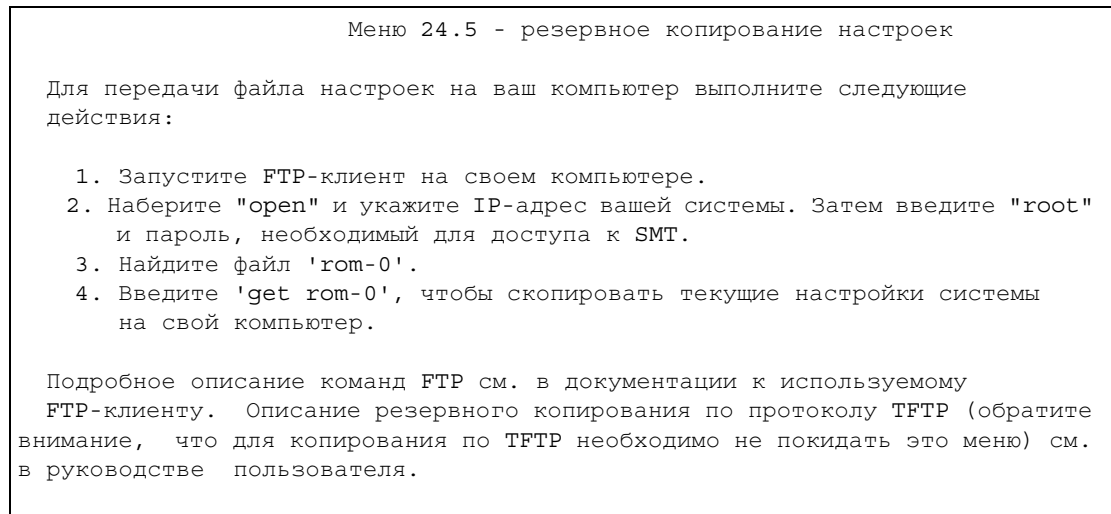
Пункт 5 в разделе **Menu 24 - System Maintenance** выполняет резервное копирование текущих настроек P-791R v2 на компьютер. Настоятельно рекомендуется выполнить резервное копирование после того, как устройство P-791R v2 будет приведено в рабочее состояние. Использование протокола FTP – предпочтительный метод резервного копирования текущих настроек на свой компьютер, поскольку он работает быстрее. Выполнять резервное копирование и восстановление в меню 24 можно также через консольный порт. Для этого годится любая программа связи через последовательные порты, однако для передачи и приема файлов необходимо использовать строго протокол Xmodem, а сами файлы не следует переименовывать.

Имейте в виду, что термины "загрузка" и "выгрузка" относятся к компьютеру. С P-791R v2 на компьютер, либо с компьютера в P-791R v2.

29.3.1 Резервное копирование настроек

Следуйте указаниям, приведенным на показанном ниже экране.

Рис. 159 Меню 24.5: Backup Configuration

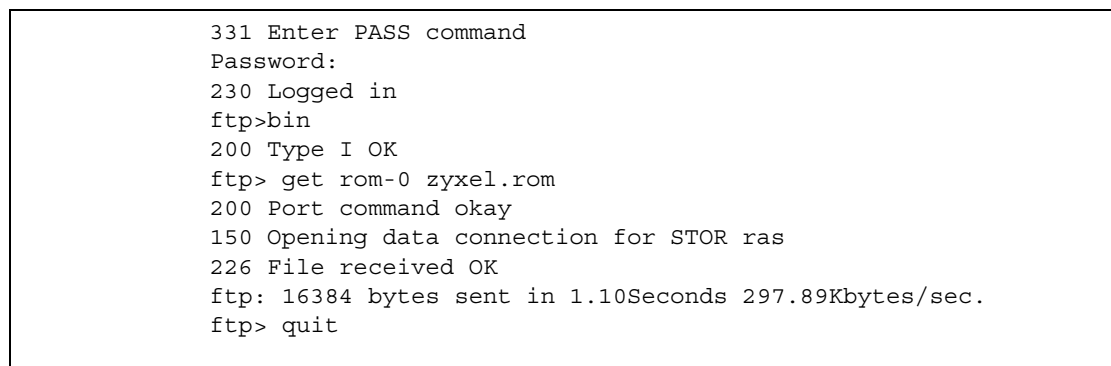


29.3.2 Выполнение команды FTP из командной строки

- 1 Запустите FTP-клиент на своем компьютере.
- 2 Наберите "open", пробел, и укажите IP-адрес P-791R v2.
- 3 Когда будет запрошено имя пользователя, нажмите [ENTER].
- 4 Введите пароль по требованию (по умолчанию – "1234").
- 5 Введите "bin" для установки бинарного режима передачи.
- 6 Для передачи файлов с P-791R v2 на компьютер используйте команду "get". Например, "get rom-0 config.rom" передает файл настроек с P-791R v2 на компьютер, сохраняя его под именем "config.rom". Подробнее о принятой схеме именования файлов см. выше в данной главе.
- 7 Введите "quit" для выхода из приглашения ftp.

29.3.3 Пример выполнения команд FTP из командной строки

Рис. 160 Пример сеанса FTP



29.3.4 Клиенты FTP на основе графического интерфейса пользователя

В следующей таблице описываются некоторые команды, которые можно увидеть в клиентах FTP на основе GUI (графического интерфейса пользователя).

Таблица 86 Общие команды для клиентов FTP на основе GUI.

КОМАНДА	ОПИСАНИЕ
Host Address	Введите адрес хост-сервера.
Login Type	Анонимный. Используется, когда идентификатор пользователя и пароль автоматически предоставляются серверу для анонимного доступа. Анонимная регистрация выполняется только в том случае, если оператор или администратор услуг включил эту опцию. Нормальный. Серверу требуется уникальный идентификатор пользователя и пароль для регистрации.
Transfer Type	Передача файлов в режиме ASCII (формат простого текста) или бинарном режиме. Файлы настроек и микропрограмм должны передаваться в двоичном режиме.
Initial Remote Directory	Укажите удаленную директорию по умолчанию (путь).
Initial Local Directory	Укажите локальную директорию по умолчанию (путь).

29.3.5 Управление файлами через WAN

В следующих случаях управление со стороны WAN по протоколам TFTP, FTP невозможно:

- 1 Служба Telnet отключена в меню 24.11.
- 2 Применен фильтр в меню 3.1 (LAN) или в меню 11.5 (WAN) для блокирования службы Telnet.
- 3 IP-адрес в поле **Secured Client IP** (IP-адрес защищенного клиента) в меню 24.11 не соответствует IP-адресу клиента. При таком несоответствии P-791R v2 немедленно прерывает сеанс Telnet.
- 4 Выполняется консольная сессия SMT.

29.3.6 Резервное копирование настроек посредством TFTP

P-791R v2 поддерживает загрузку / выгрузку микропрограмм и файла настроек с использованием TFTP (упрощенный протокол передачи файлов) через LAN. Хотя TFTP тоже должен работать через WAN, это не рекомендуется.

Для использования TFTP компьютер пользователя должен содержать клиентов telnet и TFTP. Для резервного копирования файла настроек выполните действия, указанные ниже.

- 1 Используйте telnet со своего компьютера для подключения к устройству P-791R v2 и зарегистрируйтесь. Поскольку TFTP не имеет системы проверки безопасности, P-791R v2 записывает IP-адрес клиента telnet и принимает запросы TFTP только с этого адреса.

- 2 Находясь в SMT, перейдите в интерпретатор команд (CI), набрав 8 в разделе **Menu 24 – System Maintenance**.
- 3 Введите команду “sys stdio 0” для отключения времени ожидания SMT, чтобы пересылка TFTP не прерывалась. Введите команду “sys stdio 5” для восстановления пятиминутного времени ожидания SMT (по умолчанию), когда завершится передача файлов.
- 4 Запустите клиент TFTP на своем компьютере и подключитесь к P-791R v2. Установите бинарный режим передачи перед тем, как начинать пересылку данных.
- 5 Используйте клиент TFTP (смотрите пример ниже) для передачи файлов между P-791R v2 и компьютером. Имя конфигурационного файла – “rom-0” (rom-ноль, а не заглавная буква "O").

Обратите внимание на то, что соединение telnet должно быть активным, и SMT должен находиться в режиме CI перед и во время передачи по TFTP. Для дополнительной информации о командах TFTP (смотрите следующий пример) обращайтесь к документации о программе-клиенте TFTP. При работе в системе UNIX используйте команду “get” для передачи файлов с P-791R v2 на компьютер и команду “binary” для установки режима передачи двоичных файлов.

29.3.7 Пример команды TFTP

Ниже дан пример команды TFTP:

```
tftp [-i] host get rom-0 config.rom
```

где "i" указывает на передачу в режиме двоичных файлов (используйте этот режим для передачи нетекстовых файлов), "host" – IP-адрес P-791R v2, "get" передает исходный файл в P-791R v2 (rom-0, имя файла настроек в P-791R v2) в целевой файл на компьютере и переименовывает его в config.rom.

29.3.8 Клиенты TFTP на основе графического интерфейса пользователя

В следующей таблице описываются некоторые поля, которые можно увидеть в клиентах TFTP на основе GUI (графического интерфейса пользователя).

Таблица 87 Общие команды для клиентов TFTP на основе GUI

КОМАНДА	ОПИСАНИЕ
Host	Введите IP-адрес P-791R v2. 192.168.1.1 – заводской IP-адрес P-791R v2.
Send/Fetch	"Send" ("Отправить") используется для загрузки файла в P-791R v2, а "Fetch" ("Получить") – для резервного копирования файла на компьютер.
Local File	Введите путь и имя файла микропрограммы (расширение *.bin) или файл настроек (расширение *.rom) в своем компьютере.
Remote File	Это имя файла настроек в P-791R v2. Имя файла микропрограммы - "ras", а для конфигурационного файла – "rom-0".
Binary	Передача файла в бинарном режиме.
Abort	Остановка передачи файла.

Настройки, запрещающие доступ по TFTP или FTP через WAN, описаны в [разд. 29.3.5 на стр. 258](#).

29.3.9 Резервное копирование через консольный порт

Ниже описана процедура резервного копирования через консольный порт с помощью программы NuregTerminal. Для других коммуникационных программ порядок действий будет аналогичным.

- 1 Откройте меню 24,5 и введите “y” на следующем экране.

Рис. 161 Обслуживание системы: Backup Configuration

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

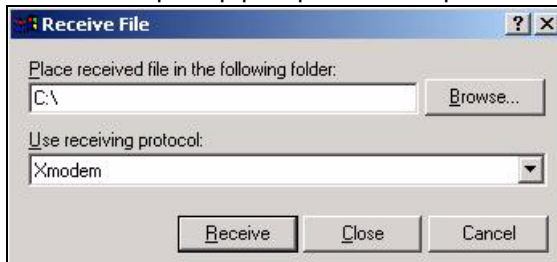
- 2 Следующий экран означает, что прием файла по протоколу Xmodem начался.

Рис. 162 Обслуживание системы: экран начала приема файла по Xmodem

```
You can enter ctrl-x to terminate operation any time.
Starting XMODEM download...
```

- 3 В программе NuregTerminal выберите **Transfer** (Передача) и **Receive File** (Принять файл), чтобы появилось окно, показанное ниже.

Рис. 163 Пример резервного копирования настроек



Введите путь для сохранения файла настроек или нажмите кнопку **Browse** (Обзор), чтобы указать местоположение файла.

Выберите протокол **Xmodem**.

Затем нажмите кнопку **Receive** (Принять).

- 4 После успешного выполнения резервного копирования появится следующий экран. Для возврата в меню SMT нажмите любую клавишу.

Рис. 164 Экран подтверждения выполнения резервного копирования

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

29.4 Восстановление настроек

В этом разделе показан способ восстановления ранее сохранённых настроек. Обратите внимание на то, что эта функция приводит к удалению текущей конфигурации перед восстановлением предыдущих настроек; не пытайтесь ее восстановить, если на диске не сохранен резервный файл настроек.

FTP – предпочтительный метод восстановления текущих настроек P-791R v2 с компьютера, поскольку FTP работает быстрее. Имейте в виду, что необходимо подождать, пока система не перезапустится автоматически после того, как завершится передача файла.



Не прерывайте процесс передачи файлов, иначе P-791R v2 может НЕОБРАТИМО ВЫЙТИ ИЗ СТРОЯ. После завершения восстановления настроек P-791R v2 автоматически перезагрузится.

29.4.1 Восстановление с использованием FTP

Для получения подробных сведений о резервном копировании с использованием (Т)FTP обращайтесь к разделам выше в данной главе, где описана загрузка файлов в устройство по протоколам FTP и TFTP.

Рис. 165 Меню 24.6: Restore Configuration

Меню 24.6 – восстановление настроек

Для передачи файла микропрограммы или настроек выполните следующие действия:

1. Запустите FTP-клиент на своем компьютере.
2. Наберите "open" и укажите IP-адрес вашей системы. Затем введите "root" и пароль, необходимый для доступа к SMT.
3. Введите "put резервная_копия rom-0", где резервная_копия – имя файла с резервной копией настроек на компьютере, а rom-0 – имя файла на удаленной системе. При этом будут восстановлены сохраненные настройки системы.
4. После успешного завершения передачи файла система автоматически перезагрузится.

Подробное описание команд FTP см. в документации к используемому FTP-клиенту. Описание восстановления настроек по протоколу TFTP (обратите внимание, что для восстановления по TFTP необходимо не покидать это меню) см. в руководстве пользователя.

- 1** Запустите FTP-клиент на своем компьютере.
- 2** Наберите "open", пробел, и укажите IP-адрес P-791R v2.
- 3** Когда будет запрошено имя пользователя, нажмите [ENTER].
- 4** Введите пароль по требованию (по умолчанию – "1234").

- 5 Введите "bin" для установки бинарного режима передачи.
- 6 На компьютере найдите файл "rom" для передачи в P-791R v2.
- 7 Используйте "put" для передачи файлов с компьютера на P-791R v2, например, команда "put config.rom-0" вызывает передачу файла настроек "config.rom", находящегося на компьютере, в P-791R v2. Подробнее о принятой схеме именования файлов см. выше в данной главе.
- 8 Введите "quit" для выхода из приглашения ftp. P-791R v2 автоматически перезагружается после успешного выполнения процесса восстановления.

29.4.2 Пример восстановления с использованием сеанса FTP

Рис. 166 Пример восстановления с использованием 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
```

Подробнее о настройках, запрещающих доступ по TFTP и FTP из сети WAN, см. в [разд. 29.3.5 на стр. 258](#).

29.4.3 Восстановление через консольный порт

Ниже описана процедура восстановления через консольный порт с помощью программы HyperTerminal. Для других коммуникационных программ порядок действий будет аналогичным.

- 1 Откройте меню 24,6 и введите "y" на следующем экране.

Рис. 167 Обслуживание системы: Restore Configuration

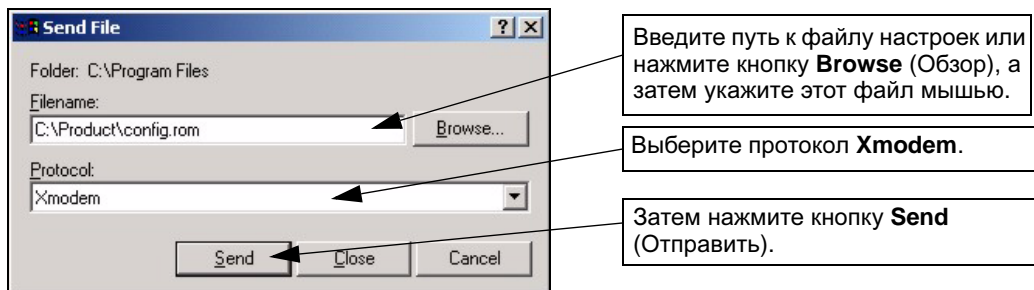
```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

- 2 Следующий экран означает, что прием файла по протоколу Xmodem начался.

Рис. 168 Обслуживание системы: экран начала приема файла по Xmodem

```
Starting XMODEM download (CRC mode) ...CCCCCCCC
```

- 3 Запустите программу HyperTerminal и выберите **Transfer** (Передача) и **Send File** (Отправить файл), чтобы появилось окно, показанное ниже.

Рис. 169 Пример восстановления настроек

- 4 После успешного восстановления настроек появится следующий экран. Нажмите любую клавишу, чтобы перезагрузить P-791R v2 и возвратиться в меню SMT.

Рис. 170 Экран подтверждения восстановления настроек

```
Save to ROM
Hit any key to start system reboot.
```

29.5 Загрузка микропрограммы и файлов настроек в устройство

В этом разделе описано, как загружать в устройство микропрограмму и файлы настроек. Для загрузки файлов настроек в устройство можно руководствоваться [разд. 29.4 на стр. 261](#) или указаниями на экране **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (при доступе через консольный порт).



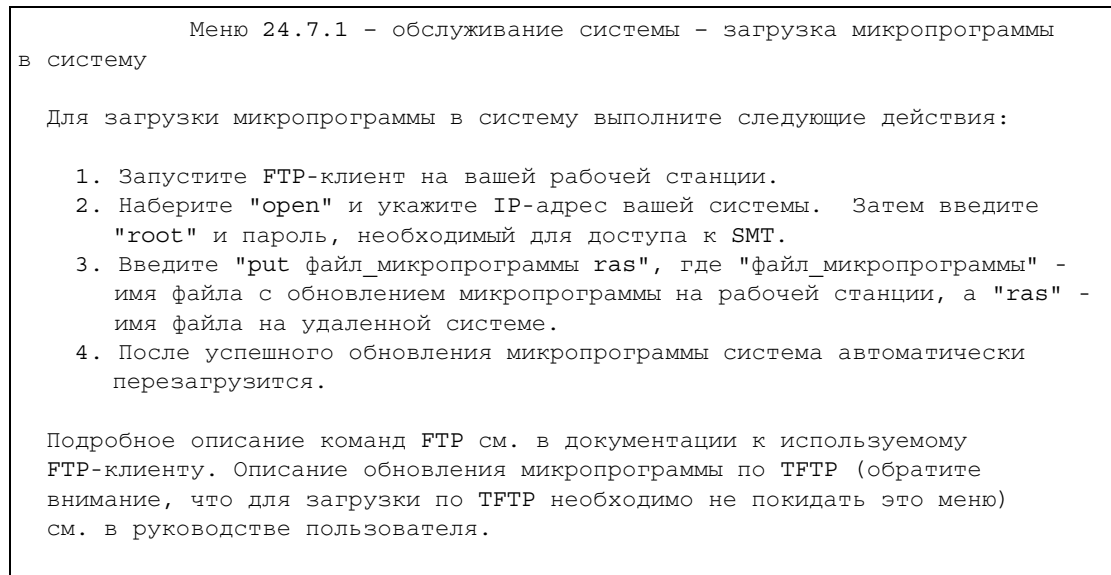
Не прерывайте процесс передачи файлов, иначе P-791R v2 может НЕОБРАТИМО ВЫЙТИ ИЗ СТРОЯ.

29.5.1 Загрузка файла микропрограммы в устройство

FTP – предпочтительный метод загрузки микропрограмм и файлов настроек. Для использования этой возможности ваш компьютер должен иметь FTP-клиента.

Если доступ к P-791R v2 осуществляется по протоколу Telnet, вы увидите следующие экраны, описывающие порядок загрузки микропрограмм и файлов настроек по FTP.

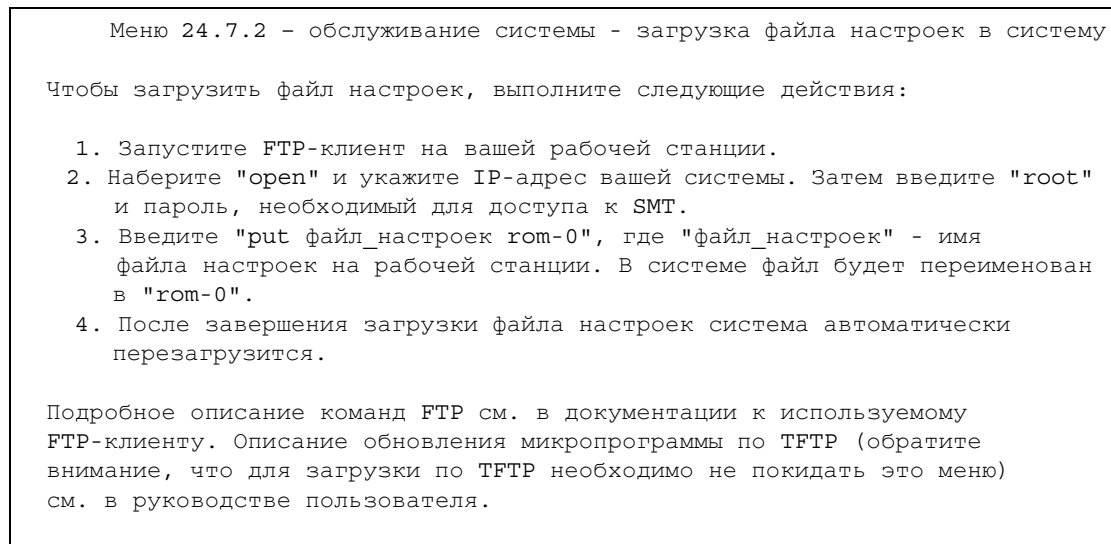
Рис. 171 Меню 24.7.1: обслуживание системы – загрузка микропрограммы



29.5.2 Загрузка файла настроек в устройство

При входе в меню 24.7.2 в сеансе Telnet отображается следующий экран.

Рис. 172 Меню 24.7.2: обслуживание системы – загрузка файла настроек



Для загрузки микропрограммы и файла настроек следуйте приведенным ниже примерам.

29.5.3 Пример команды загрузки файла по FTP из приглашения DOS

- 1 Запустите FTP-клиент на своем компьютере.
- 2 Наберите "open", пробел, и укажите IP-адрес P-791R v2.

- 3 Когда будет запрошено имя пользователя, нажмите [ENTER].
- 4 Введите пароль по требованию (по умолчанию – "1234").
- 5 Введите "bin" для установки бинарного режима передачи.
- 6 Для передачи файлов с компьютера в P-791R v2 используйте команду "put". Например, "put firmware.bin ras" передает микропрограмму с компьютера (firmware.bin) в P-791R v2 и переименовывает ее в "ras". Подобным образом команда "put config.rom rom-0" передает файл настроек с компьютера (config.rom) в P-791R v2, переименовывая его в "rom-0". Аналогичным образом "get rom-0 config.rom" обеспечивает передачу файла настроек с P-791R v2 в компьютер и переименование его в "config.rom". Подробнее о схеме именования файлов см. выше в этой главе.
- 7 Введите "quit" для выхода из приглашения ftp.

29.5.4 Пример сессии FTP для загрузки файла микропрограммы

Рис. 173 Пример сессии FTP для загрузки файла микропрограммы

```

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

```

Дополнительные команды (имеющиеся у клиентов FTP на основе GUI) перечислены выше в данной главе.

Настройки, запрещающие доступ по TFTP или FTP через WAN, описаны в [разд. 29.3.5 на стр. 258](#).

29.5.5 Загрузка файла по протоколу TFTP

P-791R v2 также поддерживает загрузку файлов микропрограмм через локальную сеть с использованием TFTP (упрощенного протокола передачи файлов). Хотя TFTP тоже должен работать через WAN, это не рекомендуется.

Для использования TFTP компьютер пользователя должен содержать клиентов telnet и TFTP. Для передачи микропрограммы и файла настроек выполните действия, указанные ниже.

- 1 Используйте telnet со своего компьютера для подключения к устройству P-791R v2 и зарегистрируйтесь. Поскольку TFTP не имеет системы проверки безопасности, P-791R v2 записывает IP-адрес клиента telnet и принимает запросы TFTP только с этого адреса.
- 2 Находясь в SMT, перейдите в интерпретатор команд (CI), набрав 8 в разделе **Menu 24 – System Maintenance**.

- 3 Введите команду “`sys stdio 0`” для отключения времени ожидания, чтобы пересылка TFTP не прерывалась. Введите команду “`command sys stdio 5`” для восстановления пятиминутного времени ожидания консоли (по умолчанию), когда завершится передача файлов.
- 4 Запустите клиент TFTP на своем компьютере и подключитесь к P-791R v2. Установите бинарный режим передачи перед тем, как начинать пересылку данных.
- 5 Используйте клиент TFTP (смотрите пример ниже) для передачи файлов между P-791R v2 и компьютером. Имя файла микропрограммы – “`ras`”.

Обратите внимание, что до и во время передачи по TFTP Telnet-соединение должно быть активным, а устройство P-791R v2 должно находиться в режиме командной строки. Для дополнительной информации о командах TFTP (смотрите следующий пример) обращайтесь к документации о программе-клиенте TFTP. При работе в системе UNIX используйте команду “`get`” для передачи от P-791R v2 к компьютеру, “`put`” – в обратном направлении и “`binary`” для установки режима бинарной передачи.

29.5.6 Пример команды загрузки по TFTP

Ниже дан пример команды TFTP:

```
tftp [-i] host put firmware.bin ras
```

где “`i`” указывает на передачу в режиме двоичных файлов (используйте этот режим для передачи нетекстовых файлов), “`host`” – IP-адрес P-791R v2, “`put`” передает исходный файл с компьютера (`firmware.bin` - имя файла микропрограммы на компьютере) в целевой файл на P-791R v2 и переименовывает его в `ras`.

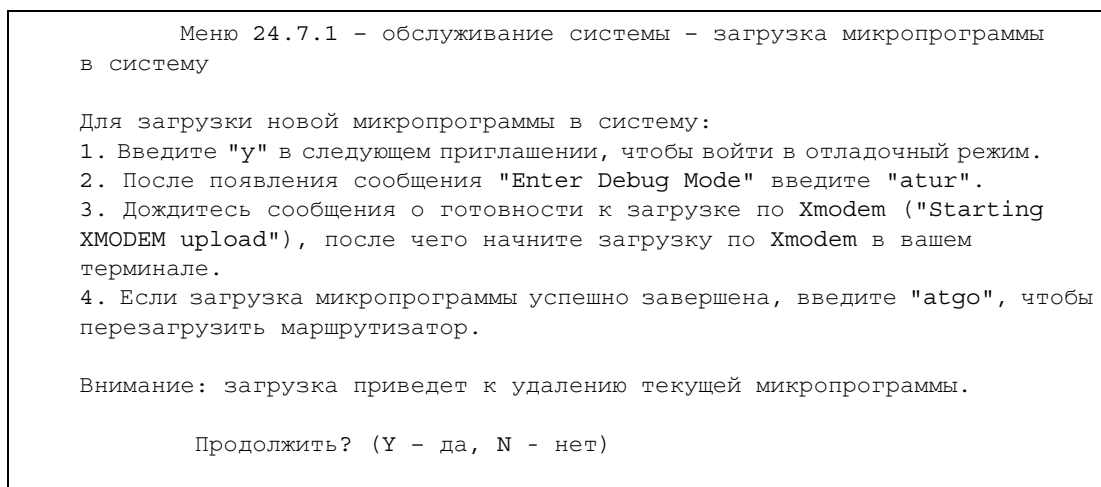
Команды, имеющиеся в клиентах TFTP на основе GUI, перечислены выше в данной главе.

