

Модем ADSL2+ с портом Ethernet

Руководство
пользователя

Модель P-660RT EE

The logo for ZyXEL, featuring the brand name in a bold, italicized, sans-serif font. The letters are white and set against a dark gray background that has a subtle geometric pattern of overlapping triangles.

Интернет-
техника
для дома

series
òmni

Важная информация

Юридический адрес изготовителя

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

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

© ZyXEL, 2005. Все права защищены.

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

Оглавление

Важная информация	2
Оглавление	3
Перечень рисунков	13
Перечень таблиц	18
Предисловие	21
Введение в DSL	23
Глава 1	
Знакомство с P-660RT	24
1.1 Знакомство с P-660RT	24
1.1.1 Функции модема	24
1.1.2 Применение модема	29
1.1.2.1 Доступ в Интернет	29
1.1.2.2 Организация соединения между локальными сетями	30
1.1.3 Установка и подключение оборудования	30
1.1.4 Светодиоды на передней панели	30
Глава 2	
Знакомство с Web-конфигуратором	32
2.1 Описание Web-конфигуратора	32
2.1.1 Доступ к Web-конфигуратору модема	32
2.1.2 Сброс модема к заводским установкам	33
2.1.2.1 Использование кнопки сброса к заводским установкам	33
2.1.3 Интерфейс Web-конфигуратора модема	34
Глава 3	
Мастер установки	36
3.1 Введение	36
3.1.1 Инкапсуляция	36
3.1.1.1 ENET ENCAP	36
3.1.1.2 PPP over Ethernet (протокол "точка-точка" поверх Ethernet)	36
3.1.1.3 PPPoA (протокол "точка-точка" поверх ATM)	37
3.1.1.4 RFC 1483	37

3.1.2 Мультиплексирование	37
3.1.2.1 Мультиплексирование на базе VC	37
3.1.2.2 Мультиплексирование на базе LLC	37
3.1.3 VPI и VCI	38
3.1.4 Мастер установки доступа в Интернет: Первое окно	38
3.2 IP-адрес и маска подсети	39
3.2.1 Назначение IP-адреса	40
3.2.1.1 Назначение IP с инкапсуляцией PPPoA или PPPoE	40
3.2.1.2 Назначение IP с инкапсуляцией RFC 1483	40
3.2.1.3 Назначение IP с инкапсуляцией ENET ENCAP	40
3.2.1.4 IP-адреса для частных сетей	40
3.2.2 Постоянное соединение (PPP)	41
3.2.3 NAT	41
3.2.4 Мастер установки доступа в Интернет: Второе окно	41
3.2.5 Настройка DHCP	46
3.2.5.1 Настройка диапазона IP	46
3.2.6 Мастер установки доступа в Интернет: Третье окно	46
3.2.7 Мастер установки доступа в Интернет: Тестирование соединения	49
3.2.7.1 Проверьте подключение к Интернету	49
Глава 4	
Установка пароля	50
4.1 Введение	50
4.1.1 Изменение пароля	50
Глава 5	
Настройка локальной сети	52
5.1 Обзор локальной сети	52
5.1.1 Локальные, глобальные сети и модем	52
5.2 Адрес сервера DNS	53
5.3 Назначение адреса сервера DNS	53
5.4 Настройка TCP/IP локальной сети	54
5.4.1 Настройки локальной сети, установленные изготовителем по умолчанию	54
5.4.2 IP-адрес и маска подсети	54
5.4.3 Настройка RIP	54
5.4.4 Многоадресная рассылка	55
5.5 Any IP (Любой IP)	56
5.5.1 Как работает функция Any IP (Любой IP)	57
5.6 Настройка локальной сети	57