29.5.7 Загрузка файлов в устройство через консольный порт

FTP и TFTP – рекомендуемые протоколы для загрузки микропрограмм в P-791R v2. Однако в случае недоступности устройства по сети загрузить файлы в P-791R v2 можно только по прямому соединению через консольный порт. В обычных случаях прибегать к загрузке через консольный порт не рекомендуется, поскольку FTP и TFTP отличаются намного большей скоростью. Для загрузки файлов годится любая программа связи через последовательные порты, однако для передачи и приема необходимо использовать строго протокол Xmodem.

29.5.8 Загрузка файлов микропрограммы через консольный порт

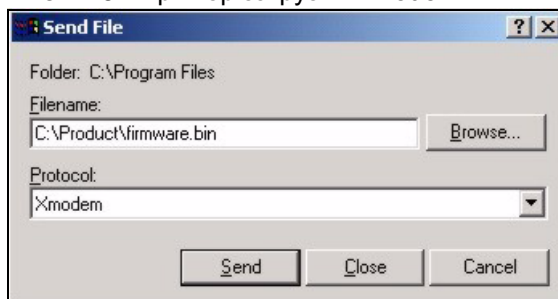
- 1 Находясь в разделе меню “`Menu 24.7 – System Maintenance – Upload Firmware`”, введите 1, чтобы перейти на экран “`Menu 24.7.1 - System Maintenance - Upload System Firmware`”, и следуйте указаниям на экране.

Рис. 174 Меню 24.7.1 при доступе через консольный порт

- 2 После появления сообщения "Starting Xmodem upload" запустите протокол Xmodem на компьютере. Для программы HyperTerminal следуйте указаниям, приведенным выше. Для других коммуникационных программ порядок действий будет аналогичным.

29.5.9 Пример загрузки файла микропрограммы по протоколу Xmodem с помощью программы HyperTerminal

Нажмите **Transfer** (Передача), затем **Send File** (Отправить файл). Появится следующий экран.

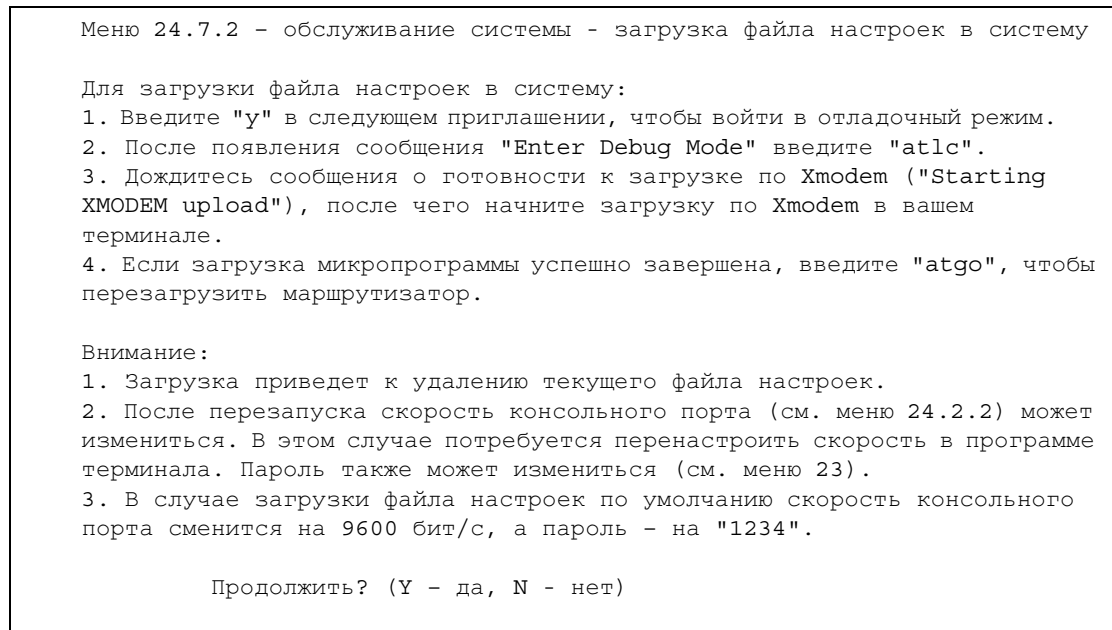
Рис. 175 Пример загрузки Xmodem

По завершении загрузки микропрограммы P-791R v2 автоматически перезагрузится.

29.5.10 Загрузка файлов настроек через консольный порт

- 1 В разделе "Menu 24.7 - System Maintenance - Upload Firmware" выберите 2, чтобы перейти на экран "Menu 24.7.2 - System Maintenance - Upload System Configuration File". Следуйте указаниям, приведенным на показанном ниже экране.

Рис. 176 Меню 24.7.2 при доступе через консольный порт

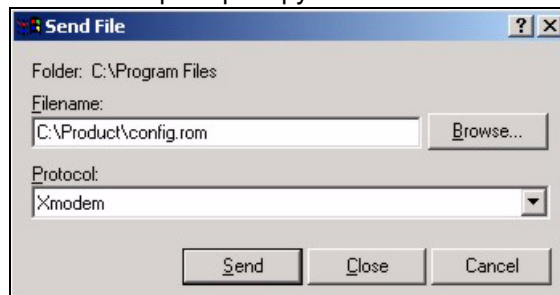


- 2 После появления сообщения "Starting Xmodem upload" запустите протокол Xmodem на компьютере. Для программы HyperTerminal следуйте указаниям, приведенным выше. Для других коммуникационных программ порядок действий будет аналогичным.
- 3 Введите "atgo", чтобы перезагрузить P-791R v2.

29.5.11 Пример загрузки файла настроек по протоколу Xmodem с помощью программы HyperTerminal

Нажмите **Transfer** (Передача), затем **Send File** (Отправить файл). Появится следующий экран.

Рис. 177 Пример загрузки по Xmodem



По завершении загрузки настроек необходимо перезагрузить P-791R v2, набрав команду "atgo".

Разделы меню с 24.8 по 24.11

В этой главе рассматриваются меню SMT 24.8 – 24.11.

30.1 Режим интерпретатора команд

Интерпретатор командной строки (КС) является частью микропрограммы маршрутизатора. СИ обеспечивает почти те же функциональные возможности, что и SMT, а также некоторые функции настройки низкого уровня и диагностики. Введите СИ из SMT, выбрав меню 24.8. Командная строка доступна по Telnet и на консольном порту. При этом некоторые команды доступны только через консольный порт. Подробную информацию о командах см. на прилагающемся компакт-диске или на www.zyxel.ru. В меню **Menu 24 - System Maintenance** введите 8.



Использование недокументированных команд или некорректное выполнение настроек может нарушить работоспособность устройства или вывести его из строя.

Рис. 178 Режим 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 (Режим интерпретатора
команд)
9. Call Control
10. Установка даты и времени
11. Remote Management
  
```

30.1.1 Синтаксис команд

Ключевые слова команд приводятся шрифтом Courier New.

Введите ключевые слова команд именно так, как показано ниже, не сокращая.

Обязательные поля команды заключены в угловые скобки <>.

Необязательные поля команды заключены в квадратные скобки [].

Знак "|" означает "или".

Например,

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

означает, что необходимо указать тип фильтра netbios и то, нужно ли его включить или выключить.

30.1.2 Использование команд

Чтобы получить список команд, в приглашении командной строки введите help или ?. Всегда вводите команду полностью. Введите "exit" для возвращения в главное меню SMT после завершения действий.

Рис. 179 Допустимые команды

```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          device         ether
wan          poe           xdsl           aux
config      etherdbg      ip             ppp
bridge      hdap          lan
ras>
```

30.2 Поддержка управления вызовами

В P-791R v2 предусмотрена функция управления вызовами для реализации бюджетных ограничений. Необходимо учесть, что это меню применяется только в том случае, когда в поле **Encapsulation** в меню 4 или 11.1 выбран режим **PPPoE** или **PPPoA**.

Функция управления бюджетом позволяет лимитировать на P-791R v2 суммарную продолжительность исходящих вызовов за определенный период времени. Если общее время исходящих вызовов превышает лимит, текущий вызов отбрасывается и все последующие исходящие вызовы блокируются.

История вызовов содержит сведения о предыдущих входящих и исходящих вызовах.

Для доступа к меню управления вызовом выберите пункт 9 в меню 24, чтобы перейти в раздел **Menu 24.9 — System Maintenance — Call Control**, показанный ниже.

Рис. 180 Меню 24.9: обслуживание системы – управление вызовами

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management
```

30.2.1 Управление бюджетом

В меню 24.9.1 показаны статистические данные об управлении бюджетом для исходящих вызовов. Введите 1 в разделе **Menu 24.9 - System Maintenance - Call Control** для открытия показанного ниже меню. Доступные поля будут зависеть от модели устройства.

Рис. 181 Меню 24.9.1 - Budget Management

Menu 24.9.1 - 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. -----	---	---

Общий бюджет – лимит времени в аккумулярованном периоде для вызовов, исходящих по направлению к удаленному узлу. Когда этот лимит достигнут, вызов отбрасывается и дальнейшие исходящие вызовы на этот удаленный узел блокируются. После завершения каждого периода общий бюджет сбрасывается. Значение по умолчанию для общего бюджета – 0 минут, период – 0 часов, что означает отсутствие управления бюджетом. Можно сбросить аккумулярованное время соединения в этом меню, введя индекс удаленного узла. Введите 0 для обновления этого экрана. Бюджет и период сброса можно настроить в меню 11.1 для удаленного узла.

Таблица 88 Меню 24.9.1 – управление бюджетом

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Remote Node	Введите порядковый номер удаленного узла, который необходимо сбросить (в данном случае только один).	1
Connection Time/ Total Budget	Это – общее истекшее время соединения (в пределах выделенного бюджета, установленного в меню 11.1).	5/10 означает, что израсходовано 5 минут из выделенных 10 минут.
Elapsed Time/Total Period	Этот период – цикл времени в часах, в соответствии с которым сбрасывается выделенный бюджет (см. меню 11.1). Время работы – это время, использованное в пределах данного периода.	0.5/1 означает, что израсходовано 30 минут из выделенного 1 часа.
Введите 0 для обновления экрана или нажмите [ESC] ([ВЫХОД]) для возвращения к предыдущему экрану.		

30.3 Установка даты и времени

В устройстве P-791R v2 имеются часы реального времени, хранящие текущее время и дату. Имеется также программный механизм установки времени вручную или получения текущего времени и даты с внешнего сервера при включении P-791R v2. Меню 24.10 позволяет обновить текущую дату и время в P-791R v2. Время отображается в журналах устройства P-791R v2.

Выберите меню 24 в главном меню для открытия меню **Menu 24 - System Maintenance**, как показано ниже.

Рис. 182 Меню 24: обслуживание 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. Установка даты и времени
11. Remote Management

```

Чтобы изменить настройки даты и времени в P-791R v2, перейдите в раздел **Menu 24.10 - System Maintenance - Time and Date Setting**, показанный на следующем рисунке.

Рис. 183 Меню 24.10: управление системой – настройка времени и даты

```

Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= None
Time Server Address= N/A

Current Time:                06 : 43 : 17
New Time (hh:mm:ss):        06 : 43 : 00

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2000 - 01 - 01

Time Zone= (GMT+0100) Brussels, Copenhagen, Madrid, Paris

Daylight Saving= No
Start Date (mm-nth-week-hr): Jan. - 1st - Sun.(02) - 00
End Date (mm-nth-week-hr):  Jan. - 1st - Sun.(02) - 00

```


Поля изображённого выше экрана описаны в следующей таблице.

Таблица 89 Меню 24.10: управление системой – настройка времени и даты

ПОЛЕ	ОПИСАНИЕ
Use Time Server When Bootup	Нажмите клавишу [SPACE BAR] ([ПРОБЕЛ]) и введите протокол службы времени, который используется сервером точного времени. Не все серверы точного времени поддерживают полный набор протоколов; обратитесь к оператору/администратору сети или подберите работающий протокол методом проб и ошибок. В основном они отличаются форматом. Формат Daytime (RFC 867) : день/месяц/год/часовой пояс, в котором находится сервер. Формат Time (RFC-868) : целое число длиной 4 байта, означающее количество секунд, прошедшее с 0:0:0 01.01.1970 (1970/1/1 в 0:0:0). По умолчанию используется протокол NTP (RFC-1305) , являющийся аналогом протокола Time (RFC-868) . Выберите None , чтобы вручную задать новое время и дату.
Time Server Address	Введите IP-адрес или имя домена сервера времени. Если вы не уверены в том, какие значения требуется ввести, обратитесь к провайдеру или администратору сети. Значение по умолчанию – tick.stdtime.gov.tw
Current Time	В этом поле отображается обновленное время только после повторного входа в это меню.
New Time (hh:mm:ss)	Введите новое время в формате “часы : минуты : секунды”.
Current Date	В этом поле отображается обновленная дата только после повторного входа в это меню.
New Date (yyyy-mm-dd)	Введите новую дату в формате “год – месяц – день”.
Time Zone	Нажмите пробел и [ENTER] для установки разницы во времени между данной временной зоной и гринвичским временем (GMT).
Daylight Saving	Летнее время – это период между поздней весной и началом осени, когда во многих странах стрелки переводятся вперед на 1 час по отношению к обычному местному времени, чтобы продлить светлое время в конце дня. Если нужно использовать переход на летнее время, выберите Yes (Да) .
Start Date (mm-dd): (Начальная дата (месяц-день))	Укажите месяц и день перехода на летнее время, если в поле Enable Daylight Saving (Разрешить переход на летнее время) выбрано значение Yes . В поле hr используется 24-часовой формат. Примеры: На большей части территории США летнее время начинается во второе воскресенье марта. Для каждого часового пояса летнее время в США начинает действовать с 2:00 по местному времени. Поэтому для США необходимо выбрать Second, Sunday, March . В Европейском союзе и в России летнее время начинается в последнее воскресенье марта. Во всех часовых поясах на территории Евросоюза летнее время начинается одновременно (в 1:00 по Гринвичу или UTC). В странах Евросоюза необходимо выбрать Mar., Last, Sun . Время, вводимое в поле hr , зависит от вашего часового пояса. Например, для Германии, где время на один час опережает гринвичское (GMT+1), следует ввести 2.

Таблица 89 Меню 24.10: управление системой – настройка времени и даты

ПОЛЕ	ОПИСАНИЕ
End Date (mm-dd): (Конечная дата (месяц-день))	<p>Укажите месяц и день перехода на зимнее время, если в поле Enable Daylight Saving (Разрешить переход на летнее время) выбрано значение Yes. В поле hr используется 24-часовой формат. Примеры:</p> <p>В США летнее время заканчивается в первое воскресенье ноября. Для каждого часового пояса летнее время в США заканчивает действовать в 2:00 по местному времени. Поэтому для США необходимо выбрать First, Sunday, November.</p> <p>В Европейском союзе и в России летнее время заканчивается в последнее воскресенье октября. Во всех часовых поясах на территории Евросоюза летнее время заканчивается одновременно (в 1:00 по Гринвичу или UTC). В странах Евросоюза необходимо выбрать Oct., Last, Sun. Время, вводимое в поле hr, зависит от вашего часового пояса. Например, для Германии, где время на один час опережает гринвичское (GMT+1), следует ввести 2.</p>
<p>После завершения работы с данным меню нажмите клавишу [ENTER] ([ВВОД]) в сообщении "Press ENTER to Confirm or ESC to Cancel" ("Нажмите ВВОД для подтверждения или ВЫХОД для Отмены") для сохранения конфигурации или клавишу [ESC] ([ВЫХОД]) для отмены операции.</p>	

30.4 Удаленное управление

Для отключения удаленного доступа через одну из служб выберите **Disable** в соответствующем поле **Server Access**. Введите 11 в меню 24, чтобы открыть раздел **Menu 24.11 – Remote Management Control**.

Рис. 184 Меню 24.11 – настройка удаленного управления

Menu 24.11 - Remote Management Control	
TELNET Server: Server Port = 23 Secured Client IP = 0.0.0.0	Server Access = ALL
FTP Server: Server Port = 21 Secured Client IP = 0.0.0.0	Server Access = ALL
Web Server: Server Port = 80 Secured Client IP = 0.0.0.0	Server Access = ALL

Поля изображённого выше экрана описаны в следующей таблице.

Таблица 90 Меню 24.11 – настройка удаленного управления

ПОЛЕ	ОПИСАНИЕ
TELNET Server FTP Server Web Server	Каждое из этих не редактируемых полей обозначает тип сетевой службы, используемой для дистанционного управления P-791R v2.
Server Port	В данном поле показан номер порта для службы или протокола. При необходимости можно изменить номер порта, но для доступа к P-791R v2 можно использовать только этот номер порта.

Таблица 90 Меню 24.11 – настройка удаленного управления (продолжение)

ПОЛЕ	ОПИСАНИЕ
Server Access	Если требуется указать интерфейс доступа, нажмите пробел и [ENTER], чтобы выбрать один из следующих вариантов: LAN only (Только LAN) , WAN only (Только WAN) , ALL (ВСЕ) или Disable (Отключить) .
Secured Client IP	Значение по умолчанию 0.0.0.0 позволяет любому клиенту использовать эту службу или протокол для дистанционного управления P-791R v2. Введите IP-адрес для ограничения доступа к клиенту с соответствующим IP-адресом.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel" для сохранения настроек или клавишу [ESC] для отмены.	

30.4.1 Ограничения удаленного управления

Удаленное управление через LAN или WAN не работает в следующих случаях:

- 1 Фильтр в меню 3.1 (LAN) или в меню 11.5 (WAN) применяется для блокировки служб Telnet, FTP или веб-служб.
- 2 Данная служба отключена в меню 24.11.
- 3 IP-адрес в поле **Secured Client IP (Надежный IP-адрес клиента)** (меню 24.11) не соответствует IP-адресу клиента. При таком несоответствии P-791R v2 немедленно прерывает сеанс.
- 4 Выполняется консольная сессия SMT.
- 5 Уже выполняется другой сеанс удаленного управления с равным или более высоким приоритетом. В каждый момент времени может выполняться только один сеанс удаленного управления.

Настройка политик маршрутизации IP

Это меню служит для просмотра и настройки политик маршрутизации.

31.1 Назначение политик маршрутизации

Обычно решения о маршрутизации принимаются только по адресу получателя, и P-791R v2 выбирает для отправки пакета кратчайший путь. Политика маршрутизации IP (IPPR) реализует алгоритм, заменяющий стандартный механизм маршрутизации и позволяющий изменить правила пересылки пакетов в зависимости от политики, настраиваемой администратором. Политики применяются ко входящим пакетам на каждом интерфейсе до обычной маршрутизации.

31.2 Преимущества

- Маршрутизация на основе источников – администраторы сетей могут использовать маршрутизацию на основе политик для пересылки трафика от различных пользователей по разным соединениям.
- Ограничение полосы пропускания – применение политик маршрутизации в корпоративной среде позволяет классифицировать трафик по приоритетам, распределяя полосу пропускания требуемым образом.
- Экономия – IPPR позволяет организациям направлять ценный интерактивный трафик через дорогостоящие широкополосные каналы, а для пакетных передач использовать более дешевые маршруты.
- Распределение нагрузки – администраторы сетей могут использовать IPPR для распределения трафика по нескольким путям.
- NAT – P-791R v2 по умолчанию применяет NAT к трафику, проходящему через интерфейс **ge1**. Защищенный механизм трансляции адресов (SNAT), реализуемый политиками маршрутизации, позволяет администраторам задавать определенный IP-адрес источника для трафика, принимаемого через определенные интерфейсы.

31.3 Политики маршрутизации

Отдельные политики маршрутизации являются частью общей схемы IPPR. Политика определяет критерии сравнения и действия, выполняемые над пакетами, которые отвечают этим критериям. Действие выполняется только при удовлетворении всем критериям. Критериями могут являться: имя пользователя, исходный адрес и входной интерфейс, адрес получателя, расписание, протокол IP (ICMP, UDP, TCP и т. п.) и номер порта.

Могут выполняться следующие действия:

- Пересылка пакета через другой шлюз, выходной интерфейс, или группу каналов.
- Ограничение доступной полосы пропускания и упорядочение трафика по приоритетам.

Структура и реализация IPPR во многом повторяет существующее средство фильтрации пакетов в составе RAS.

31.4 IP Routing Policy Setup

Это меню служит для просмотра сводки политик маршрутизации. Чтобы открыть это меню, в основном меню введите 25.

Рис. 185 Меню 25: IP Routing Policy Setup

Menu 25 - IP Routing Policy Setup			
Policy Set #	Name	Policy 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

- 1 Выберите набор фильтров, которые необходимо настроить (1-12), и нажмите [ENTER].
- 2 Введите описательное название или комментарий в поле **Edit Name** и нажмите [ENTER].
- 3 В сообщении [Press ENTER to confirm] нажмите [ENTER], чтобы войти в раздел **Menu 25.1 - IP Routing Policy Setup**.

31.5 IP Routing Policy Setup

Этот раздел меню служит для поиска политик маршрутизации. Для входа в это меню укажите номер и название политики маршрутизации из меню 25.

Рис. 186 Меню 25.1: IP Routing Policy Setup

```

Menu 25.1 - IP Routing Policy Setup

# A                               Criteria/Action
-----
1 N 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:

```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 91 Меню 25.1: настройка политик маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается номер правила.
Criteria/Action	См. таб. 92 на стр. 279.
Enter Policy Rule Number (1-6) to Configure:	Введите номер редактируемого правила.

Таблица 92 Меню 25: настройка политик маршрутизации IP, сокращения

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
SA	IP-адрес источника
SP	Порт источника
DA	IP-адрес получателя
DP	Порт получателя
P	Номер IP-протокола 4-го уровня (TCP=6, UDP=17...)
T	Тип обслуживания (ToS) во входящем пакете
PR	Приоритет входящего пакета
Действия: GW	IP-адрес шлюза
T	Тип службы для исходящего трафика
P	Приоритет исходящего трафика

Таблица 92 Меню 25: настройка политик маршрутизации IP, сокращения

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
Уровень обслуживания: NM	Обычный
MD	Минимальная задержка
MT	Максимальная пропускная способность
MR	Максимальная надежность
MC	Минимальная стоимость

31.6 Меню IP Routing Policy

Это меню служит для настройки маршрутов в соответствии с политиками. Для входа в это меню, находясь в меню 25, выберите **Edit** и введите соответствующий номер правила.

Рис. 187 Меню 25.1.1: меню IP Routing Policy

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= ex1
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 type      = Gateway addr    Gateway addr    = 0.0.0.0
Type of Service= No Change          Gateway node    = 0
Precedence       = No Change        Log= No
    
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 93 Меню 25.1.1: политика маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
Policy Set Name	В этом поле указывается описательное название политики маршрутизации, выбранной в меню Menu 25.1 - IP Routing Policy Summary .
Active	Чтобы активировать политику, выберите Yes , нажав пробел и [ENTER].
Criteria	
IP Protocol	Введите номер протокола уровня 4 IP. Например, UDP=17, TCP=6, ICMP=1, любой протокол=0.

Таблица 93 Меню 25.1.1: политика маршрутизации IP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Type of Service	Укажите приоритет входящего трафика: Don't Care (не имеет значения), Normal (нормальный), Min Delay (минимальная задержка), Max Thruput (максимальная скорость передачи) и Max Reliable (максимальная надежность).
Precedence	Приоритет входящего пакета. Нажмите пробел и [ENTER], чтобы выбрать приоритет из списка: от 0 до 7 или Don't Care (не имеет значения).
Packet Length	Введите длину входящих пакетов (в байтах). Операторы в следующем поле (Len Comp) применяются к пакетам этой длины.
Len Comp	Нажмите пробел и ENTER, чтобы выбрать критерий сравнения длины: Equal (равно), Not Equal (не равно), Less (меньше), Greater (больше), Less or Equal (меньше или равно) или Greater or Equal (больше или равно).
Source	
addr start / end	Начало и конец диапазона IP-адресов источника.
port start / end	Начало и конец диапазона номеров портов источника (только для протоколов TCP/UDP).
Destination	
addr start / end	Начало и конец диапазона IP-адресов адресата.
port start / end	Начало и конец диапазона номеров портов адресата (только для протоколов TCP/UDP).
Action	Указывает, должно ли описанное действие выполняться при соответствии или несоответствии критериям.
Gateway Type	Нажмите клавишу [SPACE BAR] ([ПРОБЕЛ]), а затем — клавишу [ENTER] ([ВВОД]), чтобы выбрать Gateway addr и введите IP-адрес шлюза, если его необходимо указать. Шлюз — это непосредственно соседствующая с P-791R v2 система, которая направляет пакет к месту назначения. Необходимо, чтобы в качестве шлюза использовался маршрутизатор того же сегмента, к которому относится порт LAN или WAN устройства P-791R v2. Нажмите клавишу [SPACE BAR] ([ПРОБЕЛ]), а затем — [ENTER] ([ВВОД]) для выбора Gateway node , чтобы ввести номер удаленного узла шлюза, если необходимо, чтобы устройство P-791R v2 доставляло трафик, соответствующий политике маршрутизации данных через определенный порт WAN.
Gateway addr	Если выбран Gateway addr в поле Gateway type , введите IP-адрес шлюза, которому P-791R v2 направляет пакет. Шлюз должен непосредственно соседствовать с P-791R v2, находясь в одной подсети с P-791R v2, если он относится к сети LAN, или иметь IP-адрес удаленного узла, если он относится к сети WAN. Чтобы указать шлюз по умолчанию, введите 0.0.0.0.
Type of Service	Укажите новое значение TOS для исходящего пакета, выбрав No Change (без изменения), Normal (нормальный), Min Delay (минимальная задержка), Max Thruput (максимальная скорость передачи), Max Reliable (максимальная надежность) или Min Cost (минимальная стоимость).
Gateway Node	Если выбран Gateway node в поле Gateway type , введите номер удаленного узла (от 1 до 8), которому P-791R v2 направляет пакет. Удаленный узел представляет как удаленный межсетевой шлюз, так и сеть, находящуюся за ним в соединении WAN. Для получения дополнительной информации о настройке профиля удаленного узла см. Меню 11: Remote Node Setup в разд. 22.2 на стр. 195.

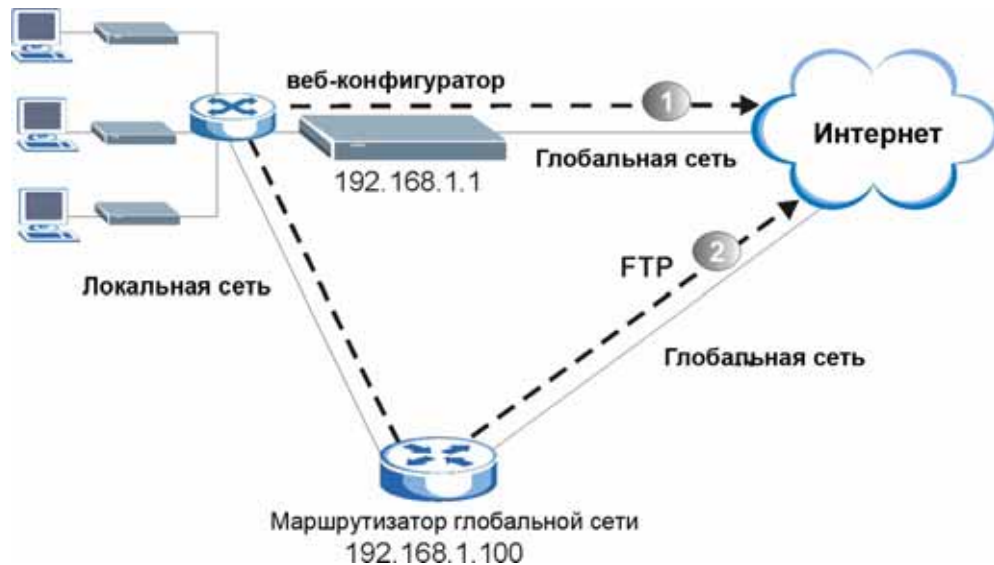
Таблица 93 Меню 25.1.1: политика маршрутизации IP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Precedence	Укажите новый приоритет исходящего пакета, выбрав одно из значений: от 0 до 7 или Don't Care (не имеет значения).
Log	Чтобы оставлять в системном журнале отметку при выполнении политики, выберите Yes , нажав пробел и [ENTER].

31.7 Пример IP-маршрутизации с использованием политик

Если одна сеть имеет соединения с Интернетом и удаленным узлом, можно использовать две разные политики: для маршрутизации пакетов WWW в Интернет и для маршрутизации пакетов FTP в удаленную сеть. Этот пример проиллюстрирован на следующем рисунке.

Маршрут 1 является маршрутом IP по умолчанию, а маршрут 2 представляет собой отдельно настроенный маршрут IP.

Рис. 188 Пример IP-маршрутизации с использованием политик

Чтобы принудительно перенаправлять пакеты WWW от клиентов с IP-адресами из диапазона 192.168.1.33 – 192.168.1.64 в Интернет через порт WAN на устройстве ZyWALL, выполните следующие операции.

- 1 Создайте правило в меню **Menu 25.1 - IP Routing Policy Setup**, как показано ниже.

Рис. 189 Политика маршрутизации IP. Пример 1.

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= example1
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care          Packet length= 10
  Precedence      = Don't Care          Len Comp= Equal
Source:
  addr start= 192.168.1.33             end= 192.168.1.64
  port start= 0                        end= N/A
Destination:
  addr start= 0.0.0.0                  end= N/A
  port start= 80                       end= 80
Action= Matched
Gateway addr      = 192.168.1.1        Log= No
Type of Service= Max Thruput
Precedence       = 0

```

- 2 Чтобы применить политику к пакетам, получаемым через порт LAN, в меню 25.1.1 выберите **Yes** в поле **LAN**.
- 3 Проверьте, успешно ли добавлено правило, в разделе **Menu 25 - IP Routing Policy Summary**.
- 4 В меню 25.1 создайте новое правило, разрешающее пересылать пакеты от любого хоста (IP-адрес 0.0.0.0 обозначает любой хост) по протоколу TCP для порта FTP через другой шлюз (192.168.1.100).