Глава 6	
Настройка глобальной сети	60
6.1 Обзор глобальной сети	60
6.2 Метрика	60
6.3 Инкапсуляция PPPoE	61
6.4 Формирование трафика	61
6.5 Доступ в Интернет с использованием Zero Configuration (Автоматическая настройка на провайдера)	62
6.6 Настройка подключения к глобальной сети	63
6.7 Перенаправление трафика	67
6.8 Настройка резервного подключения к глобальной сети	68
Глава 7	
Окна NAT (Трансляция сетевых адресов).....	71
7.1 Обзор NAT	71
7.1.1 Определения NAT	71
7.1.2 Назначение NAT	72
7.1.3 Как работает NAT	72
7.1.4 Применение NAT	73
7.1.5 Типы отображения NAT	74
7.2 Сравнение SUA (Учетная запись одиночного пользователя) и NAT	75
7.3 Сервер SUA	76
7.3.1 IP-адрес сервера по умолчанию	76
7.3.2 Переадресация портов: Службы и номера портов	77
7.3.3 Настройка серверов, расположенных за SUA (Пример)	77
7.4 Выбор режима NAT	78
7.5 Настройка сервера SUA	79
7.6 Настройка правил отображения адресов	81
7.7 Редактирование правил отображения адресов	82
Глава 8	
Настройка динамической DNS	85
8.1 Динамическая система доменных имен	85
8.1.1 Шаблоны DYNDNS	85
8.2 Настройка динамической DNS	85
Глава 9	
Время и дата	87
9.1 Установка времени и даты	87
Глава 10	
Настройка удаленного управления.....	90
10.1 Обзор удаленного управления	90

10.1.1 Ограничения на удаленное управление	90
10.1.2 Удаленное управление и NAT	91
10.1.3 Время бездействия системы	91
10.2 Управление с помощью Telnet	91
10.3 FTP	91
10.4 Web	92
10.5 Настройка удаленного управления	92
Глава 11	
Универсальная функция Plug and Play (UPnP)	93
11.1 Описание универсальной функции Plug and Play	93
11.1.1 Как узнать, используется ли UPnP?	93
11.1.2 NAT Transversal	93
11.1.3 Предупреждения по использованию UPnP	94
11.2 UPnP и ZyXEL	94
11.2.1 Настройка UPnP	94
11.3 Пример установки UPnP в Windows	95
11.4 Пример использования UPnP в Windows XP	99
Глава 12	
Сопровождение	107
12.1 Описание обслуживания	107
12.2 Окно Состояние системы	107
12.2.1 Статистика системы	109
12.3 Окно Таблица DHCP	111
12.4 Окно Таблица Any IP	112
12.5 Окна диагностики	113
12.5.1 Окно общей диагностики	113
12.5.2 Окно диагностики DSL линии	114
12.6 Окно микропрограммы	116
Глава 13	
Знакомство с SMT	119
13.1 Описание SMT	119
13.1.1 Процедура настройки при помощи SMT через соединение Telnet ..	119
13.1.2 Ввод пароля	119
13.1.3 Обзор меню SMT модема	120
13.2 Работа с интерфейсом SMT	120
13.2.1 Описание интерфейса SMT	122
13.3 Изменение системного пароля	123

Глава 14	
Меню 1 - Настройка общих параметров	124
14.1 Настройка общих параметров	124
14.2 Процедура настройки в Меню 1	124
14.2.1 Процедура настройки динамической DNS	126
Глава 15	
Меню 2 - Настройка резервного подключения к глобальной сети.....	128
15.1 Описание настройки резервного подключения к глобальной сети	128
15.2 Настройка резервного подключения в Меню 2	128
15.2.1 Настройка перенаправления трафика	129
Глава 16	
Меню 3 - Настройка локальной сети.....	131
16.1 Настройка локальной сети	131
16.1.1 Общая настройка сети Ethernet	131
16.2 Настройка Ethernet в зависимости от используемого протокола	132
16.3 Настройка Ethernet с TCP/IP и DHCP	132
Глава 17	
Доступ в Интернет.....	135
17.1 Описание доступа в Интернет	135
17.2 Стратегии IP	135
17.3 Псевдоним IP	135
17.4 Создание псевдонимов IP	136
17.5 Настройка маршрута IP	138
17.6 Настройка доступа в Интернет	138
Глава 18	
Настройка удаленного узла.....	141
18.1 Описание настройки удаленного узла	141
18.2 Настройка удаленного узла	141
18.2.1 Профиль удаленного узла	141
18.2.2 Сценарии инкапсуляции и мультиплексирования	142
18.2.2.1 Сценарий 1: Один виртуальный канал, несколько протоколов ...	142
18.2.2.2 Сценарий 2: Один виртуальный канал, один протокол (IP) ...	142
18.2.2.3 Сценарий 3: Несколько виртуальных каналов	142
18.2.3 Протокол аутентификации исходящих вызовов	145
18.3 Параметры сетевого уровня удаленного узла	145
18.3.1 IP-адреса в поле My WAN Addr (Мой адрес в глобальной сети)	147
18.4 Фильтр удаленного узла	148
18.4.1 Правила фильтров безопасности Интернет в Web-конфигураторе	149