Рис. 190 Политика маршрутизации IP. Пример 2.

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= example2
Active= No
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care          Packet length= 10
  Precedence      = Don't Care          Len Comp= Equal
Source:
  addr start= 0.0.0.0                  end= N/A
  port start= 0                        end= N/A
Destination:
  addr start= 0.0.0.0                  end= N/A
  port start= 20                       end= 21
Action= Matched
Gateway addr      = 0.0.0.0            Log= No
Type of Service= No Change
Precedence       = No Change

```

- 5 Проверьте, успешно ли добавлено правило, в разделе **Menu 25 - IP Routing Policy Summary**.

Настройка расписания

Это меню служит для просмотра и настройки наборов расписаний в P-791R v2.

32.1 Краткие сведения о наборах расписаний

Расписания вызовов (применяется только для инкапсуляции PPPoA или PPPoE) позволяют P-791R v2 определять, когда и на какое время должен вызываться удаленный узел. Эта функция подобна функции планировщика, в котором можно указывать период времени для записи телевизионной программы на видеокассету или систему цифрового телевидения.

32.2 Настройка расписания

Это меню действует только для соединений с Интернетом, использующих инкапсуляцию PPPoE. Это меню служит для просмотра наборов расписаний в P-791R v2. Чтобы открыть это меню, в основном меню введите 26.

Рис. 191 Меню 26: настройка расписания

```

Menu 26 - Schedule Setup

Schedule                               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

```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 94 Меню 26: настройка расписания

ПОЛЕ	ОПИСАНИЕ
1-12	В этом поле отображается начало названия каждого набора расписаний. Наборы с более низкими номерами обладают приоритетом над наборами с более высокими номерами, что позволяет избежать конфликтов между расписаниями. Например, если к удаленному узлу применяются наборы 1, 2, 3 и 4, набор 1 имеет приоритет над наборами 2, 3 и 4.
Enter Schedule Set Number to Configure	Для настройки набора расписаний введите в этом поле номер статического маршрута, в поле Edit Name введите имя расписания, затем нажмите [ENTER]. Появится меню 26.1. Чтобы удалить набор расписаний, введите в этом поле номер статического маршрута, в поле Edit Name оставьте пустое имя и нажмите [ENTER].
Edit Name	Введите имя настраиваемого расписания или оставьте поле пустым, чтобы удалить указанный набор расписаний.

32.3 Настройка набора расписаний

Это меню действует только для соединений с Интернетом, использующих инкапсуляцию PPPoE. Это меню служит для настройки наборов расписаний в P-791R v2. Чтобы открыть это меню, введите номер набора расписаний в поле **Enter Schedule Set Number to Configure**, введите имя набора расписаний в поле **Edit Name** и нажмите [ENTER] в меню 26.

Рис. 192 Меню 26.1: настройка набора расписаний

```

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

```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 95 Меню 26.1: настройка набора расписаний

ПОЛЕ	ОПИСАНИЕ
Active	Нажмите клавишу [SPACE BAR] ([ПРОБЕЛ]) для выбора значения Yes (Да) или No (Нет) . Выберите Yes и нажмите [ENTER] для активации набора расписаний.
Start Date	Должен ли набор расписаний повторяться еженедельно или использоваться только один раз? Нажмите пробел, затем - [ENTER], чтобы выбрать Once (однократно) или Weekly (еженедельно). Эти опции взаимоисключающие. Если выбрано значение Once (Один раз) , все настройки рабочего дня недоступны (N/A). При выборе значения Once (Один раз) правило расписания удаляется автоматически после истечения времени расписания.
How Often	Введите дату начала, когда набор должен вступить в силу, в формате год – месяц – дата. Действительными датами являются все даты от текущей до 5 февраля 2036 г.
Once	
Date	Если в поле How Often выбрано значение Once , введите дату, когда набор должен активироваться, в формате год-месяц-день.
Weekdays	При выборе значения Weekly в поле How Often , укажите дни, в которые набор должен активироваться (и повторяться), перейдя к соответствующим дням и нажав пробел для выбора значения Yes , затем нажмите [ENTER].
Start Time	Введите время начала, когда набор расписаний должен вступать в силу, в формате час – минута.
Duration	Введите максимальную длину времени данного соединения в формате час – минута.
Action	<p>Forced On (Принудительное) означает, что соединение устанавливается независимо от того, есть ли вызов с запросом на линии, и будет поддерживаться в течение того периода времени, который указан в поле Duration (Продолжительность).</p> <p>Forced Down (Принудительное отключение) означает, что соединение блокируется независимо от того, есть ли вызов с запросом на линии.</p> <p>Enable Dial-On-Demand (Включить набор по требованию) означает, что это расписание допускает вызов по требованию на линии.</p> <p>Disable Dial-On-Demand (Выключить набор по требованию) означает, что это расписание не допускает вызов по требованию на линии.</p>

Поиск и устранение неполадок

В этой главе приведены рекомендации по решению возможных проблем. Проблемы сгруппированы в несколько категорий.

- [Питание, подключение оборудования, светодиоды](#)
- [Доступ к на P-791R v2 и вход в систему](#)
- [Доступ к Интернету](#)

33.1 Питание, подключение оборудования, светодиоды



на P-791R v2 не включается. Не горит ни один светодиод.

- 1 Убедитесь, что питание на P-791R v2 включено.
- 2 Убедитесь, что используются шнур и источник питания из комплекта поставки на P-791R v2.
- 3 Убедитесь, что блок питания или шнур соединены с на P-791R v2 и включены в соответствующую розетку. Убедитесь, что источник питания включен.
- 4 Выключите на P-791R v2 и включите устройство снова.
- 5 Если проблему не удастся устранить, обратитесь к поставщику.



Показания одного из светодиодов не соответствуют обычному состоянию.

- 1 Убедитесь, что вы верно понимаете показания светодиодов в нормальном режиме. См. [разд. 1.4 на стр. 35](#).
- 2 Проверьте правильность подключения оборудования. См. Руководство по быстрому запуску.
- 3 Осмотрите кабели на предмет повреждений. Для замены поврежденных кабелей обратитесь к поставщику.
- 4 Выключите на P-791R v2 и включите устройство снова.
- 5 Если проблему не удастся устранить, обратитесь к поставщику.

33.2 Доступ к на P-791R v2 и вход в систему



Утерян IP-адрес на P-791R v2.

- 1 По умолчанию устройству присвоен IP-адрес **192.168.1.1**.
- 2 Подключитесь к на P-791R v2 через консольный порт (имеет внешний порт консоли).
- 3 Если вы изменили IP-адрес устройства и забыли его, узнать IP-адрес на P-791R v2 можно, сверившись с IP-адресом шлюза по умолчанию на вашем компьютере. В большинстве компьютеров с ОС Windows это можно сделать, выбрав **Start (Пуск) > Run (Выполнить)**, введя **cmd** и набрав **ipconfig**. Полученный IP-адрес шлюза по умолчанию (**Default Gateway**) может совпадать с IP-адресом на P-791R v2 (это зависит от конфигурации сети). Попробуйте ввести этот IP-адрес в браузере.
- 4 Если обратиться к устройству таким путем не получилось, может потребоваться возврат к заводским настройкам. См. [разд. 33.4 на стр. 293](#).



Утерян пароль.

- 1 Пароль по умолчанию – **1234**.
- 2 Если обратиться к устройству таким путем не получилось, может потребоваться возврат к заводским настройкам. См. [разд. 33.4 на стр. 293](#).



Не удается войти в веб-конфигуратор или обратиться к экрану Login.

- 1 Убедитесь, что IP-адрес введен верно.
 - По умолчанию устройству присвоен IP-адрес **192.168.1.1**.
 - Если вы изменили IP-адрес устройства (см. [разд. 6.3 на стр. 91](#)), используйте новый IP-адрес.
 - Если вы изменили IP-адрес устройства и впоследствии забыли его, обратитесь к указаниям, приведенным в подразделе [Утерян IP-адрес на P-791R v2..](#)
- 2 Проверьте подключения оборудования и убедитесь, что показания светодиодов соответствуют норме. См. Руководство по быстрому запуску и [разд. 33.1 на стр. 289](#).
- 3 Убедитесь, что ваш браузер не блокирует всплывающие окна (pop-up) и в нем включена поддержка JavaScript и Java. См. [Приложение С на стр. 319](#).
- 4 Убедитесь, что компьютер находится в одной подсети с на P-791R v2. (Если вам известно, что между компьютером и на P-791R v2 имеются маршрутизаторы, пропустите этот шаг.)

- Если в сети присутствует DHCP-сервер, убедитесь, что ваш компьютер использует динамический адрес IP. См. [Приложение В на стр. 303](#). По умолчанию в на P-791R v2 включен режим DHCP-сервера.
- 5 Сбросьте устройство к заводским настройкам и попробуйте обратиться к на P-791R v2, используя IP-адрес по умолчанию. См. [разд. 33.4 на стр. 293](#).
 - 6 Если проблему устранить не удалось, обратитесь к системному администратору или поставщику, либо прибегните к углубленной диагностике.

Углубленный способ диагностики

- Попробуйте обратиться к на P-791R v2 через другую сетевую службу, например, Telnet. Если вам удалось войти в на P-791R v2, проверьте настройки дистанционного управления устройством и фильтры SMT, чтобы установить причину, по которой веб-интерфейс на P-791R v2 оказался недоступен. См. [разд. 17.2 на стр. 169](#).



Экран Login доступен, но войти в управление на P-791R v2 не удается.

- 1 Убедитесь, что вы правильно вводите пароль. Пароль по умолчанию – **1234**. Пароль воспринимается с учетом регистра, поэтому при вводе индикатор клавиши [Caps Lock] не должен гореть.
- 2 Веб-конфигуратор нельзя использовать, если одновременно активен сеанс управления на P-791R v2 через SMT, Telnet или консольный порт. Завершите другой сеанс управления на P-791R v2 или попросите пользователя, работающего в этом сеансе, выйти из системы.
- 3 Выключите на P-791R v2 и включите его снова.
- 4 Если обратиться к устройству таким путем не получилось, может потребоваться возврат к заводским настройкам. См. [разд. 33.4 на стр. 293](#).



SMT недоступен, не удается войти в на P-791R v2 по Telnet.

См. указания по устранению неполадок под заголовком “[Не удается войти в веб-конфигуратор или обратиться к экрану Login.](#)”. Не обращайте внимание на указания, касающиеся браузера.



Не удается загрузить или принять по FTP файл настроек или обновить микропрограмму.

См. указания по устранению неполадок под заголовком “[Не удается войти в веб-конфигуратор или обратиться к экрану Login.](#)”. Не обращайте внимание на указания, касающиеся браузера.



Невозможно подключиться к на P-791R v2 через консольный порт.

Убедитесь, что вы используете консольный кабель из комплекта поставки, а переключатель **CON/AUX** на на P-791R v2 установлен в положение **CON**. См. Руководство по быстрому запуску.

33.3 Доступ к Интернету



Не удается выйти в Интернет.

- 1 Проверьте подключения оборудования и убедитесь, что показания светодиодов соответствуют норме. См. Руководство по быстрому запуску и [разд. 1.4 на стр. 35](#).
- 2 Убедитесь, что вы правильно ввели в мастере параметры учетной записи поставщика услуг Интернета. Пароль воспринимается с учетом регистра, поэтому индикатор клавиши [Caps Lock] не должен гореть.
- 3 Если проблему не удастся устранить, обратитесь к поставщику услуг Интернета.



Доступ в Интернет прекратился. Ранее Интернет был доступен через на P-791R v2, но сейчас соединение не функционирует.

- 1 Проверьте подключения оборудования и убедитесь, что показания светодиодов соответствуют норме. См. Руководство по быстрому запуску и [разд. 1.4 на стр. 35](#).
- 2 Выключите на P-791R v2 и включите устройство снова.
- 3 Если проблему не удастся устранить, обратитесь к поставщику услуг Интернета.



Низкая скорость или перебои в работе Интернет-соединения.

- 1 Сеть может быть перегружена трафиком. Проверьте светодиоды и обратитесь к [разд. 1.4 на стр. 35](#). Если устройство на P-791R v2 перегружено отправляемой или принимаемой информацией, закройте программы, использующие Интернет, в первую очередь – приложения для файлообменных сетей (P2P).
- 2 Выключите и снова включите на P-791R v2 и ваш компьютер.
- 3 Если проблему устранить не удалось, обратитесь к системному администратору или поставщику, либо прибегните к углубленной диагностике.



Не удается получить доступ к сайту.

Проверьте настройки фильтрации содержания и убедитесь, что вы не заблокировали себе доступ к каким-либо сайтам.



Не работает резервирование через коммутируемый доступ или переадресация трафика.

- 1 Если для резервирования через коммутируемый доступ вы используете порт **CON/AUX**, проверьте, установлен ли переключатель **CON/AUX** на на P-791R v2 в положение **AUX**. См. Руководство по быстрому запуску.
- 2 В конфигурации “точка – две точки” резервирование WAN недоступно.

33.4 Сброс на P-791R v2 к заводским настройкам

При сбросе настроек на P-791R v2 все изменения в настройках будут потеряны. на P-791R v2 восстановит настройки по умолчанию, а также исходный пароль: **1234**. Может потребоваться повторное выполнение всех настроек.



При нажатии кнопки **RESET** все изменения в настройках будут потеряны!

Чтобы сбросить настройки на P-791R v2:

- 1 Убедитесь, что светодиод **POWER** горит и не мигает.
- 2 Нажмите и держите нажатой кнопку **RESET** в течение 10 секунд. Отпустите кнопку **RESET**, когда светодиод **POWER** начнет мигать. Это означает, что настройки по умолчанию восстановлены.

Если устройство на P-791R v2 автоматически начало перезагружаться, дождитесь окончания перезагрузки на P-791R v2 и войдите в веб-конфигуратор с паролем “1234”.

Если автоматической перезагрузки на P-791R v2 не произошло, отключите и снова включите питание на P-791R v2. После этого выполните приведенные выше указания.

ЧАСТЬ VII

Приложения и предметный указатель

- Технические характеристики (297)
- Настройка IP-адреса компьютера (303)
- Разрешение всплывающих окон, сценариев JavaScript и апплетов Java (319)
- IP-адреса и деление на подсети (327)
- Конфликты в присвоении IP-адресов (337)
- Распространенные сетевые службы (341)
- Интерпретатор команд (345)
- Формат журналов (351)
- Команды фильтрации NetBIOS (363)
- Авторское право (365)
- Важная информация (367)
- Юридический адрес изготовителя (369)
- Гарантийное обслуживание ZyXEL (371)
- О компании ZyXEL (373)
- Указатель (375)

Технические характеристики

В следующих таблицах приведены сводные данные о характеристиках аппаратной части и микропрограмме P-791R v2.

Таблица 96 Технические характеристики

ТЕХНИЧЕСКАЯ ХАРАКТЕРИСТИКА	ОПИСАНИЕ
IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Пароль по умолчанию	пользователь: "user" администратор: "1234"
Пул адресов DHCP	192.168.1.33 – 192.168.1.64
Габариты (Ш x Г x В)	180 x 127 x 36 мм
Электропитание	При питании переменным током 9 В перем. тока, 1 А
Встроенный коммутатор	Четыре Ethernet-порта RJ-45 с автоматическим согласованием MDI/MDI-X 10/100 Мбит/с
Порт G.SHDSL	Интерфейсный разъем RJ-11 Скорость передачи данных: от 192 до 5700 Кбит/с Кодирование: фазоамплитудная модуляция с решетчатым кодированием (TC-PAM) Импеданс линии: 135 Вт Проводное подключение: одна пара (2 провода)
Условия эксплуатации	Температура: от 0° С до 40° С Влажность: 20% ~ 90% относительной влажности без конденсации
Условия хранения	Температура: от -20° С до 60° С Влажность: 20% ~ 90% относительной влажности
Расстояние между центрами отверстий на задней стороне корпуса	108 мм
Размер шурупов для настенного крепления	Винт М4, см. рис. 194 на стр. 301 .

Таблица 97 Микропрограмма

Поддержка режима маршрутизатора/моста	Поддерживается маршрутизация IP (RFC 791). TCP, UDP, ICMP, IGMP v1 и v2, ARP, RIP v1, RIP v2 Прозрачный режим моста (IEEE 802.1d) Поддержка PPP VCP (RFC 3185)
G.SHDSL	Фазоамплитудная модуляция с решетчатым кодированием (TC-PAM) Настройка в режиме клиента или сервера Автоматическое согласование / ручная подстройка скорости
Поддержка ATM	Многопротокольная передача поверх AAL5 (RFC1483) PPP поверх ATM (RFC 2364) PPP поверх Ethernet (RFC2516) Поддержка ATM AAL5 Поддержка восьми PVC ATM Forum UNI3.0/4.0 PVC OAM F4/F5 Loopback, RDI, AIS Режимы ограничения трафика: UBR, CBR и nrt-VBR
Совместный доступ в Интернет	NAT (включая режим "многие ко многим") / SUA, 2048 сеансов NAT Стандартный NAT с ограничением по номерам портов Серверный режим NAT (перенаправление портов) NAT для нескольких хостов Динамическая DNS (www.dyndns.org) DHCP-сервер/клиент/агент ретрансляции
Безопасность	Фильтрация пакетов Аутентификация пользователя (PAP, CHAP) при использовании PPP (RFC 1334, RFC 1994) Microsoft CHAP
Управление сетью	Веб-конфигуратор Интерфейс командной строки Поддержка доступа через Telnet по паролю Поддержка SNMP MIB I / MIB II Обновление микропрограммы и резервное копирование настроек по TFTP и FTP
Диагностические средства (для следующих подсистем)	Флэш-память Цепи и микросхемы SDSL ОЗУ Порт LAN
Прочее	Прокси-сервер для DNS Системный журнал (UNIX SYSLOG)

Таблица 98 Функциональные возможности микропрограммы

ФУНКЦИЯ	ОПИСАНИЕ
Замена управляющей микропрограммы	После выхода новой микропрограммы ее можно загрузить с сайта ZyXEL и передать в P-791R v2 с помощью веб-конфигуратора или клиента FTP/TFTP. Примечание. Используйте только микропрограмму, предназначенную для вашей модели устройства!
Резервное копирование и восстановление настроек	Создав резервную копию конфигурации P-791R v2, вы сможете в дальнейшем загрузить ее в P-791R v2, если потребуется вернуться к прежним настройкам.

Таблица 98 Функциональные возможности микропрограммы

ФУНКЦИЯ	ОПИСАНИЕ
Трансляция сетевых адресов (NAT)	Каждому компьютеру в сети должен быть присвоен собственный уникальный IP-адрес. NAT позволяет преобразовывать присвоенный вам внешний IP-адрес (диапазон адресов) в несколько частных IP-адресов, используемых компьютерами в вашей сети.
Фильтры пакетов	В P-791R v2 предусмотрены функции фильтрации пакетов для реализации механизмов безопасности и управления сетью.
Port Forwarding	Если в сети имеется сервер (например, почтовый или веб-сервер), с помощью этой функции можно обеспечить доступ к нему из Интернета.
DHCP (динамический протокол настройки хоста)	С помощью этой функции P-791R v2 может назначать компьютерам в сети IP-адреса, адрес шлюза по умолчанию и адреса DNS-серверов.
Поддержка динамической DNS	Динамическая служба DNS (система доменных имен) позволяет использовать фиксированный URL-адрес, например www.zyxel.com, с динамическим IP-адресом. Для получения такой услуги необходимо зарегистрироваться у провайдера динамической DNS.
IP Multicast	Многоадресная рассылка используется для доставки трафика определенной группе хостов. P-791R v2 поддерживает протокол IGMP (Internet Group Management Protocol - межсетевой протокол управления группами) версии 1 и 2 для присоединения к группам многоадресной рассылки (см. RFC 2236).
IP Alias	Совмещение IP-адресов (IP aliasing) позволяет разделить физическую сеть на различные логические сети через один и тот же интерфейс Ethernet. P-791R v2 в этом случае выступает в качестве шлюза для каждой подсети.
Время и дата	Текущее время и дату можно получать от внешнего сервера при включении P-791R v2. Кроме того, время можно установить вручную. Полученные дата и время в последующем используются в журналах.
Регистрация и отслеживание	Средства отслеживания пакетов и ведения журналов можно использовать для устранения неполадок. Журнальные сообщения с P-791R v2 можно передавать на внешний SYSLOG-сервер.
PPPoE	PPPoE имитирует модемное коммутируемое соединение с Интернетом.
Универсальная технология Plug and Play (UPnP)	Устройство с поддержкой UPnP может динамически присоединяться к сети, получать IP-адрес, сообщать свои возможности другим устройствам в сети.
Удаленное управление	Функция удаленного управления позволяет указать, с каких компьютеров в сети (WAN или LAN) и с использованием каких служб (например, HTTP, FTP) может осуществляться доступ к P-791R v2.

Таблица 99 Поддерживаемые стандарты

STANDARD	ОПИСАНИЕ
RFC 1483/2684 (MPOA)	Многопротокольная инкапсуляция поверх 5-го уровня адаптации ATM
RFC 2364 (PPPoA)	PPP через AAL5
RFC 2516 (PPPoE)	PPP по Ethernet (PPPoE)
ITU G.991.2 (G.SHDSL/G.SHDSL.bis)	Стандарт ITU для трансиверов для высокоскоростных абонентских цифровых каналов для одной проводной пары (SHDSL)

STANDARD	ОПИСАНИЕ
RFC 1112 (IGMP v1)	Протокол IGMP (Internet Group Management Protocol - межсетевой протокол управления группами) версия 1
RFC 2236 (IGMP v2)	Протокол IGMP (Internet Group Management Protocol - межсетевой протокол управления группами) версия 2
RFC 867	Протокол Daytime
RFC 868	Time Protocol
RFC 1305	Реализация спецификации протокола Network Time Protocol (версия 3)
RFC 1334 (PAP)	Протоколы аутентификации PPP
RFC 1994 (CHAP)	Протоколы аутентификации с предварительным согласованием вызова (CHAP) соединения PPP
RFC 1332 (IPCP)	Протокол управления протоколом IP (IPCP) соединения PPP.
RFC 1058 (RIP-1)	Информационный протокол маршрутизации
RFC 1723 (RIP-2)	Протокол маршрутизации RIP версия 2 – передача дополнительной информации
RFC 1631 (NAT)	Преобразователь IP- адресов сети (NAT)
RFC 1661 (PPP)	Протокол "точка – точка"
RFC 1157 (SNMPv1)	Упрощённый протокол управления сетью. (SNMP) версия 1
RFC 1441 (SNMPv2)	Упрощённый протокол управления сетью. (SNMP) версия 2

Инструкция по монтажу на стене

Для установки P-791R v2 на стене выполните следующие действия.



Уточните размер крепежных шурупов и расстояние между ними, обратившись к таб. 96 на стр. 297 .

- 1 Выберите место на прочной стене, которое не должно загораживаться.
- 2 Просверлите два отверстия под шурупы.

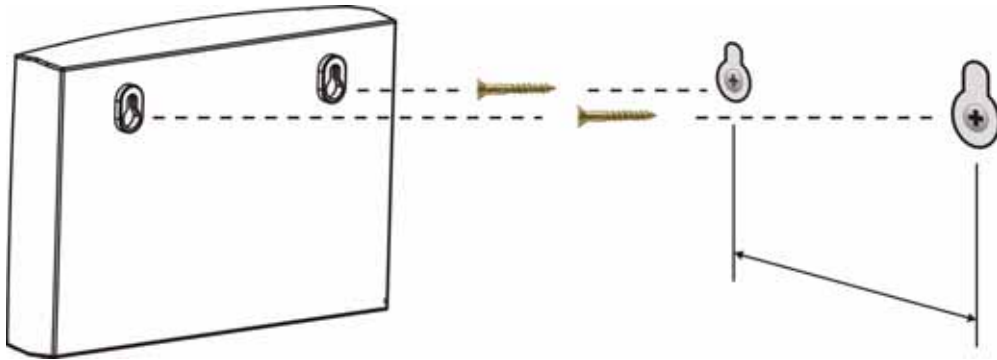


При сверлении отверстий будьте осторожны, чтобы не повредить трубы и кабели, которые могут быть проложены в стене.

- 3 Не завинчивайте шурупы в стену до конца. Оставьте небольшой зазор (примерно 0,5 см) между головками шурупов и стеной.
- 4 Убедитесь, что шурупы прочно закреплены в стене – они должны выдерживать массу P-791R v2 с соединительными кабелями.

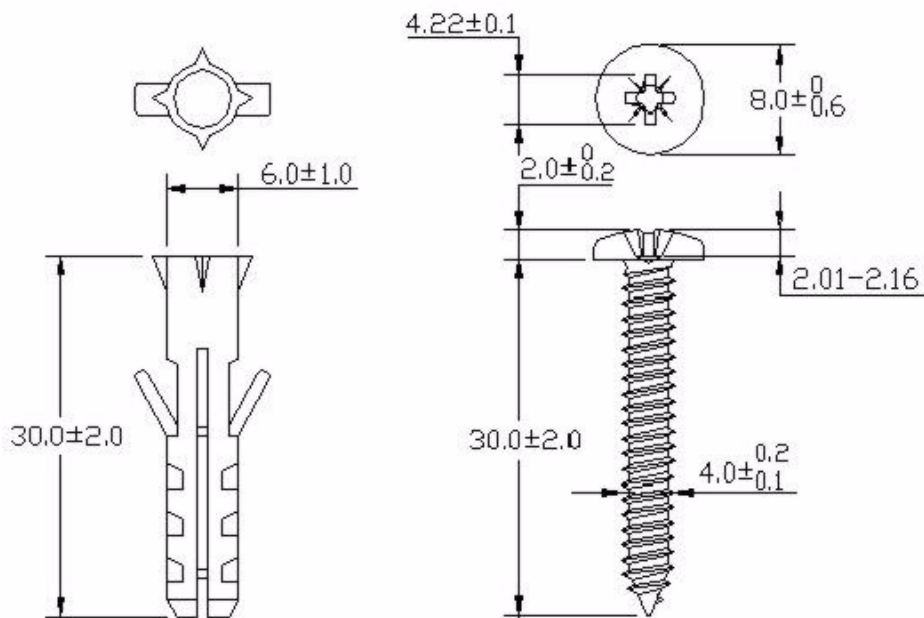
- 5** Совместите отверстия с задней стороны корпуса P-791R v2 с шурупами в стене. Повесьте P-791R v2 на шурупы.

Рис. 193 Пример монтажа на стене



Ниже приведены размеры винта М4 и пробки, используемых при монтаже на стене. Все размеры указаны в миллиметрах (мм).

Рис. 194 Пробка и винт М4



Настройка IP-адреса компьютера

Все компьютеры должны быть оборудованы адаптером Ethernet 10 или 100 Мбит/с, и на компьютерах должен быть установлен протокол TCP/IP.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 и более новые версии этих операционных систем, а также все версии UNIX/LINUX включают программные компоненты, необходимые для установки и использования протокола TCP/IP на компьютере. При работе с Windows 3.1 требуется приобретение пакета приложений TCP/IP сторонних производителей.

TCP/IP должен быть уже установлен на компьютерах под управлением Windows NT/2000/XP, Macintosh OS 7 и более поздних версий этих операционных систем.

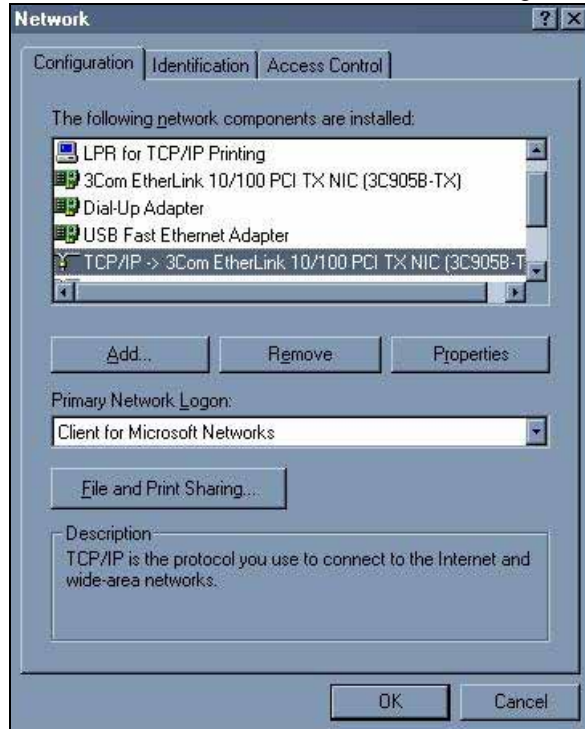
После установки необходимых компонентов TCP/IP настройте параметры TCP/IP для обмена данными через сеть.

Если вместо динамического назначения параметры IP присваиваются в ручном режиме, убедитесь в том, что компьютеры имеют IP-адреса, относящиеся к той же подсети, в которой находится LAN-порт P-791R v2.

Windows 95/98/Me

Нажмите кнопку **Start (Пуск)**, выберите **Settings (Настройки)**, **Control Panel (Панель управления)** и выберите двойным щелчком значок **Network (Сеть)** для открытия окна **Network (Сеть)**.

Рис. 195 Windows 95/98/Me: Сеть: Configuration



Установка компонентов

На вкладке **Configuration (Конфигурация)** окна **Network (Сеть)** отображается список установленных компонентов. Необходимы сетевой адаптер, протокол TCP/IP и клиент для сетей Microsoft.

Если необходим адаптер, выполните следующие действия.

- 1 В окне **Network (Сеть)** нажмите кнопку **Add (Добавить)**.
- 2 Выберите **Adapter (Адаптер)** и нажмите кнопку **Add (Добавить)**.
- 3 Выберите производителя и модель сетевого адаптера, затем нажмите кнопку **ОК**.

Если необходимо установить протокол TCP/IP, выполните следующие действия.

- 1 В окне **Network (Сеть)** нажмите кнопку **Add (Добавить)**.
- 2 Выберите **Protocol (Протокол)** и нажмите кнопку **Add (Добавить)**.
- 3 Выберите **Microsoft** в списке производителей.
- 4 Выберите **TCP/IP** в списке сетевых протоколов и нажмите кнопку **ОК**.

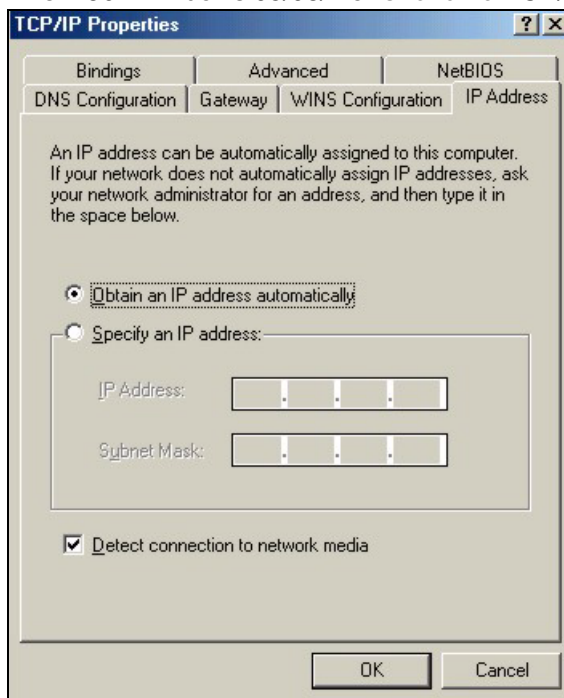
Если необходим клиент для сетей Microsoft, выполните следующие действия.

- 1 Нажмите кнопку **Add (Добавить)**.
- 2 Выберите **Client (Клиент)** и нажмите кнопку **Add (Добавить)**.
- 3 Выберите **Microsoft** в списке производителей.
- 4 Выберите **Client for Microsoft Networks (Клиент для сетей Microsoft)** в списке сетевых клиентов и нажмите кнопку **ОК**.
- 5 Перезапустите компьютер, чтобы изменения вступили в силу.

Настройка

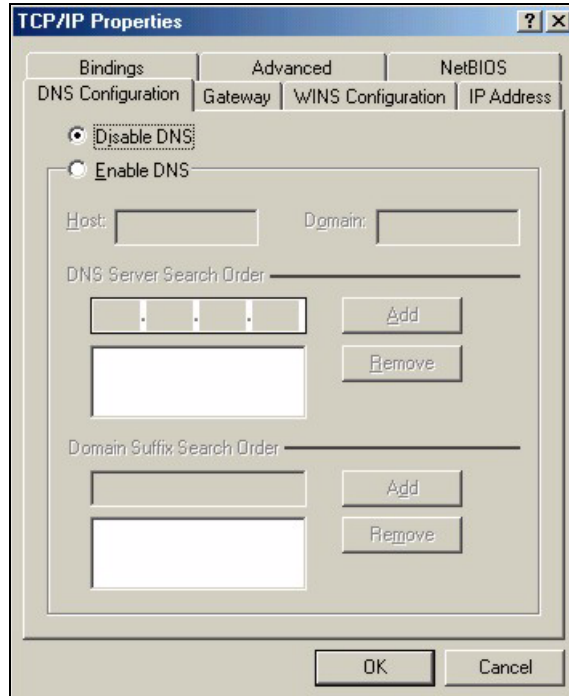
- 1 На вкладке **Configuration (Конфигурация)** окна **Network (Сеть)** выберите запись TCP/IP своего сетевого адаптера и нажмите кнопку **Properties (Свойства)**.
- 2 Выберите вкладку **IP Address (IP-адрес)**.
 - Если IP-адрес динамический, установите переключатель **Obtain an IP address automatically (Получить IP-адрес автоматически)**.
 - Если имеется статический IP-адрес, выберите переключатель **Specify an IP address (Указать IP-адрес)** и введите информацию в поля **IP Address (IP-адрес)** и **Subnet Mask (Маска подсети)**.

Рис. 196 Windows 95/98/Me: Свойства TCP/IP: IP-адрес



- 3 Выберите вкладку **DNS Configuration (Конфигурация DNS)**.
 - Если информация о DNS неизвестна, установите переключатель **Disable DNS (Отключить DNS)**.
 - Если информация о DNS известна, установите переключатель **Enable DNS (Включить DNS)** и введите информацию в полях внизу (необязательно заполнять их все).

Рис. 197 Windows 95/98/Me: Свойства TCP/IP: Конфигурация DNS



- 4 Выберите вкладку **Gateway (Шлюз)**.
 - Если IP-адрес шлюза неизвестен, удалите ранее установленные шлюзы.
 - Если IP-адрес шлюза известен, введите его в поле **New gateway (Новый шлюз)** и нажмите кнопку **Add (Добавить)**.
- 5 Нажмите кнопку **ОК** для сохранения изменений и закройте окно **TCP/IP Properties (Свойства TCP/IP)**.
- 6 Нажмите кнопку **ОК** для закрытия окна **Network (Сеть)**. При появлении запроса вставьте компакт-диск Windows.
- 7 Включите P-791R v2 и перезапустите компьютер, когда это будет предложено.

Проверка настроек

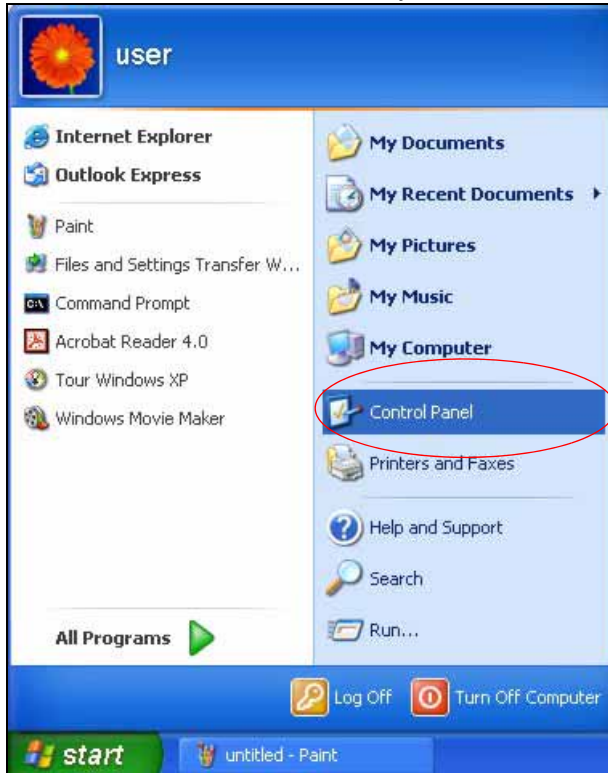
- 1 Нажмите кнопку **Start (Пуск)**, выберите **Run (Выполнить)**.
- 2 В окне **Run (Выполнить)** введите "winipcfg" и нажмите кнопку **ОК** для открытия окна **IP Configuration (Конфигурация IP)**.
- 3 Выберите свой сетевой адаптер. Вы должны увидеть IP-адрес, маску подсети и основной шлюз своего компьютера.

Windows 2000/NT/XP

В следующем примере рисунки приведены для Windows XP со стандартной темой интерфейса.

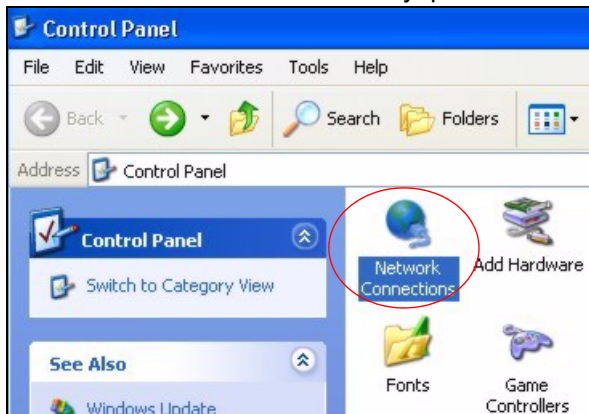
- 1 Нажмите кнопку **Пуск (Start** в англоязычных версиях Windows), **Настройка, Панель управления**.

Рис. 198 Windows XP: меню Пуск



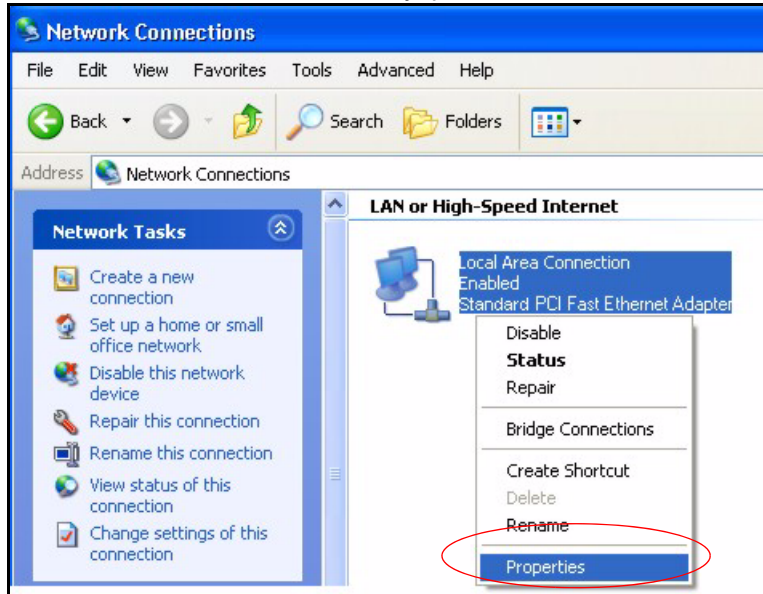
2 В Панели управления дважды щелкните на пункт **Сетевые подключения** (в Windows 2000/NT – **Сеть и коммутируемые подключения**).

Рис. 199 Windows XP: Панель управления



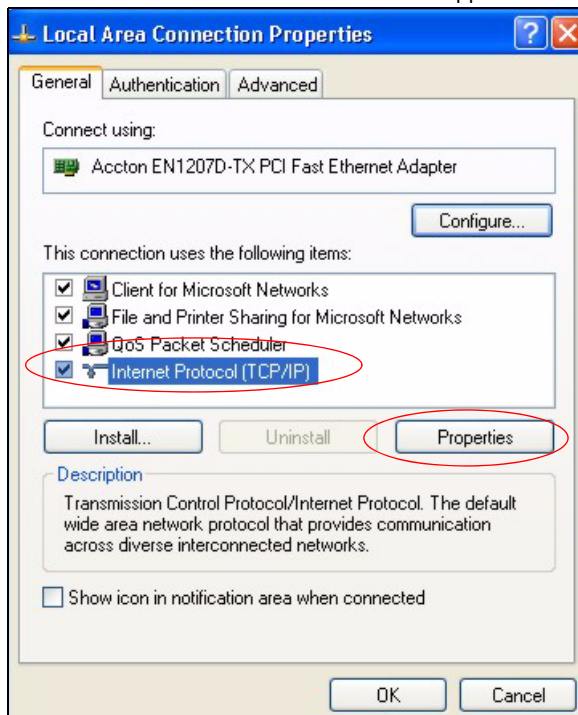
3 Щелкните правой кнопкой мыши **Local Area Connection (Подключение по локальной сети)**, затем выберите **Properties (Свойства)**.

Рис. 200 Windows XP: Панель управления: Сетевые подключения: Свойства



4 Выберите **Internet Protocol (TCP/IP) (Протокол Интернета (TCP/IP))** (на вкладке **General (Общие)** в Win XP) и щелкните **Properties (Свойства)**.

Рис. 201 Windows XP: Свойства подключения по локальной сети

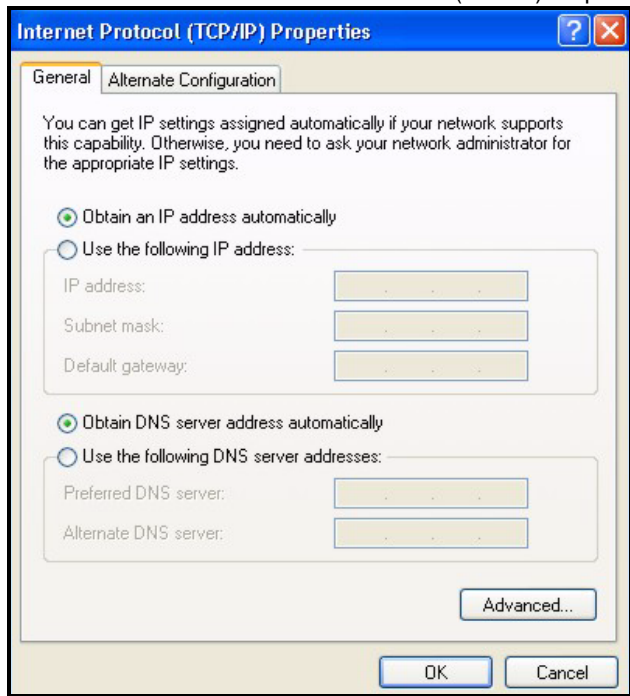


5 Откроется окно **Internet Protocol TCP/IP Properties (Свойства протокола Интернета (TCP/IP))** (вкладка **General (Общие)** в Windows XP).

- Если имеется динамический IP-адрес, установите переключатель **Obtain an IP address automatically (Получить IP-адрес автоматически)**.

- Если имеется статический IP-адрес, установите переключатель **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 кнопку **Advanced (Дополнительно)**.

Рис. 202 Windows XP: Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP))



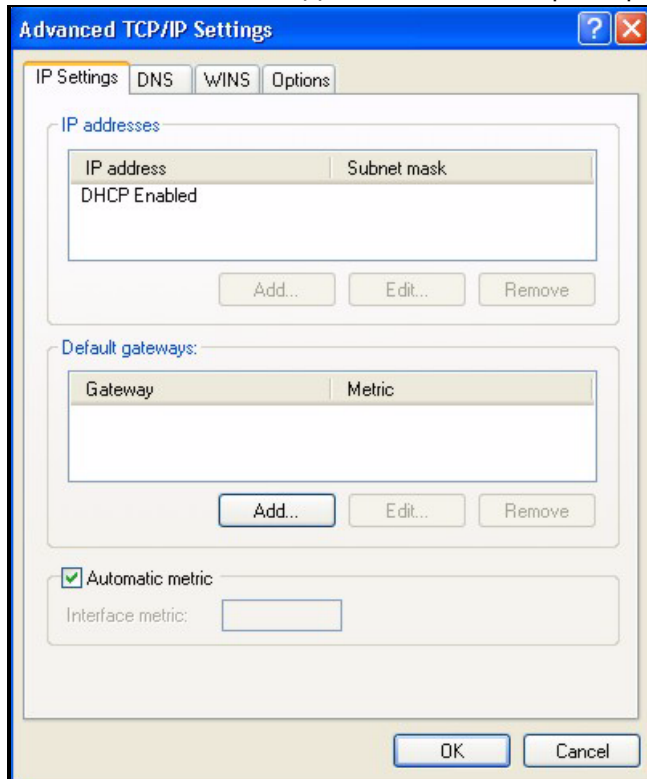
- 6** Если IP-адрес шлюза неизвестен, удалите все ранее установленные шлюзы на вкладке **Параметры IP** и нажмите кнопку **ОК**.

Если необходимо настроить дополнительные IP-адреса, выполните одно или несколько из следующих действий.

- На вкладке **IP Settings (Параметры IP)**, в разделе IP addresses (IP-адреса), нажмите кнопку **Add (Добавить)**.
- В окне **TCP/IP Address (Адрес TCP/IP)** введите IP-адрес в поле **IP address (IP-адрес)** и маску подсети в поле **Subnet mask (Маска подсети)**, затем нажмите кнопку **Add (Добавить)**.
- Выполните два вышеописанных действия для ввода каждого нового IP-адреса.
- Настройте дополнительные основные шлюзы по умолчанию на вкладке **IP Settings (Параметры IP)**, щелкнув кнопку **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)**. Чтобы вручную настроить метрику по умолчанию (количество прыжков при передаче), снимите флажок **Automatic metric (Автоматическое назначение метрики)** и введите метрику в поле **Metric (Метрика)**.
- Нажмите кнопку **Add (Добавить)**.
- Повторите три указанных выше действия для добавления каждого шлюза по умолчанию.

- Нажмите кнопку **ОК** по завершении.

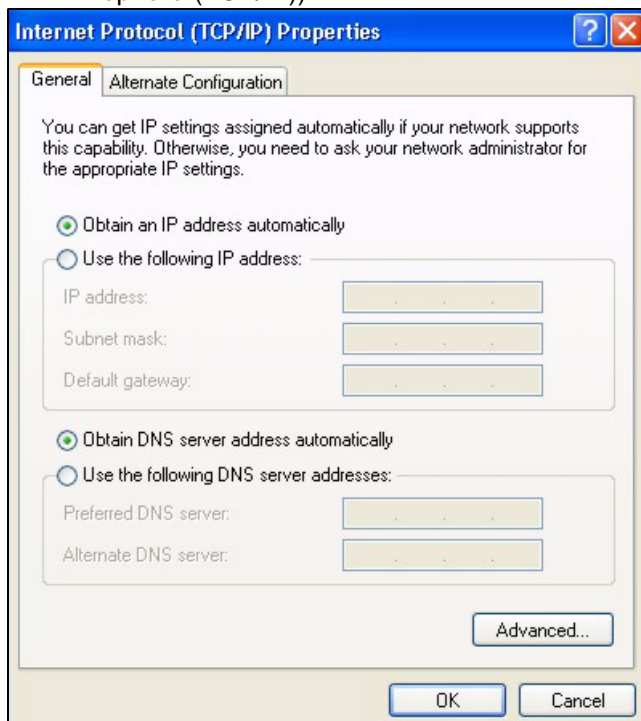
Рис. 203 Windows XP: Дополнительные параметры TCP/IP



7 В окне **Internet Protocol TCP/IP Properties (Свойства протокола Интернета (TCP/IP))** (вкладка **General (Общие)** в Windows XP) выполните следующее.

- Установите переключатель **Obtain DNS server address automatically (Получить адрес DNS-сервера автоматически)**, если адрес сервера неизвестен.
- Если IP-адрес DNS-сервера известен, установите переключатель **Use the following DNS server addresses (Использовать следующие адреса DNS-серверов)** и введите IP-адрес в полях **Preferred DNS server (Предпочитаемый DNS-сервер)** и **Alternate DNS server (Альтернативный DNS-сервер)**.
Если DNS-серверы были ранее настроены, нажмите кнопку **Advanced (Дополнительно)** и выберите вкладку **DNS** для их сортировки.

Рис. 204 Windows XP: Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP))



- 8 Нажмите кнопку **ОК** для закрытия окна **Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP))**.
- 9 Нажмите кнопку **Закреть** (в Windows 2000/NT – **ОК**), чтобы закрыть окно **Свойства подключения по локальной сети**.
- 10 Закройте окно **Сетевые подключения** (в Windows 2000/NT – **Сеть и коммутируемые подключения**).
- 11 Включите P-791R v2 и перезапустите компьютер (если это будет предложено).

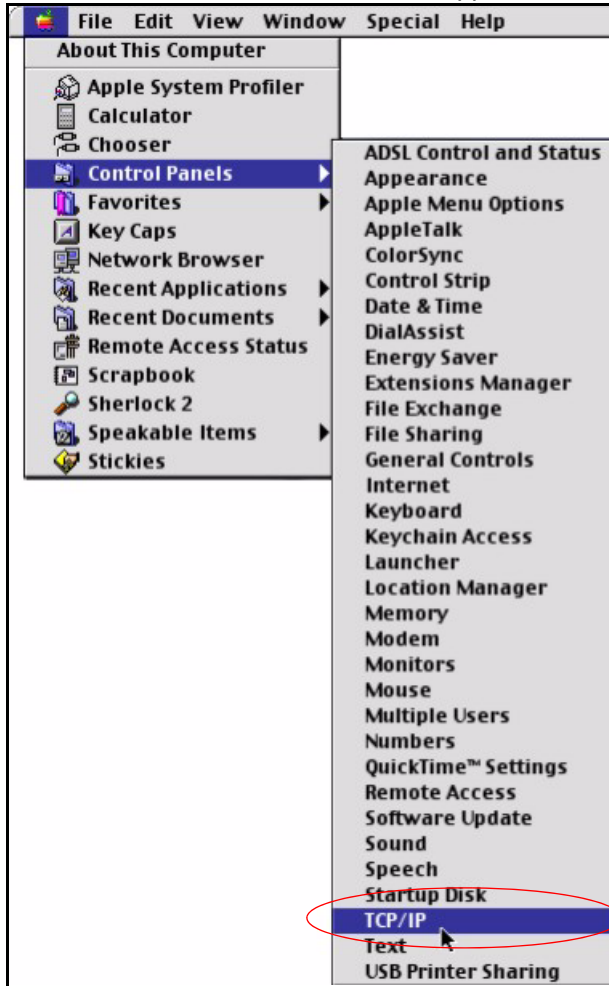
Проверка настроек

- 1 Нажмите кнопку **Start (Пуск)**, выберите **All Programs (Все программы), Accessories (Стандартные)**, затем **Command Prompt (Командная строка)**.
- 2 В окне **Command Prompt (Командная строка)** введите "ipconfig" и затем нажмите кнопку [ENTER] ([ВВОД]). Можно также открыть окно **Network Connections (Сетевые подключения)**, щелкнуть правой кнопкой мыши на сетевом подключении, выбрать пункт **Status (Состояние)**, затем – вкладку **Support (Поддержка)**.

Macintosh OS 8/9

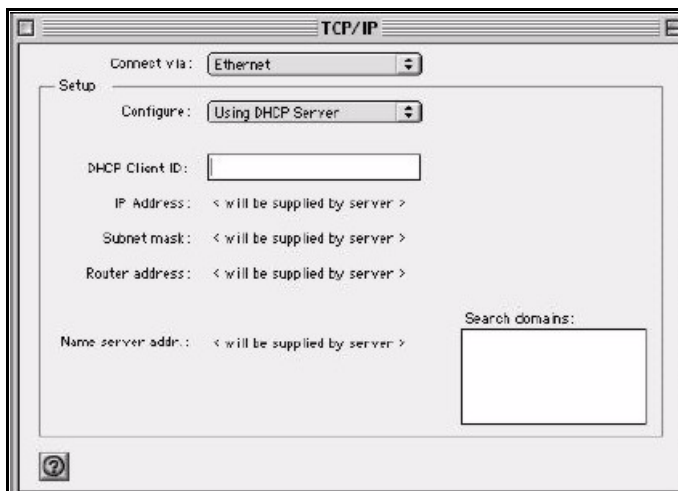
- 1 Щелкните меню **Apple, Control Panel (Панель управления)** и выберите двойным щелчком пункт **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.

Рис. 205 Macintosh OS 8/9: меню Apple



2 Выберите **Ethernet built-in (Встроенный Ethernet)** в списке **Connect via (Подключиться через)**.

Рис. 206 Macintosh OS 8/9: TCP/IP



3 Для динамически назначаемых параметров выберите пункт **Using DHCP Server (Использование сервера DHCP)** в списке **Configure: (Конфигурировать)**.

- 4 Если параметры назначаются статически, выполните следующие действия.
 - В списке **Configure (Конфигурировать)** выберите пункт **Manually (Вручную)**.
 - Введите свой IP-адрес в поле **IP Address (IP-адрес)**.
 - Введите маску подсети в поле **Subnet mask (Маска подсети)**.
 - Введите IP-адрес P-791R v2 в поле **Router address (Адрес маршрутизатора)**.
- 5 Закройте **TCP/IP Control Panel (Панель управления TCP/IP)**.
- 6 При появлении приглашения щелкните **Save (Сохранить)** для сохранения изменений конфигурации.
- 7 Включите P-791R v2 и перезапустите компьютер (если это будет предложено).

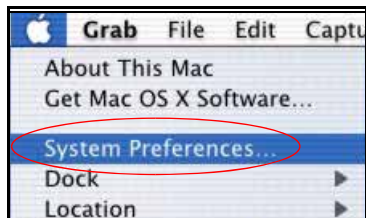
Проверка настроек

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

Macintosh OS X

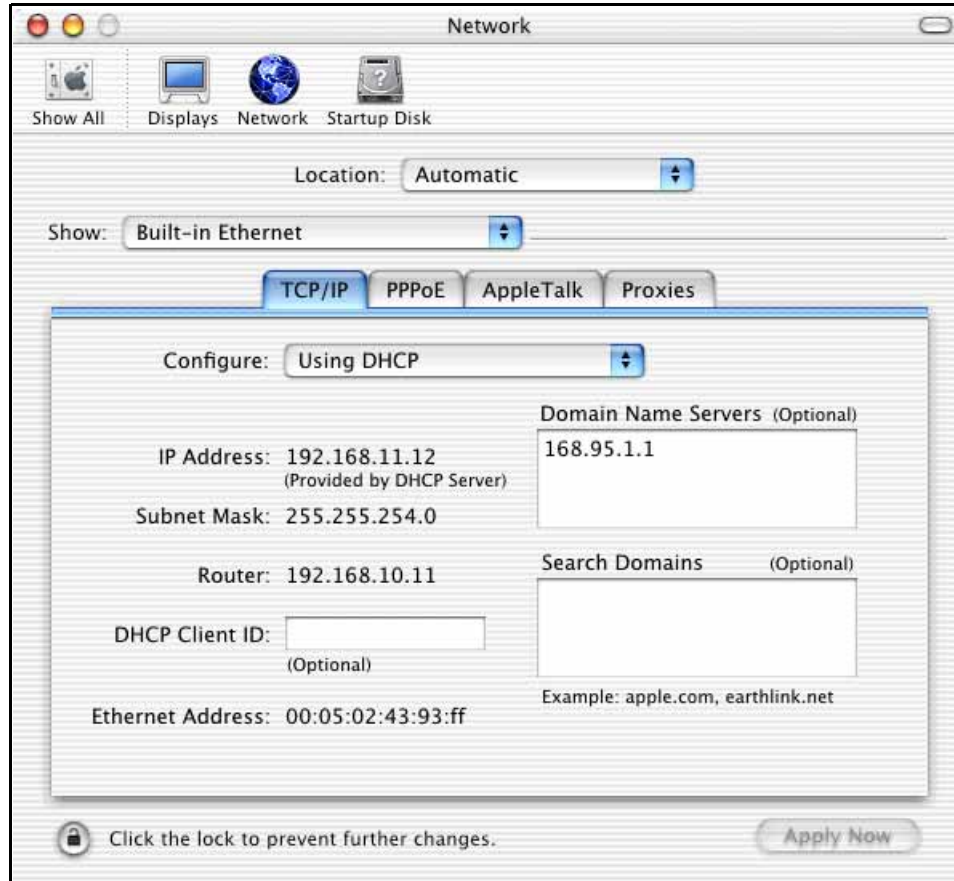
- 1 Щелкните меню **Apple**, пункт **System Preferences (Параметры системы)** для открытия окна **System Preferences (Параметры системы)**.

Рис. 207 Macintosh OS X: меню Apple



- 2 Щелкните **Network (Сеть)** на панели иконок.
 - Выберите значение **Automatic (Автоматический)** в списке **Location (Местоположение)**.
 - Выберите пункт **Built-in Ethernet (Встроенный Ethernet)** в списке **Show (Показать)**.
 - Выберите вкладку **TCP/IP**.
- 3 Если параметры назначаются динамически, выберите пункт **Using DHCP (Использование DHCP)** в списке **Configure**.

Рис. 208 Macintosh OS X: Сеть



- 4 Если параметры назначаются статически, выполните следующие действия.
 - В списке **Configure (Конфигурировать)** выберите пункт **Manually (Вручную)**.
 - Введите свой IP-адрес в поле **IP Address (IP-адрес)**.
 - Введите маску подсети в поле **Subnet mask (Маска подсети)**.
 - Введите IP-адрес P-791R v2 в поле **Router address (Адрес маршрутизатора)**.
- 5 Нажмите кнопку **Apply Now (Применить сейчас)** и закройте окно.
- 6 Включите P-791R v2 и перезапустите компьютер (если это будет предложено).

Проверка настроек

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

Linux

В этом разделе иллюстрируется настройка параметров TCP/IP в Red Hat Linux 9.0. В зависимости от используемого дистрибутива Linux и его версии методика, вид экранов и местоположение файлов могут различаться.



Убедитесь, что вы вошли в систему с правами администратора (root).

Настройка в среде K Desktop Environment (KDE)

Для настройки IP-адреса компьютера в среде KDE выполните следующие операции.

- 1 Нажмите кнопку Red Hat (в левом нижнем углу экрана), выберите **System Setting** (Системные настройки) и нажмите **Network** (Сеть).

Рис. 209 Red Hat 9.0: KDE: настройка сети: устройства



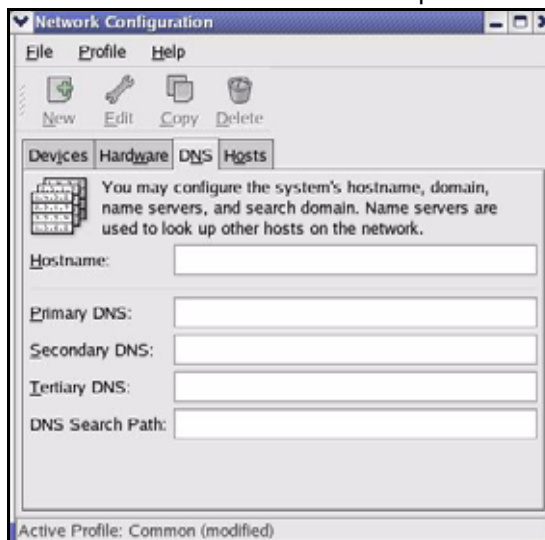
- 2 Дважды щелкните на профиле сетевой карты, который вы хотите настроить. Появится показанный ниже экран **Ethernet Device: General** (Устройство Ethernet: Общее).

Рис. 210 Red Hat 9.0: KDE: устройство Ethernet: общие настройки



- Если вам выдается динамический IP-адрес, установите флажок **Automatically obtain IP address settings with** (Автоматически получать параметры IP-адреса) и выберите **dhcp**.
 - Если вы используете статический IP-адрес, выберите **Statically set IP Addresses** (Статические IP-адреса) и заполните поля **Address** (Адрес), **Subnet mask** (Маска подсети) и **Default Gateway Address** (Шлюз по умолчанию).
- 3 Чтобы сохранить настройки и закрыть экран **Ethernet Device General**, нажмите кнопку **OK**.
 - 4 Если вам известны IP-адреса DNS-серверов, щелкните на вкладке **DNS** на экране **Network Configuration**. Введите в соответствующих полях параметры DNS-сервера.

Рис. 211 Red Hat 9.0: KDE: настройка сети: DNS



- 5 Перейдите на вкладку **Devices** (Устройства).

- 6 Чтобы изменения вступили в силу, нажмите кнопку **Activate** (Активировать). Появится изображенный ниже экран. Для сохранения изменений, выполненных на всех экранах, выберите **Yes** (Да).

Рис. 212 Red Hat 9.0: KDE: настройка сети: активация



- 7 После повторной инициализации сетевой карты убедитесь, что на экране **Network Configuration** (Настройка сети) в поле **Status** (Статус) **Active** (Активный).

Использование файлов настройки

Чтобы задать IP-адрес компьютера, отредактировав файлы настройки сети, выполните следующие операции.

- 1 Если в вашем компьютере установлена только одна сетевая карта, найдите файл `ifconfig-eth0` (где `eth0` – обозначение Ethernet-карты). Откройте файл настроек в любом редакторе текстовых файлов.
 - Если IP-адрес назначается вам динамически, в поле `BOOTPROTO=` введите **dhcp**. Пример приведен на следующем рисунке.

Рис. 213 Red Hat 9.0: задание динамического IP-адреса в файле `ifconfig-eth0`

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

- Если вы используете статический IP-адрес, в поле `BOOTPROTO=` введите **static**. Наберите `IPADDR=` и укажите ваш IP адрес (в десятичном виде через точку), затем наберите `NETMASK=` и укажите маску подсети. Ниже приведен пример для статического IP-адреса 192.168.1.10 и маски подсети 255.255.255.0.

Рис. 214 Red Hat 9.0: задание статического IP-адреса в файле `ifconfig-eth0`

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

- 2 Если вам известны IP-адреса DNS-серверов, укажите параметры DNS в файле `resolv.conf`, находящемся в каталоге `/etc`. В следующем примере настраиваются IP-адреса двух DNS-серверов.

Рис. 215 Red Hat 9.0: настройка DNS в файле `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 После редактирования и сохранения файлов настройки необходимо переинициализировать сетевую плату. Перейдите в каталог `/etc/rc.d/init.d` и введите `./network restart`. Пример приведен на следующем рисунке.

Рис. 216 Red Hat 9.0: повторная инициализация сетевой платы

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

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

Проверка настроек

Чтобы проверить настройки TCP/IP, на экране терминала введите `ifconfig`.

Рис. 217 Red Hat 9.0: проверка параметров 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]#
```