18.4.2	Наборы фильтров Web-конфигуратора	150
18.5	Редактирование параметров уровня ATM	152
18.5.1	Мультиплексирование на базе VC (не-PPP инкапсуляция)	152
18.5.2	Мультиплексирование на базе LLC или инкапсуляция PPP	153
18.5.3	Параметры дополнительной настройки	153
Глава 19		
Настройка статических маршрутов.....		156
19.1	Описание статических маршрутов IP	156
19.2	Настройка	156
Глава 20		
Настройка межсетевого моста		159
20.1	Общие сведения о межсетевом мосте	159
20.2	Настройка Ethernet для организации моста	159
20.2.1	Настройка межсетевого моста для удаленного узла	159
20.2.2	Создание статического маршрута для межсетевого моста	161
Глава 21		
Трансляция сетевых адресов (NAT).....		163
21.1	Сравнение SUA (Учетная запись одиночного пользователя) и NAT	163
21.2	Применение NAT	163
21.3	Настройка NAT	165
21.3.1	Наборы отображения адресов	165
21.3.1.1	Набор отображения адресов SUA	166
21.3.1.2	Наборы отображения адресов, определяемые пользователем ..	167
21.3.1.3	Порядок применения правил	168
21.4	Настройка сервера, расположенного за NAT	171
21.5	Примеры применения NAT	172
21.5.1	Пример 1: Только доступ в Интернет	173
21.5.2	Пример 2: Доступ в Интернет с внутренним сервером	174
21.5.3	Пример 3: Несколько общедоступных IP-адресов для внутренних серверов	174
21.5.4	Пример 4: Прикладные программы, не поддерживающие NAT	178
Глава 22		
Настройка фильтров.....		180
22.1	О фильтрации	180
22.1.1	Структура фильтра модема	183
22.2	Настройка набора фильтров для модема	183
22.3	Сводное меню правил фильтра	184
22.4	Настройка правила фильтра	185

22.4.1	Правило фильтра TCP/IP	186
22.4.2	Правило общего фильтра	189
22.5	Типы фильтров и NAT	191
22.6	Пример фильтра	192
22.7	Применение фильтров и заводских настроек по умолчанию	194
22.7.1	Трафик Ethernet	194
22.7.2	Фильтры для удаленного узла	195
Глава 23		
	Настройка SNMP	196
23.1	О протоколе SNMP	196
23.2	Поддерживаемые базы управляющей информации	197
23.3	Настройка SNMP	197
23.4	Прерывания SNMP	199
Глава 24		
	Информация о системе и диагностика	200
24.1	Обзор	200
24.2	Состояние системы	200
24.3	Информация о системе	202
24.3.1	Информация о системе	203
24.3.2	Скорость консольного порта	205
24.4	Журнал регистрации и трассировка	205
24.4.1	Просмотр журнала регистрации ошибок	205
24.4.2	Системный журнал и учет ресурсов	206
24.5	Диагностика	209
Глава 25		
	Сопровождение файлов конфигурации и микропрограммы.....	211
25.1	Структура имен файлов	211
25.2	Резервное копирование конфигурации	212
25.2.1	Резервное копирование конфигурации	212
25.2.2	Использование команд FTP в командной строке	213
25.2.3	Пример использования команд FTP в командной строке	213
25.2.4	Клиенты FTP на основе GUI	214
25.2.5	Ограничения на управление с помощью TFTP и FTP по глобальной сети	214
25.2.6	Резервное копирование конфигурации с помощью TFTP	215
25.2.7	Пример команды TFTP	215
25.2.8	Клиенты TFTP на основе GUI	216
25.3	Восстановление конфигурации	216
25.3.1	Восстановление конфигурации с помощью FTP	217
25.3.2	Пример восстановления конфигурации с помощью сеанса FTP	218