Разрешение всплывающих окон, сценариев JavaScript и апплетов Java

Чтобы пользоваться веб-конфигуратором, нужно разрешить веб-браузеру следующее.

- На компьютере в веб-браузере нужно разрешить всплывающие окна.
- Сценарии JavaScript (их выполнение разрешено по умолчанию).
- Разрешения на выполнение Java-кода (включены по умолчанию).



Здесь рассмотрены экраны Internet Explorer 6. Экраны в других версиях Internet Explorer могут отличаться.

Блокирование всплывающих окон в Internet Explorer

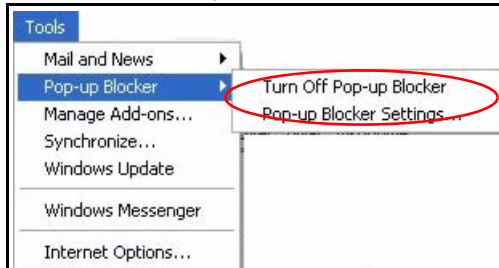
Для входа в устройство может потребоваться отключить блокирование всплывающих окон.

Для этого следует либо полностью отключить блокирование (которое по умолчанию включено Windows XP с пакетом исправлений Service Pack 2), либо включить блокирование, создав исключение для IP-адреса вашего устройства.

Отключение блокирования всплывающих окон

- 1 В Internet Explorer выберите **Tools** (Сервис), **Pop-up Blocker** (Блокирование всплывающих окон) и выберите **Turn Off Pop-up Blocker** (Отключить блокирование всплывающих окон).

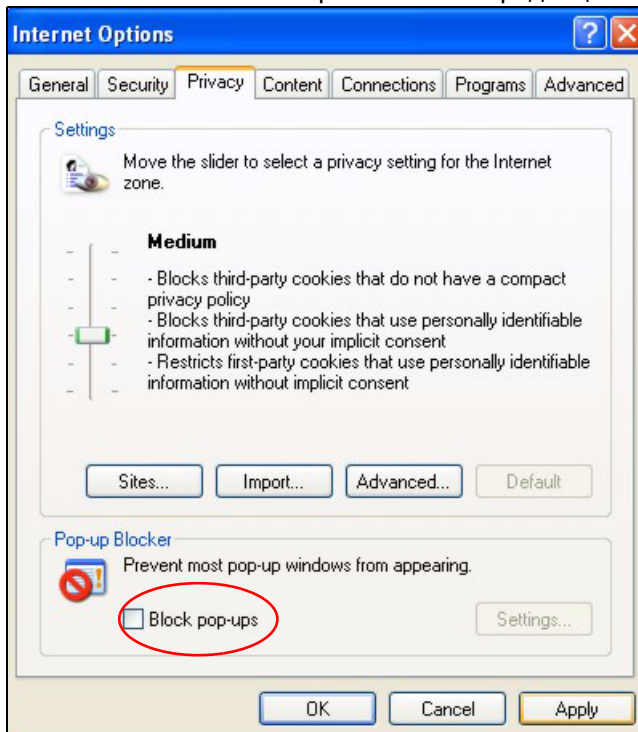
Рис. 218 Блокирование всплывающих окон



Проверить, включено ли блокирование всплывающих окон, можно в разделе **Pop-up Blocker** (Блокирование всплывающих окон) на закладке **Privacy** (Конфиденциальность).

- 1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя), **Privacy** (Конфиденциальность).
- 2 Снимите флажок **Block pop-ups** (Блокировать всплывающие окна) в разделе **Pop-up Blocker** (Блокирование всплывающих окон). При этом отключаются все средства блокирования всплывающих окон, которые могли быть активированы.

Рис. 219 Свойства обозревателя: Конфиденциальность



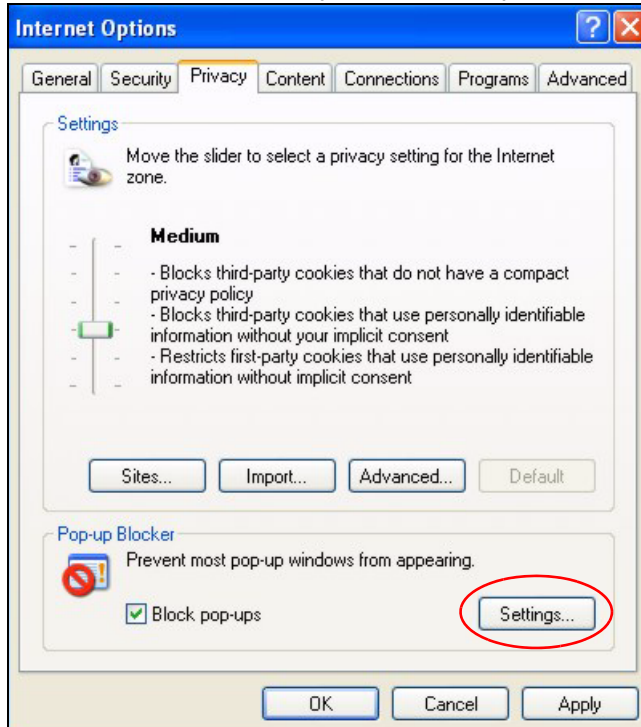
- 3 Чтобы сохранить настройки, нажмите кнопку **Apply**.

Разрешение всплывающих окон в исключительном порядке

Вместо полного снятия блокирования можно разрешить всплывающие окна только от вашего устройства. Для этого выполните описанные ниже операции.

- 1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Privacy** (Конфиденциальность).
- 2 Выберите **Settings** (Параметры), чтобы открыть экран **Pop-up Blocker Settings** (Параметры блокирования всплывающих окон).

Рис. 220 Свойства обозревателя: Конфиденциальность



- 3 Введите IP-адрес вашего устройства (web-страница, которую Вы не хотите блокировать) с префиксом ghttp: //h. Пример: http://192.168.167.1.
- 4 Нажмите **Add** (Добавить), чтобы внести IP-адрес в список **Allowed sites** (Разрешенные узлы).

Рис. 221 Параметры блокирования всплывающих окон



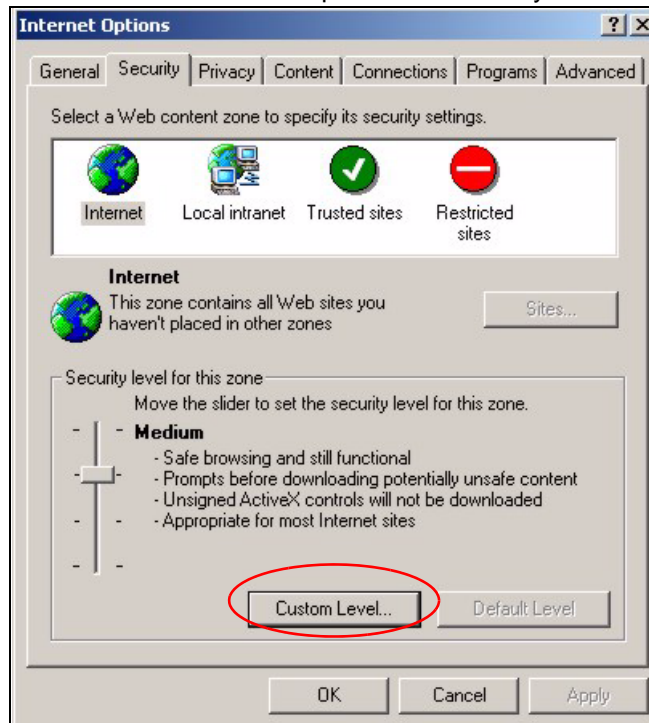
- 5 Нажмите **Close** (Закреть), чтобы вернуться на экран **Privacy** (Конфиденциальность).
- 6 Чтобы сохранить настройки, нажмите кнопку **Apply**.

Сценарии JavaScript

Если страницы веб-конфигуратора в Internet Explorer отображаются неправильно, проверьте, разрешено ли выполнение сценариев JavaScript.

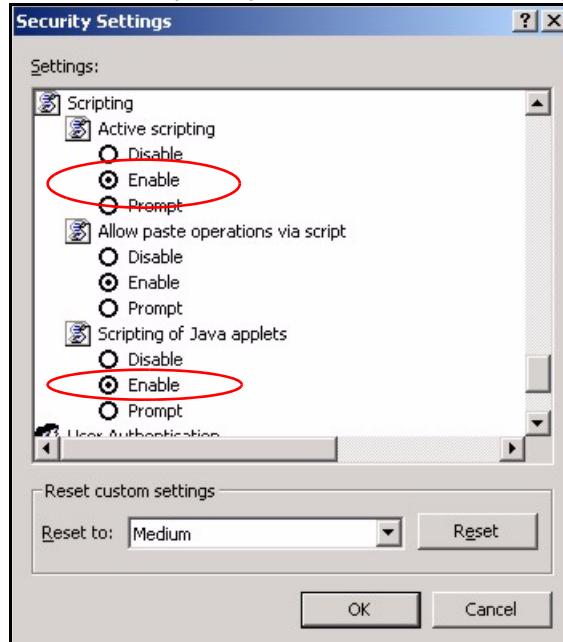
- 1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Security** (Безопасность).

Рис. 222 Свойства обозревателя: Security



- 2 Нажмите кнопку **Custom Level...** (Другой).
- 3 Пролистайте список до раздела **Scripting** (Сценарии).
- 4 В подразделе **Active scripting** (Активные сценарии) проверьте, выбран ли переключатель **Enable** (Разрешить; этот вариант выбран по умолчанию).
- 5 В подразделе **Scripting of Java applets** (Выполнять сценарии приложений Java) проверьте, выбран ли переключатель **Enable** (Разрешить; этот вариант выбран по умолчанию).
- 6 Нажмите кнопку **OK**, чтобы закрыть окно.

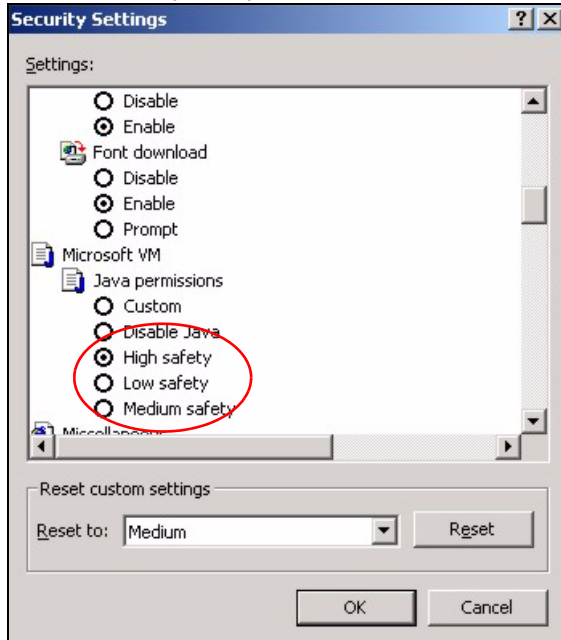
Рис. 223 Параметры безопасности – сценарии JavaScript



Разрешения на выполнение Java-апплетов

- 1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Security** (Безопасность).
- 2 Нажмите кнопку **Custom Level...** (Другой).
- 3 Пролистайте список до раздела **Microsoft VM** (Виртуальная машина Microsoft).
- 4 В подразделе **Java permissions** (Разрешения Java) проверьте, выбран ли уровень безопасности.
- 5 Нажмите кнопку **ОК**, чтобы закрыть окно.

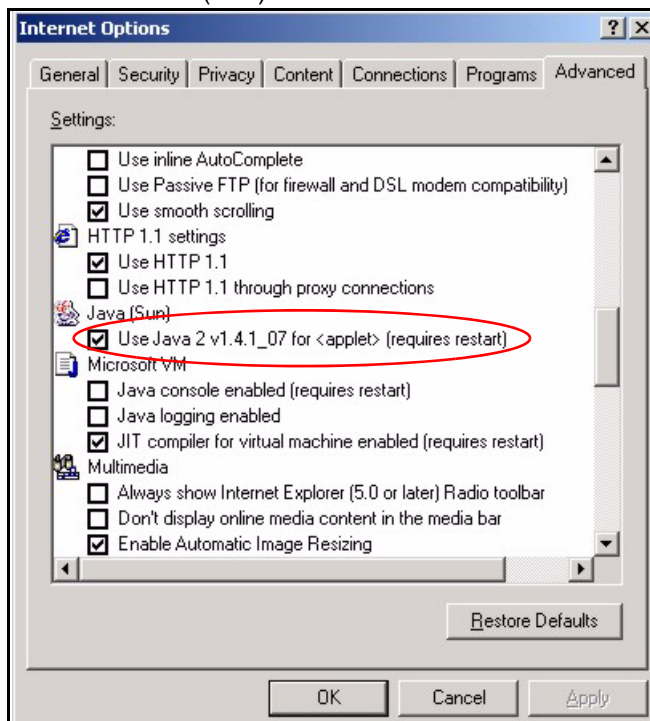
Рис. 224 Параметры безопасности – Java-апплеты



JAVA (Sun)

- 1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Advanced** (Дополнительно).
- 2 Убедитесь, что в подразделе **Java (Sun)** выбран пункт **Use Java 2 for <applet>**.
- 3 Нажмите кнопку **ОК**, чтобы закрыть окно.

Рис. 225 Java (Sun)



IP-адреса и деление на подсети

В этом приложении рассмотрены IP-адреса и маски подсетей.

IP-адреса идентифицируют отдельные устройства в сети. Каждое сетевое устройство (включая компьютеры, серверы, маршрутизаторы, принтеры и т.п.), осуществляющее самостоятельный обмен данными с сетью, должно иметь IP-адрес. Такие сетевые устройства называются хостами.

Маски подсетей определяют максимально возможное число хостов в сети. Маски подсетей можно также использовать для деления одной сети на несколько подсетей.

Общие сведения об IP-адресах

IP-адрес состоит из двух частей: маски подсети и идентификатора хоста. Подобно домам на улице, для которых общим является название улицы, хосты в сети связаны общим номером сети. Уникальным номером, аналогичным номеру дома, в этом случае является идентификатор хоста. Маршрутизаторы ориентируются по номеру подсети для отправки пакетов в соответствующую сеть. Конкретный хост затем находится по идентификатору хоста.

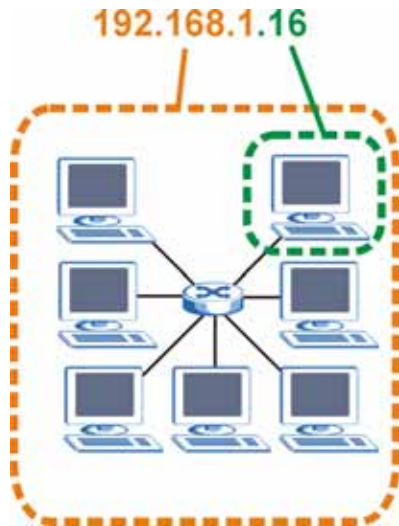
Структура

IP-адрес состоит из четырёх частей, которые записываются в десятичной форме через точку, например, 192.168.1.1. Отдельные части называются октетами. Октет – это восьмиразрядное двоичное число (например, 11000000, что в десятичном виде равно 192).

Таким образом каждый октет имеет возможный диапазон значений от 00000000 до 11111111 в двоичном счислении или от 0 до 255 в десятичном счислении.)

На следующем рисунке приведен пример IP-адреса, в котором первые три октета (192.168.1) представляют собой номер сети, а четвертый октет (16) – идентификатор хоста.

Рис. 226 Номер сети и идентификатор хоста



Число разрядов IP-адреса, занимаемое номером подсети или идентификатором хоста, зависит от маски подсети.

Маски подсетей

Маска подсети определяет, какие биты образуют номер сети и какие биты соответствуют идентификатору хоста (с помощью логического "И"). Термин "подсеть" обозначает часть более крупного адресного пространства.

Маска подсети состоит из 32 двоичных разрядов. Если один из разрядов содержит единицу, соответствующий бит в IP-адресе является частью номера сети. Если один из разрядов содержит ноль, соответствующий бит в IP-адресе является частью идентификатора хоста.

В следующем примере приведена маска подсети, в которой отмечены номер сети (жирным шрифтом) и идентификатор хоста в составе IP-адреса (192.168.1.2 в десятичном виде).

Таблица 100 Пример номера сети и идентификатора хоста в IP-адресе

	1-ЫЙ ОКТЕТ: (192)	2-ОЙ ОКТЕТ: (168)	3-ИЙ ОКТЕТ: (1)	4-ЫЙ ОКТЕТ: (2)
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Маска подсети (двоичная)	11111111	11111111	11111111	00000000
Номер сети	11000000	10101000	00000001	
Идентификатор хоста				00000010

Маски подсетей принято задавать в виде непрерывной последовательности единиц, начинающейся со старшего бита, за которой следует непрерывная последовательность нулей; обе последовательности в сумме составляют 32 бита.