25.4	Загрузка файлов конфигурации и микропрограммы	218
25.4.1	Загрузка микропрограммы	218
25.4.2	Загрузка файла конфигурации	219
25.4.3	Пример загрузки файлов с помощью сеанса FTP из командной строки DOS	220
25.4.4	Пример загрузки микропрограммы с помощью сеанса FTP	220
25.4.5	Загрузка файлов с помощью TFTP	221
25.4.6	Пример команды для загрузки файла с помощью сеанса TFTP	221
Глава 26		
Сопровождение системы.....		222
26.1	Режим интерпретатора команд	222
26.2	Контроль вызовов	223
26.2.1	Управление бюджетом	223
26.3	Установка времени и даты	225
26.3.1	Обновление времени	227
Глава 27		
Удаленное управление		228
27.1	Описание удаленного управления	228
27.2	Удаленное управление	228
27.2.1	Настройка удаленного управления	228
27.2.2	Ограничения на удаленное управление	229
27.3	Удаленное управление и NAT	230
27.4	Время бездействия системы	230
Глава 28		
Маршрутизация на базе стратегии IP		231
28.1	Описание маршрутизации на базе стратегии IP (IP Policy Routing)	231
28.2	Преимущества маршрутизации на базе стратегии IP	231
28.3	Стратегия маршрутизации	232
28.4	Настройка стратегий маршрутизации IP	232
28.5	Применение стратегии IP	236
28.5.1	Стратегии IP для Ethernet	236
28.6	Пример маршрутизации на базе стратегии IP	237
Глава 29		
Расписание вызовов		241
29.1	Введение	241
Глава 30		
Поиск и устранение неисправностей.....		245
30.1	Неисправности при запуске модема	245

30.2 Неисправность светодиода LAN	245
30.3 Неисправность светодиода DSL	246
30.4 Неисправность интерфейса LAN	246
30.5 Неисправность интерфейса WAN	246
30.6 Неисправность при доступе в Интернет	247
30.7 Неисправности, связанные с паролем	247
30.8 Неисправности, связанные с Web-конфигуратором	248
30.9 Неисправности при удаленном управлении	248
Приложение А	
Сплиттеры и микрофильтры	249
Подключение телефонного сплиттера.....	249
Телефонные микрофильтры.....	250
Использование модема с ISDN	250
Приложение В	
Установка IP-адреса компьютера.....	252
Windows 95/98/Me.....	252
Установка компонент	253
Настройка	254
Проверка конфигурации	255
Windows 2000/NT/XP	256
Проверка конфигурации	260
Macintosh OS 8/9.....	260
Проверка конфигурации	262
Macintosh OS X	262
Проверка конфигурации	264
Приложение С	
Организация подсетей IP	265
Адресация IP	265
Классы IP	265
Маска подсети	266
Организация подсетей	267
Пример: Две подсети.....	268
Пример: Четыре подсети	269
Пример: Восемь подсетей	271
Организация подсетей в сетях класса А и класса В.....	272
Приложение D	
PPPoE	273
PPPoE в действии	273

Преимущества PPPoE	273
Традиционный сценарий доступа по коммутируемой линии	273
Как работает PPPoE	274
Модем в качестве клиента PPPoE	274
Приложение E	
Топология виртуальной цепи	276
Приложение F	
Интерпретатор команд	277
Синтаксис команд	277
Использование команд	277
Приложение G	
Описание регистрационных журналов	278