Маски подсетей часто обозначаются числом разрядов, отводимых под номер сети (т.е. количеством битов, равных единице). Например, термин “8-битная маска” означает, что первые 8 битов маски заполнены единицами, а оставшиеся 24 бита – нулями.

Маски подсетей записываются в десятичном виде через точку, как и IP-адреса. В следующем примере показаны двоичные и десятичные представления для 8-, 16-, 24- и 29-битных масок подсетей.

Таблица 101 Маски подсетей

	ДВОИЧНАЯ				ДЕСЯТИЧНАЯ
	1-ЫЙ ОКТЕТ	2-ОЙ ОКТЕТ	3-ИЙ ОКТЕТ	4-ЫЙ ОКТЕТ	
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Разрядность номера сети определяет максимальное число хостов, которое может содержаться в сети. Чем больше битов содержит номер, тем меньше битов доступно для использования в качестве идентификаторов хостов.

IP-адрес, в котором идентификатор хоста состоит целиком из нулей, является IP-адресом сети (пример – 192.168.1.0 с 24-битной маской). IP-адрес, в котором идентификатор хоста состоит целиком из единиц, является широковещательным адресом (пример – 192.168.1.255 с 24-битной маской).

Поскольку эти два IP-адреса не могут использоваться конкретными хостами, вычислить максимальное возможное число хостов в сети можно следующим образом:

Таблица 102 Максимально возможное число хостов

МАСКА ПОДСЕТИ		РАЗМЕР ИДЕНТИФИКАТОРА ХОСТА		МАКСИМАЛЬНОЕ ЧИСЛО ХОСТОВ
8 битов	255.0.0.0	24 битов	$2^{24} - 2$	16777214
16 битов	255.255.0.0	16 битов	$2^{16} - 2$	65534
24 битов	255.255.255.0	8 битов	$2^8 - 2$	254
29 битов	255.255.255.248	3 битов	$2^3 - 2$	6

Способ записи

Поскольку маска всегда состоит из непрерывной последовательности единиц и непрерывной последовательности нулей, достаточно указывать только число единиц, не записывая значение каждого октета. Для этого обычно после адреса указывается знак “/”, за которым следует число единиц в маске подсети.

Например, обозначение 192.1.1.0 /25 соответствует номеру 192.1.1.0 с маской подсети 255.255.255.128.

В следующей таблице представлены некоторые допустимые маски подсетей, записанные обоими способами.

Таблица 103 Альтернативный способ записи маски подсети

МАСКА ПОД-СЕТИ	АЛЬТЕРНАТИВ-НЫЙ СПОСОБ ЗАПИСИ	ПОСЛЕДНИЙ ОКТЕТ (ДВО-ИЧНЫЙ)	ПОСЛЕДНИЙ ОКТЕТ (ДЕСЯ-ТИЧНЫЙ)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

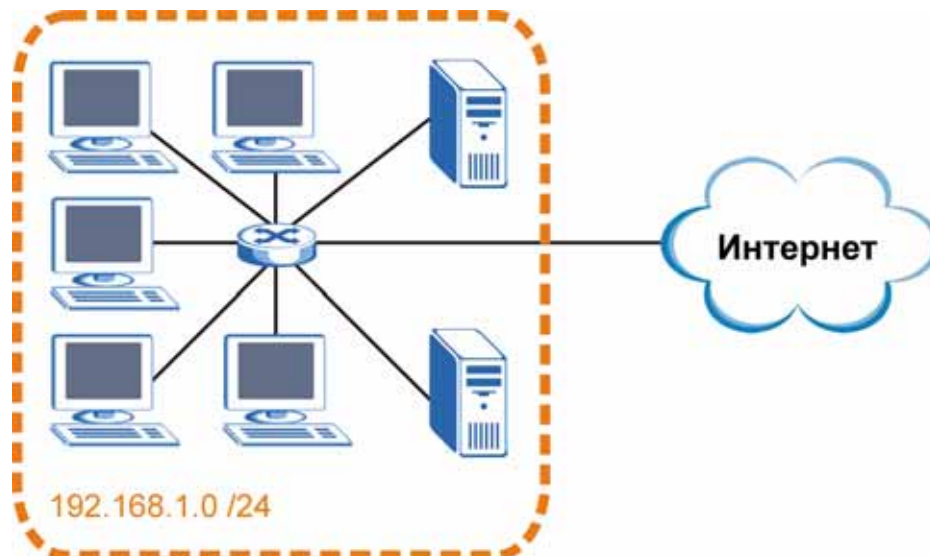
Деление на подсети

Подсети можно использовать для деления одной сети на несколько меньших сегментов. В следующем примере системный администратор создает две подсети, чтобы изолировать группу серверов от остальной части сети по соображениям безопасности.

В этом примере сеть компании имеет адрес 192.168.1.0. Первые три цифры адреса (192.168.1) относятся к номеру подсети, а оставшийся октет содержит идентификатор хоста, обеспечивая до $2^8 - 2 = 254$ возможных хостов.

Структура сети компании до деления на подсети приведена на следующем рисунке.

Рис. 227 Пример деления на подсети: до деления

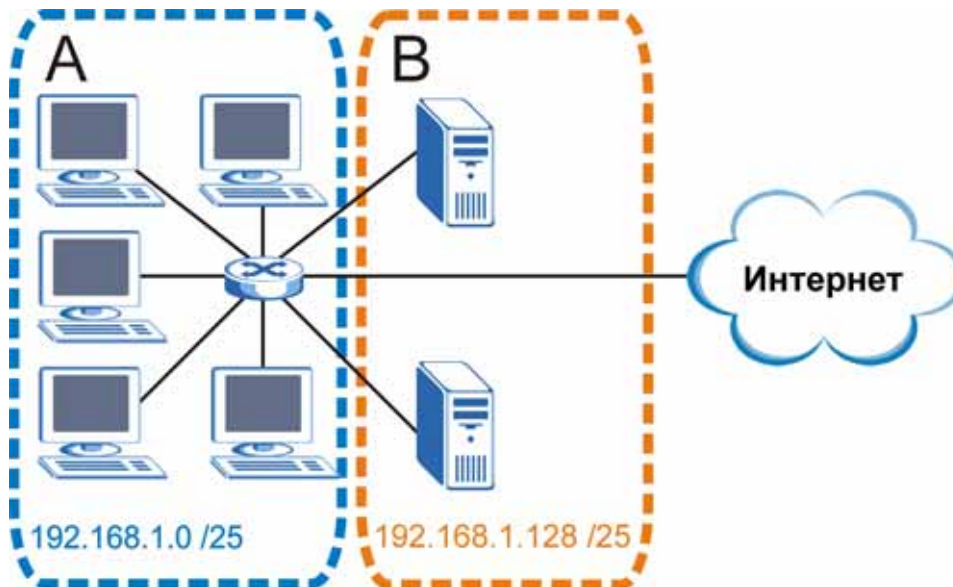


Для деления сети 192.168.1.0 на две логические подсети можно “позаимствовать” один из битов идентификатора хоста. Маска подсети теперь состоит из 25 битов (255.255.255.128 или /25).

“Позаимствованный” бит идентификатора хоста может принимать значения 0 и 1, давая в итоге две подсети: 192.168.1.0 /25 и 192.168.1.128 /25.

Структура сети компании после деления на подсети приведена на следующем рисунке. Теперь имеются две подсети: **A** и **B**.

Рис. 228 Пример деления на подсети: после деления



В 25-битовой подсети идентификатор хоста имеет длину 7 битов, таким образом, каждая подсеть может содержать до $2^7 - 2 = 126$ хостов (идентификатор хоста, целиком состоящий из нулей, используется как адрес подсети, а идентификатор, целиком состоящий из единиц, обозначает широковещательный адрес).

192.168.1.0 с маской 255.255.255.128 - это адрес самой подсети **A**, а 192.168.1.127 с маской 255.255.255.128 - это целевой адрес широковещательной рассылки для данной подсети. Таким образом, непосредственным хостам в подсети **A** могут назначаться адреса от 192.168.1.1 до 192.168.1.126 включительно.

Аналогично, для подсети **B** диапазон адресов хостов – от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В рассмотренном выше примере применялась 25-разрядная маска подсети для деления 24-битного адреса пространства на две подсети. Аналогичным образом 24-битный адрес можно поделить и на четыре подсети; для этого необходимо “позаимствовать” из номера хоста два бита, которые вместе имеют следующие возможные значения: 00, 01, 10 и 11. Маска подсети состоит из 26 битов: 11111111.11111111.11111111.11000000 или 255.255.255.192.

Каждой подсети выделяется по 6 битов под идентификатор хоста, в общей сложности каждая подсеть может иметь до 2^6-2 или 62 хостов (идентификаторы хостов, целиком состоящие из нулей, идентифицируют саму подсеть, а идентификатор, целиком состоящий из единиц, используется для широковещательной рассылки в подсети).

Таблица 104 Подсеть 1

IP-АДРЕС/МАСКА ПОД-СЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес (десятичный)	192.168.1.	0
IP-адрес (двоичный)	11000000.10101000.00000001.	00000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.0	Адрес первого хоста: 192.168.1.1	
Широковещательный адрес: 192.168.1.63	Адрес последнего хоста: 192.168.1.62	

Таблица 105 Подсеть 2

IP-АДРЕС/МАСКА ПОД-СЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP Address	192.168.1.	64
IP-адрес (двоичный)	11000000.10101000.00000001.	01000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.64	Адрес первого хоста: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Адрес последнего хоста: 192.168.1.126	

Таблица 106 Подсеть 3

IP-АДРЕС/МАСКА ПОД-СЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP Address	192.168.1.	128
IP-адрес (двоичный)	11000000.10101000.00000001.	10000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.128	Адрес первого хоста: 192.168.1.129	
Широковещательный адрес: 192.168.1.191	Адрес последнего хоста: 192.168.1.190	

Таблица 107 Подсеть 4

IP-АДРЕС/МАСКА ПОД-СЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP Address	192.168.1.	192
IP-адрес (двоичный)	11000000.10101000.00000001.	11000000
Маска подсети (двоичная)	11111111.11111111.11111111.	11000000

Таблица 107 Подсеть 4 (продолжение)

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
Адрес подсети: 192.168.1.192	Адрес первого хоста: 192.168.1.193	
Широковещательный адрес: 192.168.1.255	Адрес последнего хоста: 192.168.1.254	

Пример: восемь подсетей

Аналогичным образом можно создать восемь подсетей, используя 27-разрядную маску (000, 001, 010, 011, 100, 101, 110 и 111).

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

Таблица 108 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

Планирование структуры подсетей

В следующей таблице перечислены варианты деления на подсети для сети с 24-битным номером.

Таблица 109 Планирование подсетей в сети с 24-битным номером

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

В следующей таблице перечислены варианты деления на подсети для сети с 16-битным номером.

Таблица 110 Планирование подсетей в сети с 16-битным номером

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

Настройка IP-адресов

В зависимости от конкретной ситуации этот номер присваивается различными службами. Если поставщик услуг Интернета или администратор вашей сети присвоил вам блок зарегистрированных IP-адресов, необходимо следовать его указаниям по выбору IP-адресов и маски подсети.

Если поставщик услуг Интернета не сообщил вам номер IP-подсети в явном виде, то наиболее вероятно, что вы используете единственную учетную запись пользователя, и поставщик услуг Интернета назначит вам динамический IP-адрес при установлении соединения. В этом случае рекомендуется выбрать номер сети из диапазона от 192.168.0.0 до 192.168.255.0. Комитет по цифровым адресам в Интернете (Internet Assigned Number Authority, IANA) зарезервировал определённые диапазоны адресов специально для частных применений; все адреса, которые не принадлежат этим диапазонам, не должны использоваться без специальных на то указаний. Также необходимо включить на P-791R v2 трансляцию сетевых адресов (NAT).

После выбора номера сети выберите для P-791R v2 легко запоминающийся IP-адрес, например, 192.168.1.1, но убедитесь, что этот адрес не используется никаким другим устройством в вашей сети.

Маска подсети указывает на долю номеров IP-адресов в сети. P-791R v2 автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. В отсутствие специальных указаний изменять маску подсети, предлагаемую P-791R v2, не следует.

Частные IP-адреса

Каждому компьютеру в Интернете должен соответствовать уникальный адрес. В сетях, которые отделены от Интернета - например, в сети между двумя филиалами, можно назначать хостам любые IP-адреса, не испытывая каких-либо затруднений. Тем не менее, Комитет по цифровым адресам в Интернете (IANA) специально для частных сетей зарезервировал следующие три блока IP-адресов:

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

IP-адрес может быть выдан IANA или поставщиком услуг Интернета, либо присвоен в рамках частной сети. Для небольших организаций, получающих доступ в Интернет от поставщика услуг Интернета, Интернет-адреса для локальных сетей могут выдаваться непосредственно поставщиком услуг. В то же время подразделениям более крупных организаций следует согласовывать назначение IP-адресов с сетевым администратором.

Независимо от конкретных обстоятельств выбирать произвольные IP-адреса ни в коем случае не следует; всегда необходимо придерживаться приведённых выше указаний. Более подробно присвоение адресов описано в документах RFC 1597 (*выделение адресов для частных интрасетей*) и RFC 1466 (*регламент адресного пространства IP*).

Конфликты в присвоении IP-адресов

В данном приложении рассматриваются ситуации, в которых могут возникнуть конфликты IP-адресов. Абоненты с дублирующимися IP-адресами не смогут выходить в Интернет.

Случай А: - работает с одним и тем же IP-адресом в сетях LAN и WAN

На следующем рисунке показан пример, в котором - использует IP-адрес на стороне WAN, совпадающий с IP-адресом компьютера в сети LAN.

Рис. 229 Конфликты IP-адресов: случай А

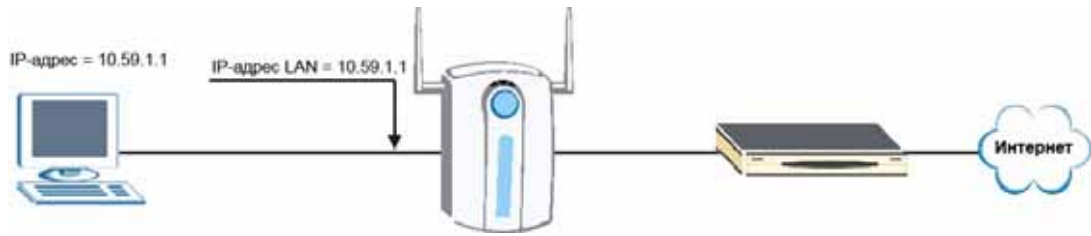


Если в - включён DHCP-сервер, необходимо задать для - различные IP-адреса LAN и WAN из непересекающихся подсетей. Например, в сети WAN можно назначить IP-адрес 192.59.1.1 а в сети LAN - адрес 10.59.1.1. В остальных случаях рекомендуется использовать для - глобальный IP-адрес в сети WAN.

Случай В: IP-адрес - в сети LAN конфликтует с IP-адресом DHCP-клиента

На следующем рисунке рассмотрена работа - в качестве DHCP-сервера. IP-адрес, присвоенный устройством - DHCP-клиенту в локальной сети, совпал с IP-адресом порта LAN.

Рис. 230 Конфликты IP-адресов: случай В

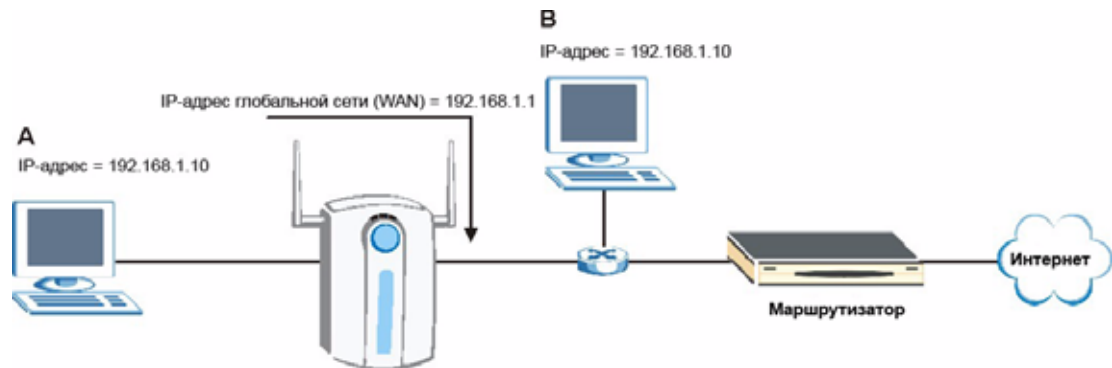


Чтобы разрешить эту проблему, необходимо убедиться, что IP-адрес - на стороне LAN не входит в пул IP-адресов DHCP.

Случай С: IP-адрес абонента совпадает с IP-адресом сетевого устройства

На следующем рисунке приведён пример, в котором IP-адрес абонента совпадает с IP-адресом некоего сетевого устройства, не подключённого напрямую к -.

Рис. 231 Конфликты IP-адресов: случай С



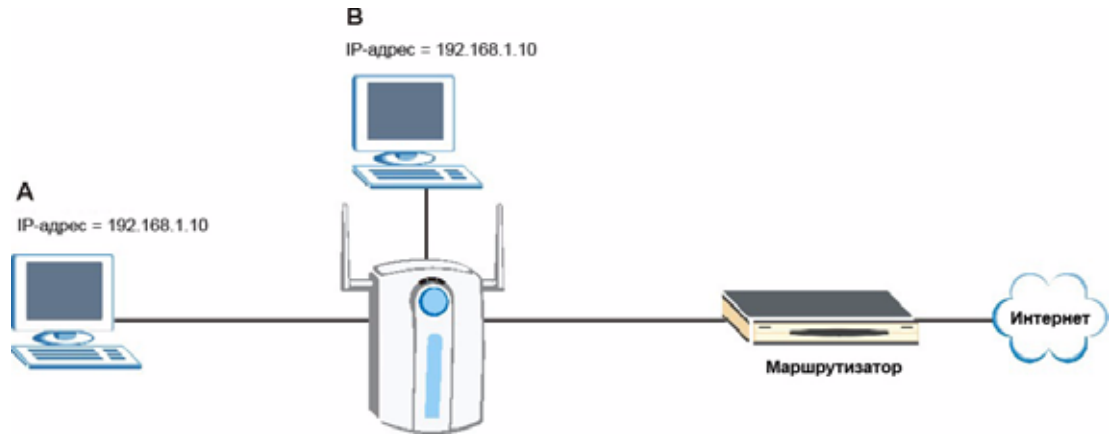
Если в - включён DHCP-сервер, необходимо задать для - различные IP-адреса LAN и WAN из непересекающихся подсетей. Например, в сети WAN можно назначить IP-адрес 192.59.1.1 а в сети LAN - адрес 10.59.1.1. В остальных случаях рекомендуется использовать для - глобальный IP-адрес в сети WAN.

Случай D: двое или несколько абонентов имеют одинаковый IP-адрес.

Преобразуя все частные IP-адреса в IP-адрес, используемый в сети WAN, - обеспечит выход в Интернет пользователям с различными настройками сети. Однако в некоторых ситуациях два или более абонентов могут иметь одинаковый частный IP-адрес. Это происходит, в частности, в тех случаях, когда настроенный у одного из абонентов статический (фиксированный) IP-адрес совпадает с адресом, присвоенным DHCP-сервером устройства - другому абоненту, чей компьютер является клиентом DHCP.

При этом абоненты не смогут выходить в Интернет.

Рис. 232 Конфликты IP-адресов: случай D:



Для устранения этой проблемы необходимо включить в сеть коммутатор с поддержкой VLAN или перевести все компьютеры в режим динамического получения IP-адресов.

Распространенные сетевые службы

В следующей таблице перечислены часто используемые сетевые службы и соответствующие им типы протоколов и номера портов. Подробный перечень номеров портов и сетевых служб, а также кодов и типов сообщений ICMP см. на сайте IANA (Комитета по цифровым адресам в Интернете).

- **Наименование:** это краткое название службы. Можно использовать это название или указать другое.
- **Протокол:** это тип протокола IP, используемого данной службой. Если в этом поле указано **TCP/UDP**, то для данной службы на одном номере порта используются одновременно TCP и UDP. Если в качестве протокола указан **ПОЛЬЗОВАТЕЛЬСКИЙ**, то в графе **Порт(ы)** указан номер протокола IP, а не номер порта.
- **Порт(ы):** значение зависит от содержимого поля **Протокол**. Дополнительные сведения о номерах портов см. в документе RFC 1700.
 - Если в графе **Протокол** указан **TCP, UDP** или **TCP/UDP**, здесь приводится номер порта IP.
 - Если в графе **Протокол** указан **ПОЛЬЗОВАТЕЛЬСКИЙ**, здесь приводится номер протокола IP.
- **Описание:** ниже приведено краткое описание применений каждой службы и ситуаций, в которых она используется.

Таблица 111 Часто используемые сетевые службы

NAME	PROTOCOL	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	Пользовательский	51	Эта служба используется протоколом туннелирования IPSEC AH (Authentication Header – заголовок аутентификации).
AIM/New-ICQ	TCP	5190	Служба мгновенного обмена сообщениями America Online. Этот порт также используется ICQ по умолчанию в качестве входного порта.
AUTH	TCP	113	Протокол аутентификации, используемый некоторыми серверами.
BGP	TCP	179	Протокол для граничных маршрутизаторов.
BOOTP_CLIENT	UDP	68	DHCP-клиент.

Таблица 111 Часто используемые сетевые службы (продолжение)

NAME	PROTOCOL	ПОРТ(Ы)	ОПИСАНИЕ
BOOTP_SERVER	UDP	67	DHCP-сервер.
CU-SEEME	TCP UDP	7648 24032	Популярное решение для видеоконференций, разработанное White Pines Software.
DNS	TCP/UDP	53	Сервер доменных имен. Служба, которая ставит в соответствие буквенным адресам (например, www.zyxel.com) IP-адреса.
ESP (IPSEC_TUNNEL)	Пользовательский	50	Эта служба используется протоколом IPSEC ESP (Encapsulation Security Protocol – протокол защищенного сокрытия содержания).
FINGER	TCP	79	Finger – команда, позволяющая проверять состояние пользователя в системах UNIX или Интернете.
FTP	TCP TCP	20 21	Протокол передачи файлов используется для пересылки файлов, в особенности – больших объемов данных, которые невозможно передать по электронной почте.
H.323	TCP	1720	Этот протокол используется программой NetMeeting.
HTTP	TCP	80	Протокол передачи гипертекста – клиент-серверный протокол для “Всемирной паутины”.
HTTPS	TCP	443	HTTPS - защищенный сеанс HTTP, часто используемый в электронной коммерции.
ICMP	Пользовательский	1	Межсетевой протокол контрольных сообщений часто используется в диагностических целях или для установления маршрутов.
ICQ	UDP	4000	Это популярная программа для общения в Интернете.
IGMP (MULTICAST)	Пользовательский	2	Протокол Internet Group Multicast Protocol используется при отправке пакетов отдельной группе хостов.
IKE	UDP	500	Для распространения ключей и управления ключами используется алгоритм IKE (Internet Key Exchange – обмен ключами в Интернете).
IRC	TCP/UDP	6667	Это популярная служба для общения (чата) в Интернете.
MSN Messenger	TCP	1863	Служба мгновенного обмена сообщениями Microsoft Network использует этот протокол.
NEW-ICQ	TCP	5190	Программа для общения в Интернете.
NEWS	TCP	144	Протокол для групп новостей.

Таблица 111 Часто используемые сетевые службы (продолжение)

NAME	PROTOCOL	ПОРТ(Ы)	ОПИСАНИЕ
NFS	UDP	2049	Сетевая файловая система (NFS) – распределенная клиент-серверная файловая система, которая обеспечивает прозрачный совместный доступ к файлам в сетевых средах.
NNTP	TCP	119	Сетевой протокол передачи новостей – механизм доставки сообщений для групп новостей USENET.
PING	Пользовательский	1	Пакетный межсетевой объединитель (Packet INternet Grouper) – это протокол отправки эхозапросов ICMP для проверки доступности удаленного хоста.
POP3	TCP	110	Почтовый протокол версии 3 позволяет клиентскому компьютеру получать электронную почту с сервера POP3 по временному соединению (посредством TCP/IP или другого протокола).
PPTP	TCP	1723	Двухточечный протокол туннелирования обеспечивает защищенную передачу данных по сетям общего пользования. Эта служба соответствует управляющему каналу.
PPTP_TUNNEL (GRE)	Пользовательский	47	Двухточечный протокол туннелирования обеспечивает защищенную передачу данных по сетям общего пользования. Эта служба соответствует каналу данных.
RCMD	TCP	512	Служба удаленного выполнения команд.
REAL_AUDIO	TCP	7070	Протокол поточной передачи аудиоданных, обеспечивающий передачу звука в реальном времени по WWW.
REXEC	TCP	514	Демон удаленного выполнения команд.
RLOGIN	TCP	513	Служба удаленного входа в систему.
RTELNET	TCP	107	Удаленный Telnet.
RTSP	TCP/UDP	554	Протокол поточного вещания в реальном времени (RTSP) – это служба дистанционного управления мультимедиа-вещанием в Интернете.
SFTP	TCP	115	Упрощенный протокол передачи файлов.
SMTP	TCP	25	Простой протокол передачи почты – стандарт обмена почтовыми сообщениями в Интернете. SMTP позволяет передавать сообщения от одного почтового сервера к другому.
SNMP	TCP/UDP	161	Упрощенный протокол управления сетью.
SNMP-TRAPS	TCP/UDP	162	Прерывания, используемые SNMP (RFC:1215).

Таблица 111 Часто используемые сетевые службы (продолжение)

NAME	PROTOCOL	ПОРТ(Ы)	ОПИСАНИЕ
SQL-NET	TCP	1521	Язык структурированных запросов (SQL) – интерфейс для доступа к данным в различных СУБД, включая СУБД на мейнфреймах, системах среднего уровня, UNIX-системах и сетевых серверах.
SSH	TCP/UDP	22	Программа для защищенного удаленного входа в системную оболочку.
STRM WORKS	UDP	1558	Протокол Stream Works.
SYSLOG	UDP	514	SYSLOG позволяет оставлять сообщения в файле журнала на UNIX-сервере.
TACACS	UDP	49	Протокол хоста регистрации (Terminal Access Controller Access Control System – система управления доступом для контроля доступа к оконечным узлам).
TELNET	TCP	23	Telnet – протокол регистрации в системе и эмуляции терминала, распространенный в Интернете и в среде UNIX. Он предназначен для работы по сетям TCP/IP. Его основное назначение – обеспечить дистанционный доступ пользователей к хостам.
TFTP	UDP	69	TFTP (упрощенный протокол пересылки файлов) – протокол передачи файлов в Интернете, подобный FTP, но использующий UDP (протокол пользовательских датаграмм) вместо TCP (протокол управления передачей).
VDOLIVE	TCP	7000	Альтернативное решение для проведения видеоконференций.

Интерпретатор команд

Ниже приведено описание интерпретатора команд. Способ вызова интерпретатора команд из SMT описан в [разд. 30.1 на стр. 269](#). Более подробное описание этих команд см. на сайте www.zyxel.ru.



Использование недокументированных команд или некорректное выполнение настроек может нарушить работоспособность устройства или вывести его из строя.

Синтаксис команд

- Ключевые слова команд выделены шрифтом `courier new`.
- Введите ключевые слова команд именно так, как показано ниже, не сокращая.
- Обязательные поля команды заключены в угловые скобки `<>`.
- Необязательные поля команды заключены в квадратные скобки `[]`.
- Знак `|` означает “или”.

Например,

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

означает, что необходимо указать тип фильтра netbios и то, нужно ли его включить или выключить.

Использование команд

Список действительных команд можно найти, введя `help` или `?` в командной строке. Всегда вводите команду полностью. Чтобы завершить сеанс, введите `exit`.

Примеры команд

В этом разделе приведены примеры команд, поддерживаемых P-791R v2. Этот список приведен для примера и носит ориентировочный характер. Команды, поддерживаемые вашим устройством P-791R v2, могут отличаться от приведенных примеров. Дополнительные примеры см. в приложениях.

Настройка содержания журнала P-791R v2

- 1 Команда `sys logs load` загружает буфер настроек журнала, позволяющий задать типы журналов, которые будет вести устройство P-791R v2.
- 2 Список категорий журналов можно просмотреть с помощью команды `sys logs category`.

Рис. 233 Пример просмотра списка категорий журналов

```

ras> sys logs category
access          display          error            mten
upnp
    
```

- 3 Чтобы просмотреть список параметров, доступных для конкретной категории, наберите команду `sys logs category`, следом указав тип категории.

Рис. 234 Пример просмотра параметров ведения журнала

```

ras> sys logs category access
Использование: [0:none/1:log/2:alert/3:both]
    
```

- 4 Чтобы задать типы журнальных сообщений, наберите команду `sys logs category`, следом указав тип категории и параметр.
 - 0 отключает ведение журналов для данной категории, 1 указывает регистрировать только журнальные сообщения для данной категории, 2 – регистрировать только предупреждения для данной категории, 3 – регистрировать для данной категории и журнальные сообщения, и предупреждения. Для некоторых категорий определенные параметры могут быть недоступны.
- 5 Команда `sys logs save` служит для сохранения параметров в P-791R v2 (ее необходимо выполнить для сохранения журналов).

Просмотр журналов

- Команда `sys logs display` служит для просмотра всех сообщений в журнале P-791R v2.
- Команда `sys logs category display` служит для просмотра настроек журналов или для просмотра всех категорий журналов.
- Команда `sys logs display [log category]` служит для просмотра отдельной категории журналов P-791R v2.
- Команда `sys logs clear` служит для удаления всех журналов P-791R v2.

Пример команд для работы с журналами

В этом примере выполняется настройка P-791R v2 для ведения журналов доступа и предупреждений, после чего вызывается просмотр результатов.

```

ras> sys logs load
ras> sys logs category access
ras> sys logs save
ras> sys logs display access
# .time                source                destination            notes
message
0|01/01/2000 08:05:03 |192.168.1.33          |207.69.188.186       |ДОСТУП
OPPED
NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
0|01/01/2000 08:05:03 |192.168.1.33          |207.69.188.186       |ДОСТУП
OPPED
NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
2|01/01/2000 08:04:57 |192.168.1.33          |207.69.188.186       |ДОСТУП
OPPED
NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
3|01/01/2000 08:04:57 |192.168.1.33          |207.69.188.186       |ДОСТУП
OPPED
NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
4|01/01/2000 08:04:53 |192.168.1.33          |207.69.188.186       |ДОСТУП
OPPED
NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
5|01/01/2000 08:04:53 |192.168.1.33          |207.69.188.186       |ДОСТУП
OPPED
NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA

```

Команда routing

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

Эта команда указывает P-791R v2 пересылать через определенный интерфейс весь трафик, не подпадающий под правила NAT. Эта функция может использоваться, например, в том случае, если к локальной сети подключены серверы с глобальными (внешними) IP-адресами.

В следующем примере P-791R v2 пересылает весь трафик, для которого отсутствуют правила NAT, через интерфейс LAN.

Рис. 235 Пример вызова команды routing

```

ras> ip nat routing 2 0
Routing can work in NAT when no NAT rule match.
-----
LAN : yes

```

Обработка ARP и группа команд ARP ackGratuitous

P-791R v2 не принимает отклики ARP, если от P-791R v2 не был отправлен соответствующий запрос. Это исключает возможность подмены IP- и MAC-адресов в таблицы ARP P-791R v2 путем отправки фальсифицированного отклика ARP. Наличие неверной привязки IP-адреса к MAC-адресу в таблице ARP P-791R v2 может использоваться для пересылки пакетов через P-791R v2 на иные устройства вместо изначального адресата.

Команды для обработки и игнорирования произвольных запросов ARP

Хост может отправить запрос ARP для разрешения своего собственного IP-адреса. Такой запрос называется произвольным (gratuitous). IP-адреса отправителя и получателя в пакете запроса указывают на сам хост. В качестве MAC-адреса получателя в пакете содержится широковещательный адрес Ethernet (FF:FF:FF:FF:FF:FF). Это позволяет определить, имеются ли в сети другие хосты, IP-адреса которых совпадают с IP-адресом изготовителя. Кроме того, другие хосты в сети получают возможность обновить свои таблицы ARP, включив в них IP-адрес хоста и соответствующий ему MAC-адрес.

Команды `ip arp ackGratuitous` задают режим обработки произвольных запросов ARP на P-791R v2.

- Чтобы указать P-791R v2 игнорировать произвольные запросы ARP, введите команду `ip arp ackGratuitous active no`.
- Чтобы указать P-791R v2 отвечать на произвольные запросы ARP, введите команду `ip arp ackGratuitous active yes`.

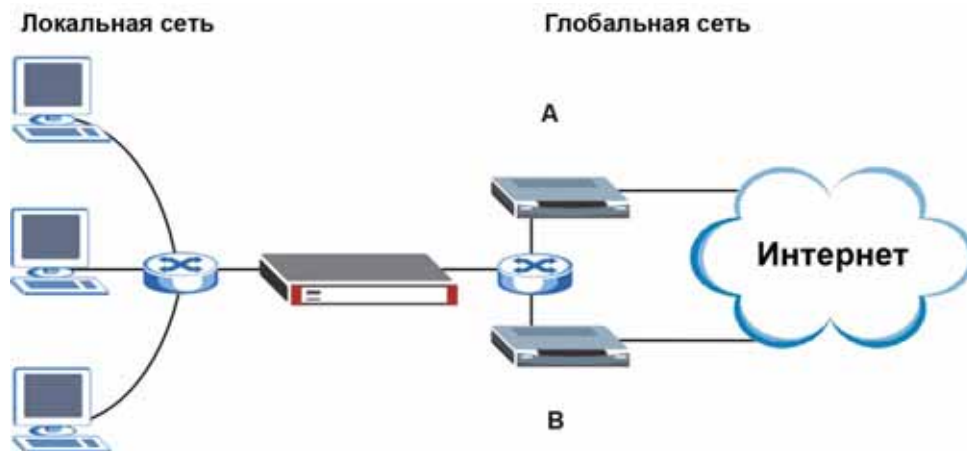
Рассмотрим следующий пример: обычно используемый шлюз становится недоступен, и резервный шлюз отправляет произвольный запрос ARP. Если IP-адрес, к которому относится запрос, отсутствует в таблице ARP P-791R v2, то P-791R v2 отправляет запрос ARP, чтобы определить, какой хост использует данный IP-адрес. После получения ответа от резервного шлюза P-791R v2 добавляет новую запись в таблицу ARP.

Если в таблице ARP P-791R v2 уже содержится запись с соответствующим IP-адресом, то ответ P-791R v2 будет зависеть от режима, выбранного командой `ip arp ackGratuitous forceUpdate`.

- Команда `ip arp ackGratuitous forceUpdate on` указывает P-791R v2 принудительно заменить MAC-адрес в таблице ARP.
- Команда `ip arp ackGratuitous forceUpdate off` отключает замену MAC-адреса в таблице ARP P-791R v2.

Использование резервного шлюза (см. следующий рисунок) является одним из случаев, когда принудительное обновление таблицы ARP в ответ на произвольные запросы необходимо. В определенный момент шлюз А перестает работать, и его место занимает резервный шлюз (В) с тем же статическим IP-адресом, что и у шлюза А. Шлюз В рассылает широковещательный запрос ARP для нахождения хоста, использующего его IP-адрес. Если параметр `ackGratuitous` включен и установлен в режим принудительного обновления, P-791R v2 примет произвольный запрос ARP и обновит свою таблицу ARP. В результате на P-791R v2 будет храниться актуальная таблица ARP, позволяющая пересылать пакеты через резервный шлюз. Если параметр `ackGratuitous` отключен или принудительное обновление не выбрано, P-791R v2 не обновит параметры записи в таблице ARP и не сможет пересылать пакеты через шлюз В.

Рис. 236 Резервный шлюз



Обновление записей ARP может сделать сеть более уязвимой к атакам с подменой адресов. Параметр `askGratuitous` и принудительное обновление рекомендуется включать только в том случае, если они необходимы, как в рассмотренном примере с резервным шлюзом. Включение принудительного обновления во всех случаях представляет повышенную опасность, поскольку P-791R v2 будет обновлять таблицу ARP даже в том случае, если соответствующая запись в ней уже существует.

Формат журналов

В этом приложении приведены расшифровки сообщений в журналах.

Таблица 112 Журналы обслуживания системы

СООБЩЕНИЕ	ОПИСАНИЕ
Time calibration is successful	Маршрутизатор скорректировал время по показаниям сервера точного времени.
Time calibration failed	Маршрутизатор не может получить информацию с сервера точного времени.
WAN interface gets IP:%s	Интерфейс WAN получил новый IP-адрес от серверов DHCP, PPPoE, PPTP или сервера коммутируемого доступа.
DHCP client IP expired	Истек срок действия IP-адреса DHCP-клиента.
DHCP server assigns%s	DHCP-сервер присвоил IP-адрес клиенту.
Successful WEB login	Пользователь вошел в интерфейс веб-конфигуратора маршрутизатора.
WEB login failed	Пользователю не удалось войти в интерфейс веб-конфигуратора маршрутизатора.
Successful TELNET login	Пользователь вошел в маршрутизатор через telnet.
TELNET login failed	Пользователю не удалось войти в маршрутизатор через telnet.
Successful FTP login	Пользователь вошел в маршрутизатор через tftp.
FTP login failed	Пользователю не удалось войти в маршрутизатор через tftp.
NAT Session Table is Full!	Превышено максимальное число записей в таблице сеансов NAT, таблица переполнена.
Starting Connectivity Monitor	Идет запуск сетевого монитора.
Time initialized by Daytime Server	Маршрутизатор получил дату и время с сервера Daytime.
Time initialized by Time server	Маршрутизатор получил дату и время с сервера точного времени.
Time initialized by NTP server	Маршрутизатор получил дату и время с сервера NTP.
Connect to Daytime server fail	Маршрутизатор не смог подключиться к серверу Daytime.
Connect to Time server fail	Маршрутизатор не смог подключиться к серверу точного времени.
Connect to NTP server fail	Маршрутизатор не смог подключиться к серверу NTP.

Таблица 112 Журналы обслуживания системы (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Too large ICMP packet has been dropped	Маршрутизатор удалил ICMP-пакет недопустимо большого размера.
Configuration Change: PC = 0x%x, Task ID = 0x%x	Маршрутизатор сохраняет изменения в настройках.
Successful SSH login	Пользователь вошел в маршрутизатор через встроенный SSH-сервер.
SSH login failed	Пользователю не удалось войти в маршрутизатор через встроенный SSH-сервер.
Successful HTTPS login	Пользователь вошел в веб-конфигуратор маршрутизатора по протоколу HTTPS.
HTTPS login failed	Пользователю не удалось войти в веб-конфигуратор маршрутизатора по протоколу HTTPS.

Таблица 113 Системные журналы ошибок

СООБЩЕНИЕ	ОПИСАНИЕ
%s exceeds the max. number of session per host!	При очередной попытке создания сеанса NAT было превышено ограничение на емкость таблицы сеансов NAT для конкретного хоста.
setNetBIOSFilter: calloc error	Маршрутизатор не смог выделить память для параметров настройки фильтра NetBIOS.
readNetBIOSFilter: calloc error	Маршрутизатор не смог выделить память для параметров настройки фильтра NetBIOS.
WAN connection is down.	Соединение с WAN отсутствует. Вы не можете получить доступ к сети через этот интерфейс.

Таблица 114 Журналы контроля доступа

СООБЩЕНИЕ	ОПИСАНИЕ
Packet without a NAT table entry blocked: [TCP UDP IGMP ESP GRE OSPF]	Маршрутизатор заблокировал пакет, для которого отсутствует соответствующая запись в таблице NAT.
Router sent blocked web site message: TCP	Маршрутизатор отправил сообщение, уведомляющее пользователя о том, что в маршрутизаторе заблокирован доступ к запрошенному пользователем веб-сайту.

Таблица 115 Журналы пакетов сброса TCP

СООБЩЕНИЕ	ОПИСАНИЕ
Under SYN flood attack, sent TCP RST	Маршрутизатор отправил пакет сброса TCP, поскольку хост подвергнулся атаке "SYN Flood" (число частично открытых сеансов TCP указывается для хоста адресата.)

Таблица 115 Журналы пакетов сброса TCP (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Exceed TCP MAX incomplete, sent TCP RST	Маршрутизатор отправил пакет сброса TCP, поскольку число частично открытых сеансов TCP превысило заданный пользователем порог (число частично открытых сеансов TCP указывается для хоста адресата.)
Peer TCP state out of order, sent TCP RST	Маршрутизатор отправил пакет сброса TCP, обнаружив нарушение порядка состояний TCP-соединения.

Таблица 116 Журналы фильтрации пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
[TCP UDP ICMP IGMP Generic] packet filter matched (set:%d, rule:%d)	Попытка доступа совпала с настроенным правилом фильтра (набор и номер правила указаны в скобках) и была заблокирована или разрешена согласно правилу.

Таблица 117 Журналы ICMP

СООБЩЕНИЕ	ОПИСАНИЕ
Packet without a NAT table entry blocked: ICMP	Маршрутизатор заблокировал пакет, для которого отсутствует соответствующая запись в таблице NAT.
Router reply ICMP packet: ICMP	Маршрутизатор отослал ответный ICMP-пакет отправителю.

Таблица 118 Журналы вызовов (CDR)

СООБЩЕНИЕ	ОПИСАНИЕ
board%d line%d channel%d, call%d,%s C01 Outgoing Call dev=%x ch=%x%s	Маршрутизатор получил требования для подготовки вызова. "call" – учетный (порядковый) номер вызова. "dev" – тип устройства (3 – коммутируемый доступ, 6 – PPPoE, 10 – PPTP). "channel" или "ch" – идентификатор канала вызова. Например, запись "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" означает, что маршрутизатор три раза вызывал сервер PPPoE.
board%d line%d channel%d, call%d,%s C02 OutCall Connected%d%s	Установлено соединение при вызове посредством PPPoE, PPTP или коммутируемого доступа.
board%d line%d channel%d, call%d,%s C02 Call Terminated	Вызов PPPoE, PPTP или коммутируемого доступа разъединен.

Таблица 119 Журналы PPP

СООБЩЕНИЕ	ОПИСАНИЕ
ppp:LCP Starting	Начат этап PPP-соединения с использованием протокола управления соединением (LCP).
ppp:LCP Opening	Открывается этап PPP-соединения с использованием протокола управления соединением (LCP).

Таблица 119 Журналы PPP (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
ppp:CHAP Opening	Открывается этап PPP-соединения с использованием протокола аутентификации с предварительным согласованием вызова (CHAP).
ppp:IPCP Starting	Начат этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).
ppp:IPCP Opening	Открывается этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).
ppp:LCP Closing	Закрывается этап PPP-соединения с использованием протокола управления соединением (LCP).
ppp:IPCP Closing	Закрывается этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).

Таблица 120 Журналы IKE

СООБЩЕНИЕ	ОПИСАНИЕ
Active connection allowed exceeded	Процесс IKE для нового соединения не выполнен из-за превышения предельного числа SA для фазы 2.
Start Phase 2: Quick Mode	Начата фаза 2 в быстром режиме.
Verifying Remote ID failed:	Соединение на фазе 2 IKE не установлено, поскольку локальные/удаленные адреса маршрутизатора и противоположной стороны соединения не совпали.
Verifying Local ID failed:	Соединение на фазе 2 IKE не установлено, поскольку локальные/удаленные адреса маршрутизатора и противоположной стороны соединения не совпали.
IKE Packet Retransmit	Маршрутизатор повторно отправил последний отправленный пакет из-за отсутствия отклика удаленной стороны.
Failed to send IKE Packet	Ошибка Ethernet не позволила маршрутизатору отправить пакеты IKE.
Too many errors! Deleting SA	SA удалена из-за недопустимо высокого числа ошибок.
Phase 1 IKE SA process done	Фаза 1 процесса IKE SA завершена.
Duplicate requests with the same cookie	Маршрутизатор получил несколько запросов от одной удаленной стороны, не успев обработать первый полученный от нее пакет IKE.
IKE Negotiation is in process	Маршрутизатор уже начал согласование соединения с удаленной стороной, но процесс IKE пока не завершен.
No proposal chosen	Параметры фазы 1 или фазы 2 не совпадают. Проверьте все протоколы и настройки. В частности, соединение невозможно, если в одном устройстве выбран алгоритм шифрования 3DES, а в другом – DES.
Local / remote IPs of incoming request conflict with rule <%d>	В качестве адреса защищенного шлюза выбран "0.0.0.0". Маршрутизатор, приняв в качестве адреса удаленной стороны локальный адрес противоположной стороны соединения, нарушил статическое правило с номером %d, и соединение было запрещено.
Cannot resolve Secure Gateway Addr for rule <%d>	Маршрутизатор не смог получить IP-адрес из доменного имени, указанного в качестве адреса защищенного маршрутизатора.

Таблица 120 Журналы IKE (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Peer ID: <код удаленной стороны> <наш удаленный тип> -<наш локальный тип>	Указанные коды не совпадают у двух сторон соединения.
vs. My Remote <наш удаленный код> -<наш локальный код>	Указанные коды не совпадают у двух сторон соединения.
vs. My Local <наш локальный код>-<наш локальный код>	Указанные коды не совпадают у двух сторон соединения.
Send <пакет>	Отправлен пакет.
Recv <пакет>	Для передачи данных в IKE используется протокол ISAKMP. Каждый пакет ISAKMP содержит несколько типов полезных нагрузок. Сведения о всех них отражаются в журнале. Полный список типов полезных нагрузок ISAKMP см. в документе RFC2408.
Recv <режим: Main или Aggressive> Mode request from <IP>	С указанного адреса удаленной стороны маршрутизатор получил запрос согласования IKE.
Send <режим: Main или Aggressive> Mode request to <IP>	Маршрутизатор начал согласование с удаленной стороной.
Invalid IP <локальный адрес удаленной стороны> / <локальный адрес удаленной стороны>	Локальный IP-адрес удаленной стороны настроен неверно.
Remote IP <IP-адрес удаленной стороны> / <IP-адрес удаленной стороны> conflicts	В качестве адреса защищенного шлюза выбран "0.0.0.0". Маршрутизатор, приняв в качестве адреса удаленной стороны локальный адрес противоположной стороны соединения, нарушил статическое правило с номером %d, и соединение было запрещено.
Phase 1 ID type mismatch	Тип удаленного идентификатора на этом маршрутизаторе отличается от типа локального идентификатора на удаленном маршрутизаторе IPSec.
Phase 1 ID content mismatch	Содержание удаленного идентификатора на этом маршрутизаторе отличается от содержания локального идентификатора на удаленном маршрутизаторе IPSec.
No known phase 1 ID type found	Маршрутизатор не смог найти известный идентификатор фазы 1 при попытке соединения.
ID type mismatch. Local / Peer: <тип локального идентификатора/тип удаленного идентификатора>	Типы идентификаторов для фазы 1 не совпали.
ID content mismatch	Содержание идентификаторов для фазы 1 не совпало.
Configured Peer ID Content: <содержание настроенного идентификатора удаленной стороны>	Содержание идентификаторов для фазы 1 не совпало. Приведено настроенное содержание идентификатора удаленной стороны.
Incoming ID Content: <содержание входящего идентификатора удаленной стороны>	Содержание идентификаторов для фазы 1 не совпало. Приведено содержание идентификатора из входящего пакета.

Таблица 120 Журналы IKE (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Unsupported local ID Type: <%d>	Типы идентификатора для фазы 1 не поддерживаются данным маршрутизатором.
Build Phase 1 ID	Маршрутизатор начал формировать идентификатор для фазы 1.
Adjust TCP MSS to%d	Маршрутизатор автоматически изменил максимальный размер сегмента TCP после установления туннеля.
Rule <%d> input idle time out, disconnect	Туннель для указанного правила удален, поскольку в течение заданного интервала отсутствовал входящий трафик.
XAUTH succeed! Username : <Username>	Маршрутизатор разрешил указанное имя пользователя с помощью расширенной аутентификации.
XAUTH fail! Username : <Username>	Маршрутизатор не смог разрешить указанное имя пользователя с помощью расширенной аутентификации.
Rule[%d] Phase 1 negotiation mode mismatch	В указанном правиле режим согласования для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 encryption algorithm mismatch	В указанном правиле алгоритм шифрования для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 authentication algorithm mismatch	В указанном правиле алгоритм аутентификации для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 authentication method mismatch	В указанном правиле метод аутентификации для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 key group mismatch	В указанном правиле группа ключей для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 protocol mismatch	В указанном правиле протокол аутентификации для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 encryption algorithm mismatch	В указанном правиле алгоритм шифрования для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 authentication algorithm mismatch	В указанном правиле алгоритм аутентификации для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 encapsulation mismatch	В указанном правиле тип инкапсуляции для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d]> Phase 2 pfs mismatch	В указанном правиле параметр защиты от разглашения использованных ключей (pfs) для фазы 2 не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 ID mismatch	В указанном правиле идентификатор для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 hash mismatch	В указанном правиле хэш для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 preshared key mismatch	В указанном правиле предварительно согласованный ключ для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.

Таблица 120 Журналы IKE (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Rule [%d] Tunnel built successfully	Туннель IPSec для указанного правила успешно создан.
Rule [%d] Peer's public key not found	Открытый ключ удаленной стороны для фазы 1 IKE не найден для указанного правила.
Rule [%d] Verify peer's signature failed	Не удалось проверить подпись удаленной стороны на фазе 1 IKE для указанного правила.
Rule [%d] Sending IKE request	IKE направляет запрос для указанного правила.
Rule [%d] Receiving IKE request	IKE принимает запрос для указанного правила.
Swap rule to rule [%d]	Маршрутизатор переключился на указанное правило.
Rule [%d] Phase 1 key length mismatch	В указанном правиле длина ключа (для алгоритма шифрования AES) для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] phase 1 mismatch	В указанном правиле параметры фазы 1 IKE не совпадают у маршрутизатора и удаленной стороны.
Rule [%d] phase 2 mismatch	В указанном правиле параметры фазы 2 IKE не совпадают у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 key length mismatch	В указанном правиле длина ключа (для алгоритма шифрования AES) для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.

Таблица 121 Журналы PKI

СООБЩЕНИЕ	ОПИСАНИЕ
Enrollment successful	Онлайновая регистрация сертификата по протоколу SCEP выполнена успешно. В поле получателя указывается IP-адрес и номер порта на сервере центра сертификации.
Enrollment failed	Не удалось выполнить онлайновую регистрацию сертификата по протоколу SCEP. В поле получателя указывается IP-адрес и номер порта на сервере центра сертификации.
Failed to resolve <URL сервера SCEP CA>	Онлайновая регистрация сертификата на сервере SCEP не выполнена, поскольку не удалось разрешить адрес сервера центра сертификации.
Enrollment successful	Онлайновая регистрация сертификата по протоколу CMP выполнена успешно. В поле получателя указывается IP-адрес и номер порта на сервере центра сертификации.
Enrollment failed	Не удалось выполнить онлайновую регистрацию сертификата по протоколу CMP. В поле получателя указывается IP-адрес и номер порта на сервере центра сертификации.
Failed to resolve <URL сервера CMP CA>	Онлайновая регистрация сертификата на сервере CMP не выполнена, поскольку не удалось разрешить адрес сервера центра сертификации.
Rcvd ca cert: <заголовок>	Маршрутизатор получил сертификат центра сертификации с указанным заголовком с сервера LDAP, IP-адрес и номер порта которого указаны в поле источника.
Rcvd user cert: <заголовок>	Маршрутизатор получил сертификат пользователя с указанным заголовком с сервера LDAP, IP-адрес и номер порта которого указаны в поле источника.

Таблица 121 Журналы PKI (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Rcvd CRL <размер>: <выпускающий>	Маршрутизатор получил с сервера LDAP, IP-адрес и номер порта которого указаны в поле источника, список CRL (отзываемых сертификатов) с указанным размером и именем выпускающего.
Rcvd ARL <размер>: <выпускающий>	Маршрутизатор получил с сервера LDAP, IP-адрес и номер порта которого указаны в поле источника, список ARL (отзываемых центров сертификации) с указанным размером и именем выпускающего.
Failed to decode the received ca cert	Маршрутизатор получил поврежденный сертификат центра сертификации с сервера LDAP, адрес и номер порта которого указаны в поле источника.
Failed to decode the received user cert	Маршрутизатор получил поврежденный сертификат пользователя с сервера LDAP, адрес и номер порта которого указаны в поле источника.
Failed to decode the received CRL	Маршрутизатор получил поврежденный CRL (список отзываемых сертификатов) с сервера LDAP, адрес и номер порта которого указаны в поле источника.
Failed to decode the received ARL	Маршрутизатор получил поврежденный ARL (список отзываемых центров сертификации) с сервера LDAP, адрес и номер порта которого указаны в поле источника.
Rcvd data <размер> too large! Max size allowed: <макс. размер>	Маршрутизатор получил каталог недопустимо большого размера (размер указан) с сервера LDAP, адрес и номер порта которого указаны в поле источника. Также приводится максимальный размер сведений из каталога, разрешенный маршрутизатором.
Cert trusted: <заголовок>	Маршрутизатор проверил путь сертификата с указанным заголовком.
Due to <коды причин>, cert not trusted: <заголовок>	По перечисленным причинам сертификат с указанным заголовком не прошел проверку пути. Эти коды причин носят ориентировочный характер, отмечая подозрительные свойства сертификата. Расшифровку кодов см. в таб. 122 на стр. 358 .

Таблица 122 Коды причин непрохождения проверки сертификата

КОД	ОПИСАНИЕ
1	Несовпадение алгоритма сертификата с условиями поиска.
2	Несовпадение используемых ключей сертификата с условиями поиска.
3	Сертификат недействителен на соответствующем отрезке времени.
4	(Не используется)
5	Сертификат недействителен.
6	Сертификат не прошел проверку подписи.
7	Сертификат отозван списком CRL.
8	Сертификат не был добавлен в кэш.
9	Сертификат не удалось декодировать.
10	Сертификат не найден (где-либо).
11	Кольцевая цепь сертификатов (невозможно найти доверенный корневой элемент)
12	Сертификат содержит важное расширение, которое не удалось обработать.
13	Выпускающий сертификата недействителен (отсутствуют характеристики CA).