Перечень рисунков

Рис. 1 Применение модема для организации доступа в Интернет	29
Рис. 2 Организация соединения между локальными сетями	30
Рис. 3 Окно ввода пароля	32
Рис. 4 Изменение пароля при входе	33
Рис. 5 Web-конфигуратор: Окно Site Map (Карта сайта)	34
Рис. 6 Мастер установки доступа в Интернет: Первое окно	38
Рис. 7 Подключение к Интернету по PPPoE	42
Рис. 8 Подключение к Интернету по RFC 1483	43
Рис. 9 Подключение к Интернету с использованием ENET ENCAP	44
Рис. 10 Подключение к Интернету с использованием PPPoA	45
Рис. 11 Мастер установки доступа в Интернет: Третье окно	47
Рис. 12 Мастер установки доступа в Интернет: Конфигурация локальной сети	48
Рис. 13 Мастер установки доступа в Интернет: Тестирование соединения	49
Рис. 14 Пароль	50
Рис. 15 Локальные и глобальные IP-адреса	52
Рис. 16 Пример: Any IP	56
Рис. 17 Настройка локальной сети	58
Рис. 18 Пример формирования трафика	62
Рис. 19 Настройка подключения к глобальной сети (PPPoE)	64
Рис. 20 Пример перенаправления трафика	67
Рис. 21 Настройка локальной сети для перенаправления трафика	68
Рис. 22 Резервное подключение к глобальной сети	69
Рис. 23 Как работает NAT	73
Рис. 24 Применение NAT с использованием псевдонимов IP	74
Рис. 25 Пример: Несколько серверов расположены за NAT	78
Рис. 26 Режим NAT	78
Рис. 27 Редактировать набор серверов SUA/NAT	80
Рис. 28 Правила отображения адресов	81
Рис. 29 Редактирование правил отображения адресов	83
Рис. 30 Динамическая система доменных имен (Dynamic DNS)	86
Рис. 31 Время и дата	87
Рис. 32 Настройка Telnet в сети TCP/IP	91
Рис. 33 Удаленное управление	92
Рис. 34 Настройка UPnP	95
Рис. 35 Установка и удаление программ: Установка Windows: Связь	96
Рис. 36 Установка и удаление программ: Установка Windows: Связь: Компоненты	96

Рис. 37 Сетевые подключения	97
Рис. 38 Мастер установки дополнительных компонентов Windows	98
Рис. 39 Сетевые службы	99
Рис. 40 Сетевые подключения	100
Рис. 41 Свойства подключения к Интернет	101
Рис. 42 Свойства подключения к Интернет: Дополнительные настройки	102
Рис. 43 Свойства подключения к Интернет: Дополнительные настройки: Добавить ..	102
Рис. 44 Значок в системной панели	103
Рис. 45 Состояние подключения к Интернет	103
Рис. 46 Сетевые подключения	104
Рис. 47 Сетевые подключения: Мое сетевое окружение	105
Рис. 48 Сетевые подключения: Мое сетевое окружение: Свойства: Пример	106
Рис. 49 Состояние системы	108
Рис. 50 Состояние системы: Показать статистику	110
Рис. 51 Таблица DHCP	112
Рис. 52 Таблица Any IP (Любой IP)	113
Рис. 53 Диагностика: Общая	114
Рис. 54 Диагностика: DSL линия	115
Рис. 55 Обновление микропрограммы	117
Рис. 56 Временное отключение сети	118
Рис. 57 Сообщение об ошибке	118
Рис. 58 Окно регистрации	120
Рис. 59 Обзор меню SMT модема	120
Рис. 60 Меню 23 - Изменение пароля	123
Рис. 61 Меню 1 - Настройка общих параметров	125
Рис. 62 Меню 1.1 - Настройка динамической DNS	126
Рис. 63 Меню 2 - Настройка резервного подключения к глобальной сети	128
Рис. 64 Меню 2.1 - Настройка перенаправления трафика	130
Рис. 65 Меню 3 - Настройка локальной сети	131
Рис. 66 Меню 3.1 - Настройка фильтра порта LAN	132
Рис. 67 Меню 3.2 - Настройка Ethernet с TCP/IP и DHCP	133
Рис. 68 Пример сети с использованием псевдонимов IP	136
Рис. 69 Меню 3.2 - Настройка TCP/IP и DHCP	136
Рис. 70 Меню 3.2.1 - Настройка псевдонима IP	137
Рис. 71 Меню 1 - Настройка общих параметров	138
Рис. 72 Меню 4 - Настройка доступа в Интернет	139
Рис. 73 Меню 11 - Настройка удаленного узла	142
Рис. 74 Меню 11.1 - Профиль удаленного узла	143
Рис. 75 Меню 11.3 - Параметры сетевого уровня удаленного узла	146
Рис. 76 Пример IP-адресов для соединения локальных сетей на базе TCP/IP	148
Рис. 77 Меню 11.5 - Фильтр удаленного узла (инкапсуляция RFC 1483 или ENET)	148
Рис. 78 Меню 11.5 - Фильтр удаленного узла (инкапсуляция RFC или ENET)	149
Рис. 79 Безопасность при работе в Интернет	150