Таблица 122 Коды причин непрохождения проверки сертификата (продолжение)

КОД	ОПИСАНИЕ
14	(Не используется)
15	Список CRL устарел.
16	Список CRL недействителен.
17	Список CRL не прошел проверку подписи.
18	Список CRL не найден (где-либо).
19	Список CRL не был добавлен в кэш.
20	Список CRL не удалось декодировать.
21	Список CRL недействителен в данный момент (но вступит в силу позднее).
22	Список CRL содержит повторяющиеся серийные номера.
23	Интервал времени не непрерывен.
24	Отсутствуют сведения о времени.
25	Истекло время выполнения метода базы данных.
26	Не удалось выполнить метод базы данных.
27	Не удалось проверить путь.
28	Достигнута максимальная длина пути.

Таблица 123 Замечания по заданию ACL

НАПРАВЛЕНИЕ ДВИЖЕНИЯ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L to W)	Для трафика из LAN в WAN	ACL задается для пакетов, пересылаемых из LAN в WAN.
(W to L)	Из WAN в LAN (WAN to LAN)	ACL задается для пакетов, пересылаемых из WAN в LAN.
(L to L)	Из LAN в LAN/P-791R v2	ACL задается для пакетов, пересылаемых из LAN в LAN или на P-791R v2.
(W to W)	Из WAN в WAN/P-791R v2	ACL задается для пакетов, пересылаемых из WAN в WAN или на P-791R v2.

Таблица 124 Пояснения к кодам ICMP

ТИП	КОД	ОПИСАНИЕ
0		Отклик на эхозапрос
	0	Сообщение с откликом на эхозапрос
3		Адресат недоступен
	0	Сеть недоступна
	1	Хост недоступен
	2	Протокол недоступен
	3	Порт недоступен
	4	Пакет, для которого требовалась фрагментация, был отброшен из-за наличия флажка DF ("не фрагментировать")

Таблица 124 Пояснения к кодам ICMP (продолжение)

ТИП	КОД	ОПИСАНИЕ
	5	Маршрутизация к источнику невозможна
4		Источник должен снизить трафик
	0	Шлюз может удалять IP-датаграммы при отсутствии достаточного буфера для накопления датаграмм перед отправкой в следующую сеть по маршруту к сети адресата.
5		Переадресация
	0	Переадресация датаграмм для сети
	1	Переадресация датаграмм для хоста
	2	Переадресация датаграмм для типа службы и сети
	3	Переадресация датаграмм для типа службы и хоста
8		Эхозапрос
	0	Сообщение эхозапроса
11		Превышено допустимое время
	0	На маршруте превышено время жизни пакета (TTL)
	1	Превышено время сборки фрагментов
12		Ошибка в параметре
	0	Ошибка отмечена указателем
13		Метка времени
	0	Сообщение запроса метки времени
14		Отклик метки времени
	0	Сообщение с откликом метки времени
15		Информационный запрос
	0	Сообщение с информационным запросом
16		Информационный отклик
	0	Сообщение с информационным откликом

Таблица 125 Журналы SYSLOG

СООБЩЕНИЕ	ОПИСАНИЕ
<pre><Объект*8 + значимость>Мес дд чч:мм:сс имя_хоста src="<IP_источника:порт_источника>" dst="<IP_адресата:порт_адресата>" msg="<сообщение>" note="<примечание>" devID="<три последних разряда MAC-адреса>" cat="<категория></pre>	<p>Это сообщение отсылается системой (в качестве имени системы, если не было настроено другое имя, указывается "RAS"), когда маршрутизатор оставляет запись в системном журнале. Тип журнального объекта задается на странице MAIN MENU->LOGS->Log Settings. В качестве уровня значимости используется класс значимости SYSLOG. Расшифровка сообщений и примечаний приведена в таблицах журнальных сообщений далее в этом приложении. Поле "devID" содержит последние три символа MAC-адреса на порту LAN маршрутизатора. Поле "cat" соответствует категории в журналах маршрутизатора.</p>

В следующей таблице приведены типы полезной нагрузки ISAKMP по стандарту RFC 2408, отображаемые в журнале. Подробное описание каждого типа см. в соответствующем документе RFC.

Таблица 126 Типы полезной нагрузки ISAKMP по стандарту RFC-2408

СОДЕРЖАНИЕ ЖУРНАЛА	ТИП ПОЛЕЗНОЙ НАГРУЗКИ
SA	Ассоциация безопасности
PROP	Предложение
TRANS	Преобразование
KE	Обмен ключами
ID	Идентификация
CER	Сертификат
CER_REQ	Запрос сертификата
HASH	Хеш
SIG	Подпись
NONCE	Псевдослучайное число
NOTFY	Уведомление
DEL	Delete
VID	Код поставщика оборудования

Команды для управления журналом

В этом разделе приведены общие примеры использования команд для работы с журналами. Вывод на экран для вашего устройства может отличаться, но общий принцип работы аналогичен.

В описании интерфейса командной строки ([Приложение Г на стр. 345](#)) поясняется вызов и использование команд.

Настройка содержания журнала P-791R v2

- 1 Для загрузки буфера настроек журналов, позволяющего задать состав журналов, формируемых P-791R v2, используется команда `sys logs load`.
- 2 Для просмотра категорий журналов служит команда `sys logs category`.

Рис. 237 Пример просмотра списка категорий журналов

```

ras>?
Valid commands are:
sys          exit          ether          aux
ip           ipsec         bridge        bm
certificates cnm           8021x         radius
ras>

```

- 3 Чтобы просмотреть список параметров, доступных для конкретной категории, наберите команду `sys logs category`, следом указав тип категории.

Рис. 238 Пример просмотра параметров ведения журнала

```
ras> sys logs category access
Использование: [0:none/1:log/2:alert/3:both]
```

- 4 Чтобы задать типы журнальных сообщений, наберите команду `sys logs category`, следом указав тип категории и параметр.
0 отключает ведение журналов для данной категории, 1 указывает регистрировать только журнальные сообщения для данной категории, 2 – регистрировать только предупреждения для данной категории, 3 – регистрировать для данной категории и журнальные сообщения, и предупреждения. Для некоторых категорий определенные параметры могут быть недоступны.
- 5 Шаг 5. Запишите настройки в P-791R v2 командой `sys logs save` (эту операцию необходимо выполнить, чтобы включить ведение журналов).

Просмотр журналов

- Команда `sys logs display` служит для просмотра всех сообщений в журнале P-791R v2.
- Команда `sys logs category` служит для просмотра настроек журналов или для просмотра всех категорий журналов.
- Команда `sys logs display [log category]` служит для просмотра отдельной категории журналов P-791R v2.
- Команда `sys logs clear` служит для удаления всех журналов из P-791R v2.

Команды фильтрации NetBIOS

Ниже описаны команды для фильтрации пакетов NetBIOS. Подробнее о структуре команд см. в [Приложении G на стр. 345](#).

Введение

NetBIOS (базовая сетевая система ввода-вывода) представляет собой широковещательные пакеты TCP или UDP, позволяющие компьютеру подключаться и взаимодействовать с локальной сетью.

Пакеты NetBIOS могут приводить к вызову служб коммутлируемого доступа посредством PPPoE или PPTP, даже если эти службы не были запрошены пользователем.

Для загрузки фильтров NetBIOS выполните следующие действия:

- Разрешать или запрещать пересылку пакетов NetBIOS из LAN в WAN и из WAN в LAN.
- Разрешать или запрещать осуществление вызовов с помощью пакетов NetBIOS.

Просматривать настройки фильтра NetBIOS.

Синтаксис: `sys filter netbios disp`

Эта команда выводит (неизменяемый) список текущих режимов фильтрации в P-791R v2.

Пример вызова команды для просмотра настроек фильтра NetBIOS

```
===== NetBIOS Filter Status =====  
Between LAN and WAN: Block  
IPSec Packets: Forward  
Trigger Dial: Disabled
```

Типы имеющихся фильтров и настройки по умолчанию для них приведены ниже.

Таблица 127 Настройки фильтра NetBIOS по умолчанию

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ПРИМЕР
Between LAN and WAN	В этом поле отображается действие, выполняемое над пакетами NetBIOS при перемещении между сетями LAN и WAN: блокирование или пересылка.	Block
Trigger dial	В этом поле указывается, разрешено ли осуществлять вызовы с помощью пакетов NetBIOS. Если этот режим отключен (disabled), пакеты NetBIOS не могут использоваться для осуществления вызовов.	Disabled

Настройка фильтра NetBIOS

Синтаксис: `sys filter netbios config <тип> <on|off>`

где

`<тип>` = номер настраиваемого фильтра (0-3)
 0 = переход между сетями LAN и WAN
 3 = пересылка пакетов по IPSec
 4 = разрешение вызова

`<on|off>` = Для типов 0 и 1 значение “on” активирует фильтр, блокируя пересылку пакетов NetBIOS. Значение “off” отключает фильтр, разрешая пересылку пакетов NetBIOS.
 Для типа 4 значение “on” разрешает пакетам NetBIOS инициировать вызов по коммутируемому резервному каналу. Значение “off” запрещает пакетам NetBIOS инициировать вызов по коммутируемому резервному каналу.

Примеры команд

`sys filter netbios config 0 on` Эта команда блокирует переход пакетов NetBIOS из сети LAN в сеть WAN и в обратном направлении.

`sys filter netbios config 3 on` Эта команда блокирует пересылку пакетов NetBIOS по IPSec.

`sys filter netbios config 4 off` Эта команда запрещает инициировать вызов по коммутируемому резервному каналу в ответ на пакеты NetBIOS.

Авторское право

Авторское право © ZyXEL Communications Corp., 2007

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 Corp.

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

Торговые марки, упомянутые в данном издании, используются только в целях идентификации и являются собственностью своих законных владельцев.

Важная информация

Регистрация покупки

По завершении установки мы рекомендуем зарегистрировать ваше изделие ZyXEL через Интернет. Регистрация дает дополнительный год бесплатной гарантии, персональную техническую поддержку, уведомление по электронной почте об обновлениях, ряд других преимуществ. Адрес сайта для регистрации в вашей стране указан в главе “Гарантийное обслуживание ZyXEL”.

Информация о сертификации

Маршрутизатор SHDSL.bis P-791R v2 одобрен для применения государственными органами по сертификации. Копии действующих в вашей стране сертификатов можно получить через Интернет на домашней странице изделия в каталоге продукции.

Система сертификации ГОСТ Р, Госстандарт России

Сертификат соответствия № РОСС ТW.АЯ46.В56758.

Срок действия с 19.06.2007 по 18.06.2010.

Соответствует требованиям: ГОСТ Р МЭК 60950-2002,

ГОСТ Р 51318.22-99 (класс Б), ГОСТ Р 51318.24-99 (группа 1), ГОСТ Р 51317.3.2-99, ГОСТ Р 51318.3.3-99.

Государственная санитарно-эпидемиологическая служба РФ

Санитарно-эпидемиологическое заключение

№ 77.01.09.650.П.057201.07.07.

Срок действия с 31.07.2007 по 30.07.2012.

Соответствует требованиям: СанПиН 2.2.2./2.4.1340-03, СанПиН 2.1.8./2.2.4.1190-03.



Юридический адрес ИЗГОТОВИТЕЛЯ

Зайксел Коммуникэйшнз Корп., Инновэйшн Род II, 6,
Сайнс-бейсд Индастриал Парк, Син-Чу, Тайвань
ZyXEL Communications Corporation, 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 Communications Corp., 2007. Все права защищены

Воспроизведение, адаптация, перевод и распространение данного документа или любой его части без предварительного письменного разрешения ZyXEL запрещены — за исключением случаев, допускаемых законодательством об авторском праве. Названия продуктов или компаний, упоминаемые в данном руководстве, могут быть товарными знаками или знаками обслуживания соответствующих правообладателей.

Компания ZyXEL не дает никакой другой гарантии на продукты и услуги, кроме явно указанной в условиях, прилагаемых к таким продуктам и услугам. Никакая часть данного документа, кроме раздела «Гарантийное обслуживание ZyXEL», не может рассматриваться как дополнительные гарантийные обязательства.

ZyXEL оставляет за собой право вносить изменения и улучшения в любой продукт, описанный в этом документе, а также в сам документ в любое время без предварительного уведомления.

Гарантийное обслуживание ZyXEL

Мы гордимся надежностью и качеством нашей продукции и верим, что она прослужит вам безотказно долгие годы. Тем не менее, если у вас возникнут вопросы при использовании этого изделия, пожалуйста, обратитесь за помощью в региональное представительство ZyXEL.

Гарантийные обязательства

Корпорация ZyXEL заявляет об отказе от любой ответственности, возникающей в силу применения или эксплуатации ее продукции или программного обеспечения, описанных в настоящем документе. Корпорация ZyXEL не выдает никаких лицензий ни в пределах своих патентных прав, ни в пределах патентных прав других сторон. Корпорация ZyXEL оставляет за собой право вносить изменения в описанную в настоящем документе продукцию без уведомления. Данный документ может быть изменен без уведомления.

1. Настоящая гарантия действует в течение трех лет с даты приобретения изделия ZyXEL и подразумевает гарантийное обслуживание при обнаружении 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 далее в таблице «Контактная информация», 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: SY Y x W - W xxxxxx, где Y Y — две последние цифры года, а W W — 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, если:
 - серийный номер на изделии изменен, стерт, удален или неразборчив;
 - изделие переделывалось без предварительного письменного согласия ZyXEL;
 - изделие неправильно эксплуатировалось, в том числе:
 - а) использовалось не по назначению или не в соответствии с руководством пользователя,
 - б) устанавливалось или эксплуатировалось в условиях, не соответствующих стандартам и нормам безопасности, действующим в стране использования;
 - изделие ремонтировалось не уполномоченными на то сервисными центрами или дилерами;
 - изделие вышло из строя по причине несчастного случая, удара молнии, затопления, пожара, неправильной вентиляции и иных причин, находящихся вне контроля ZyXEL;
 - изделие пострадало при транспортировке, за исключением случаев, когда она производится авторизованным сервисным центром;
 - изделие использовалось в дефектной системе.

Контактная информация

	Россия	Украина	Казахстан	Узбекистан
Веб-сайт	zyxel.ru	ua.zyxel.com	zyxel.kz	
Поддержка в Интернете	zyxel.ru/help	ua.zyxel.com/help	zyxel.kz/help	
Поддержка по телефону				
Бесплатный номер	(800) 200-8929	(800) 504-0040	(800) 080-0055	
Дополнительный номер	(495) 542-8929	(044) 247-6978	(3272) 590-689	
Представительство ZyXEL	ZyXEL Россия 117279, Москва, ул. Островитянова, дом 37а (495) 542-8920	ZyXEL Украина 04050, Киев, ул. Пимоненко, дом 13 (044) 494-4931	ZyXEL Казахстан 050010, Алматы, пр. Достык, 43, офис 414 (3272) 590-699	

О компании ZyXEL

О компании ZyXEL

С момента основания в 1989 году компания ZyXEL Communications самостоятельно разрабатывает и создает решения, обеспечивающие надежный и удобный доступ в Интернет. Находясь на переднем крае технологий связи, в каждом поколении своей продукции ZyXEL неизменно предлагает оптимальную реализацию промышленных стандартов. Добившись мирового признания в области модемов для коммутируемого доступа, компания предложила линейку революционных устройств широкополосного доступа и первой раскрыла тему аппаратных средств интернет-безопасности для массового пользователя. Последовательно развивая скорость связи и удобство абонентской интернет-техники, сейчас компания лидирует на рынке DSL и кропотливо работает в перспективных технологических направлениях, таких как VoIP, ЕТТН и WiMAX. Наряду с этим ZyXEL поставляет передовые инфраструктурные решения интернет-провайдерам и корпоративным заказчикам, в том числе для проектов национального масштаба. В создании новой продукции, которая сегодня поставляется в семьдесят стран мира, участвуют три научно-исследовательских центра.

На территории СНГ компания ZyXEL работает с 1992 года, взяв курс на полную адаптацию продукции к местным условиям. Подготовка сертифицированных инженеров ведется в трех авторизованных учебных центрах, услуги по обслуживанию оборудования ZyXEL осуществляет сеть авторизованных сервисных центров во всех крупных городах стран СНГ. На региональных веб-сайтах ZyXEL действует уникальная интерактивная система консультаций, а прямая бесплатная связь с Центром информации и поддержки доступна в любом населенном пункте, где есть телефон. Интернет-техникой ZyXEL пользуются миллионы домашних пользователей, и имя компании для них стало синонимом надежной связи и выхода в Интернет с первой попытки.

Указатель

А

авторские права [365](#), [367](#), [371](#), [373](#)
альтернативный способ записи маски подсети [330](#)

В

веб-конфигуратор [34](#), [37](#)
 вызов [37](#)
 минимальные требования [37](#)
Влажность: [297](#)
возврат к заводским настройкам [46](#), [161](#)
выдерживаемая скорость передачи ячеек (SCR) [67](#)
высокоскоростной доступ в Интернет [33](#)

Г

гарантия [367](#)
Глобальная сеть. См. WAN.

Д

деление на подсети [330](#)
динамическая DNS [121](#)
 шаблон [121](#)
 www.dyndns.org [121](#)
Динамический протокол настройки хоста. См. DHCP.
Доступ к Интернету [49](#)
 настройка с помощью мастеров [49](#)
другие документы [3](#)

Ж

журнал [155](#)

З

закрепленное соединение [65](#)
Значок мастера [49](#)

И

Идентификатор виртуального канала. См. VCI.
Идентификатор виртуального пути. См. VPI.
имя домена [149](#)
имя системы [149](#)
инкапсуляция [63](#)
 ENET ENCAP. См. ENET ENCAP
 PPPoA. См. PPPoA.
 PPPoE. См. PPPoE.
 RFC 1483. См. RFC 1483.
интерпретатор командной строки (KC) [269](#)
интерфейс командной строки [34](#)
интерфейс резервирования через коммутируемый доступ [79](#)
информационная база управления (MIB) [129](#)
информационный протокол маршрутизации. См. RIP.
использование команд [270](#)
использование консольного порта [266](#)
история вызовов [270](#)

К

категории журналов [156](#)
класс трафика [67](#)
 неуказанная битовая скорость (UBR) [68](#)
 переменная скорость (VBR) [68](#)
 постоянная скорость (CBR) [67](#)
Класс трафика ATM. См. "класс трафика".
класс IP-адресов
 и IGMP [91](#)
кнопка сброса [46](#)
Комитет по цифровым адресам в Интернете
 См. IANA. [335](#)
консольный порт
 для восстановления файла настроек [262](#)
 для обновления микропрограммы [266](#)

для резервного копирования файла настроек **260**
 Контроль доступа к передающей среде. См. "MAC-адрес".

Л

логическая сеть. См. "совмещение IP-адресов".
 логический интерфейс. См. "совмещение IP-адресов".
 Локальная вычислительная сеть. См. LAN.

М

маска подсети **90, 328**
 межсетевой протокол многоадресной групповой рассылки. См. IGMP.
 меры безопасности **6**
 метрика **66**
 и политика маршрутизации **66**
 и предопределенная политика **66**
 многоадресная рассылка **91**
 мультиплексирование **64**
 LLC **64**
 VC **64**

Н

набор расписаний **285**
 набор фильтров **227**
 данных **227**
 и удаленный узел **202**
 и NAT **238**
 правила фильтров TCP/IP **232**
 структура **228**
 универсальное правило фильтра **234**
 набор фильтров данных. См. набор фильтров, данных.
 неуказанная битовая скорость (UBR) **68**
 номер сети **89**
 рекомендуемые значения для сети LAN **89**

О

области применения
 высокоскоростной доступ в Интернет **33**
 соединения "точка-точка" **34**

обновление микропрограммы **159, 255, 263, 266**
 использование FTP **264**
 использование TFTP **265**
 ограничение трафика **66**
 выдерживаемая скорость передачи ячеек (SCR) **67**
 Maximum Burst Size (MBS) **67**
 Peak Cell Rate (PCR) **67**
 основной экран
 панель навигации **39**
 отказ от ответственности **365, 369**

П

панель навигации **39**
 пароль по умолчанию **37**
 пароль по умолчанию, смена **38**
 переадресация портов **104**
 политика поставщиков услуг Интернета **104**
 сервер по умолчанию **104**
 переадресация трафика **78**
 с совмещением IP-адресов **79**
 треугольный маршрут **79**
 передняя панель **35**
 перезагрузка **163**
 перезапуск **163**
 переменная скорость (VBR) **68**
 подсеть **327**
 политика маршрутизации **277**
 действия **278**
 и метрика **66**
 критерии **278**
 политики маршрутизации IP (IPPR) См. "политика маршрутизации".
 Порт DIAL BACKUP **79**
 постоянная битовая скорость
 См. Постоянная битовая скорость
 постоянная скорость (CBR) **67**
 предупреждения **155**
 привязка адресов **108**
 прокси-сервер для DNS **88**
 протокол звеньев маршрутизации с инкапсуляции MAC-адресов. См. ENET ENCAP.
 протокол PPPoA. См. PPPoA.
 Пул IP-адресов **88**

С

светодиоды **35**
 сертификация **365, 369**

просмотр [367](#)
 уведомления [367](#)
 синтаксис команд [269](#)
 Служба доменных имён. См. DNS.
 Службы DHCP [94](#)
 совмещение IP-адресов [96](#)
 и NAT [101](#)
 с переадресацией трафика [79](#)
 соединения "точка-точка" [34, 57](#)
 инкапсуляция [57](#)
 порядок действий [58](#)
 роли устройств ZyxEL [58](#)
 условия [58](#)
 client [58](#)
 server [58](#)
 статический маршрут [117](#)

Т

таймер неактивности управления [126](#)
 Терминал управления системой
 см. SMT
 Терминал управления системой. См. SMT.
 торговые марки [365](#)
 Трансляция сетевых адресов. См. NAT.
 треугольный маршрут
 с переадресацией трафика [79](#)

У

удаленное управление [125](#)
 и таймер неактивности управления [126](#)
 и NAT [126](#)
 местоположения [125](#)
 ограничения [125, 275](#)
 число сеансов [125](#)
 DNS [132](#)
 FTP [127](#)
 ICMP [133](#)
 SNMP [130](#)
 Telnet [127](#)
 WWW [126](#)
 Удаленный сервер DHCP [94](#)
 удалённый узел [195](#)
 и набор фильтров [202](#)
 управление бюджетом [270](#)
 управление вызовами [270](#)
 управление устройством
 использование интерфейса командной строки.
 См. "интерфейс командной строки".
 использование FTP. См. FTP.

использование SMT См. SMT.
 использование SNMP. См. SNMP.
 использование Telnet. См. "интерфейс
 командной строки".
 практические рекомендации [35](#)
 с помощью веб-конфигуратора.
 См. "веб-конфигуратор".
 управляющий протокол IP (IPCP) [88](#)
 Упрощённый протокол управления сетью. См.
 SNMP.
 условные обозначения и синтаксис [4](#)
 Учетная запись одного пользователя См. SUA.

Ф

файл настроек [255](#)
 восстановление [161, 261](#)
 восстановление с использованием FTP [261](#)
 восстановление через консольный порт [262](#)
 резервное копирование [161, 256](#)
 резервное копирование по протоколу FTP [257](#)
 резервное копирование по TFTP [258](#)
 резервное копирование через консольный
 порт [260](#)
 файл настроек системы (резервное копирование
 и восстановление) [161](#)

Х

характеристики [297](#)

Ш

Шлюз прикладного уровня [102](#)
 Шлюз прикладного уровня для SIP [102](#)
 Шлюз прикладного уровня См. ALG.
 шурупы [300](#)

Э

экран входа [38](#)
 экран выбора режима [39](#)
 экран смены пароля [38](#)
 Экран DHCP Relay [94](#)

A

ALG [102](#)
включение SIP/FTP/H.323 [103](#)

C

CBR [73, 78](#)

D

DHCP [88](#)
DHCP-сервер [94](#)
DNS [88](#)
удаленное управление [132](#)
DNS-сервер [88](#)
запоминание через IPCP [88](#)
статический IP-адрес [88](#)

E

ENET ENCAP [63](#)
и IP-адрес [65](#)

F

FTP [34](#)
для восстановления файла настроек [261](#)
для обновления микропрограммы [264](#)
для резервного копирования файла настроек
[257](#)
удаленное управление [127](#)

I

IANA [335](#)
ICMP [133](#)
удаленное управление [133](#)
IGMP [91](#)
и класс IP-адресов [91](#)
version [91](#)
IP-адрес
динамический [65](#)
и ENET ENCAP. [65](#)
и PPPoA/PPPoE [65](#)

и RFC 1483 [65](#)
номер сети. См. номер сети.
статический [65](#)
частный [90](#)

L

LAN [87](#)
и WAN [87](#)
LLC (мультиплексирование) [64](#)

M

MAC-адрес [95](#)
Maximum Burst Size (MBS) [67](#)

N

NAT [66, 99, 334](#)
внешний хост [99](#)
внутренний хост [99](#)
глобальный адрес [99](#)
и набор фильтров [238](#)
и удаленное управление [126](#)
локальный адрес [99](#)
многие к одному [101](#)
многие ко многим без перегрузки [101](#)
многие ко многим с перегрузкой [101](#)
назначение [100](#)
один к одному [101](#)
показания к использованию [89](#)
привязка адресов. См. "привязка адресов" [108](#)
примеры [218](#)
принцип работы [100](#)
с совмещением IP-адресов [101](#)
см. "переадресация портов". см. "переадресация портов".
типы привязки [101](#)
SUA См. SUA.
server [100, 102](#)

P

PPP поверх Ethernet См. PPPoE.
PPPoA [64](#)
закрепленное соединение [65](#)
и IP-адрес [65](#)
PPPoE [63](#)

закрепленное соединение [65](#)
и клиентское программное обеспечение [64](#)
и IP-адрес [65](#)
методы доступа и аутентификации [63](#)
сетевые службы [63](#)
Peak Cell Rate (PCR) [67](#)

R

RFC 1112. См. IGMP.
RFC 1213 [130](#)
RFC 1215 [130](#)
RFC 1466 [90](#)
RFC 1483 [64](#)
и IP-адрес [65](#)
RFC 1597 [90](#)
RFC 1631. См. NAT.
RFC 2131. См. DHCP.
RFC 2132. См. DHCP.
RFC 2236. См. IGMP.
RIP [90](#)
направление [90](#)
version [91](#)
Remote DHCP Server [94](#)

S

SIP
ALG [102](#)
SMT [34](#), [169](#)
вызов [169](#)
перемещение [174](#)
пункты меню [170](#)
SNMP [34](#), [129](#)
агент [129](#)
диспетчер [129](#)
запрос Get [130](#)
запрос GetNext [130](#)
операции [130](#)
прерывания [130](#)
удаленное управление [130](#)
MIB [129](#)
Set [130](#)
Trap [130](#)
SUA [102](#)

T

TFTP

для обновления микропрограммы [265](#)
для резервного копирования файла настроек
[258](#)
Telnet
удаленное управление [127](#)

U

UBR [73](#), [78](#)
URL по умолчанию [37](#)

V

VBR [73](#), [78](#)
VC (мультиплексирование) [64](#)
VCI [65](#)
VPI [65](#)

W

WAN [63](#)
и LAN [87](#)
WWW
удаленное управление [126](#)

ZA

temperature [297](#)
www.dyndns.org [121](#)