Рис. 80 Меню 21 - Создание наборов фильтров	151
Рис. 81 Меню 21.11 - Набор Web 11	151
Рис. 82 Меню 21.12 - Набор Web 12	152
Рис. 83 Меню 11.6 - Мультиплексирование на базе VC	153
Рис. 84 Меню 11.6 - Мультиплексирование на базе LLC или инкапсуляция PPP	153
Рис. 85 Меню 11.1- Профиль удаленного узла	154
Рис. 86 Меню 11.8 - Параметры дополнительной настройки	155
Рис. 87 Пример топологии статической маршрутизации	156
Рис. 88 Меню 12 - Настройка статического маршрута	157
Рис. 89 Меню 12.1 - Настройка статического маршрута IP	157
Рис. 90 Меню 12.1.1 - Редактирование статического маршрута IP	157
Рис. 91 Меню 11.1 - Профиль удаленного узла	160
Рис. 92 Меню 11.3 - Параметры сетевого уровня удаленного узла	160
Рис. 93 Меню 12.3.1 - Редактировать статический маршрут для моста	161
Рис. 94 Меню 4 - Применение NAT для доступа в Интернет	164
Рис. 95 Применение NAT в Меню 4 и Меню 11.3	164
Рис. 96 Меню 15 - Настройка NAT	165
Рис. 97 Меню 15.1 - Наборы отображения адресов	166
Рис. 98 Меню 15.1.255 - Правила отображения адресов SUA	166
Рис. 99 Меню 15.1.1 - Первый набор	168
Рис. 100 Меню 15.1.1.1 - Редактирование/Создание конкретного правила в наборе ..	170
Рис. 101 Меню 15.2 - Наборы серверов за NAT	171
Рис. 102 Меню 15.2.1 - Настройка серверов за NAT	172
Рис. 103 Пример: Несколько серверов расположены за NAT	172
Рис. 104 Пример применения NAT 1	173
Рис. 105 Меню 4 - Пример доступа в Интернет при использовании NAT	173
Рис. 106 Пример применения NAT 2	174
Рис. 107 Меню 15.2.1 - Определение внутреннего сервера	174
Рис. 108 Пример применения NAT 3	175
Рис. 109 Пример 3: Меню 11.3	176
Рис. 110 Пример 3: Меню 15.1.1.1	177
Рис. 111 Пример 3: Окончательный вид Меню 15.1.1	177
Рис. 112 Пример 3: Меню 15.2.1	178
Рис. 113 Пример применения NAT 4	178
Рис. 114 Пример 4: Меню 15.1.1.1 - Правило отображения адресов	179
Рис. 115 Пример 4: Меню 15.1.1 - Правила отображения адресов	179
Рис. 116 Процесс фильтрации исходящего пакета	181
Рис. 117 Процесс реализации правил фильтра	182
Рис. 118 Меню 21 - Настройка наборов фильтров	183
Рис. 119 Сводка правил фильтра NetBIOS_WAN	184
Рис. 120 Сводка правил фильтра NetBIOS_LAN	184
Рис. 121 Меню 21.x.1 - Правило фильтра TCP/IP	187
Рис. 122 Применение фильтра IP	189

Рис. 123 Меню 21.5.1 - Правило общего фильтра	190
Рис. 124 Наборы фильтров протоколов и фильтров устройств	192
Рис. 125 Пример фильтра Telnet	192
Рис. 126 Меню 21.6.1 - Пример фильтра	193
Рис. 127 Меню 21.6.1 - Сводка правил фильтра, созданного в примере	193
Рис. 128 Фильтрация трафика Ethernet	195
Рис. 129 Фильтрация трафика удаленного узла	195
Рис. 130 Модель управления SNMP	196
Рис. 131 Меню 22 - Настройка SNMP	198
Рис. 132 Меню 24 - Сопровождение системы	200
Рис. 133 Меню 24.1 - Сопровождение системы: Состояние	201
Рис. 134 Меню 24.2 - Информация о системе и скорость консольного порта	203
Рис. 135 Меню 24.2.1 - Сопровождение системы: Информация	204
Рис. 136 Меню 24.2.2 - Сопровождение системы: Изменение скорости консольного порта 205	
Рис. 137 Меню 24.3 - Сопровождение системы: Журнал регистрации и трассировка	205
Рис. 138 Пример сообщений об ошибках и уведомлениях	206
Рис. 139 Меню 24.3.2 - Сопровождение системы: Системный журнал и учет ресурсов 207	
Рис. 140 Пример системного журнала	208
Рис. 141 Меню 24.4 - Сопровождение системы: Диагностика	210
Рис. 142 Сеанс Telnet в Меню 24.5	213
Рис. 143 Пример сеанса FTP	214
Рис. 144 Установка соединения Telnet в Меню 24.6	217
Рис. 145 Пример восстановления конфигурации с помощью сеанса FTP	218
Рис. 146 Подключение Telnet в Menu 24.7.1 - Загрузка системной микропрограммы	219
Рис. 147 Подключение с помощью Telnet в Меню 24.7.2 - Сопровождение системы	219
Рис. 148 Пример загрузки микропрограммы с помощью сеанса FTP	220
Рис. 149 Командный режим в Меню 24	222
Рис. 150 Доступные команды	223
Рис. 151 Меню 24.9 - Сопровождение системы: Контроль вызовов	223
Рис. 152 Меню 24.9.1 - Сопровождение системы: Управление бюджетом	224
Рис. 153 Меню 24 - Сопровождение системы	225
Рис. 154 Меню 24.10 - Сопровождение системы: Установка времени и даты	226
Рис. 155 Меню 24.11 - Контроль удаленного управления	229
Рис. 156 Меню 25 - Настройка стратегий маршрутизации IP	232
Рис. 157 Меню 25.1 - Настройка стратегий маршрутизации IP	233
Рис. 158 Меню 25.1.1 - Стратегия маршрутизации IP	234
Рис. 159 Меню 3.2 - Настройка TCP/IP и DHCP для Ethernet	236
Рис. 160 Меню 11.3 - Параметры сетевого уровня удаленного узла	237
Рис. 161 Пример маршрутизации на базе стратегии IP	238
Рис. 162 Маршрутизация на базе стратегии IP. Пример 1	238
Рис. 163 Маршрутизация на базе стратегии IP. Пример 2	239

Рис. 164 Пример применения стратегий IP	240
Рис. 165 Меню 26 - Создание расписания	241
Рис. 166 Меню 26.1 - создание набора расписания	242
Рис. 167 Применение расписания к удаленному узлу (PPPoE)	244
Рис. 168 Подключение телефонного сплиттера	249
Рис. 169 Подключение микрофильтра	250
Рис. 170 Использование модема с ISDN	251
Рис. 171 Windows 95/98/Me: Сеть: Конфигурация	253
Рис. 172 Windows 95/98/Me: Свойства TCP/IP: IP-адрес	254
Рис. 173 Windows 95/98/Me: Свойства TCP/IP: Конфигурация DNS	255
Рис. 174 Windows XP: Меню Start (Пуск)	256
Рис. 175 Windows XP: Панель управления	256
Рис. 176 Windows XP: Панель управления: Сетевые подключения: Свойства	257
Рис. 177 Windows XP: Свойства подключения по локальной сети	257
Рис. 178 Windows XP: Дополнительные параметры TCP/IP	258
Рис. 179 Windows XP: Свойства: Протокол Интернета (TCP/IP)	260
Рис. 180 Macintosh OS 8/9: Меню Apple	261
Рис. 181 Macintosh OS 8/9: TCP/IP	262
Рис. 182 Macintosh OS X: Меню Apple	263
Рис. 183 Macintosh OS X: Сеть	263
Рис. 184 Конфигурация оборудования "один маршрутизатор для одного компьютера" 274	
Рис. 185 Модем в качестве клиента PPPoE	275
Рис. 186 Топология виртуальной цепи	276

Перечень таблиц

Табл. 1 Стандарты ADSL	24
Табл. 2 Описание светодиодов передней панели	30
Табл. 3 Сводная таблица окон Web-конфигуратора	34
Табл. 4 Мастер установки доступа в Интернет: Первое окно	38
Табл. 5 Подключение к Интернету с использованием PPPoE	42
Табл. 6 Подключение к Интернету с использованием RFC 1483	43
Табл. 7 Подключение к Интернету с использованием ENET ENCAP	44
Табл. 8 Подключение к Интернету с использованием PPPoA	45
Табл. 9 Мастер установки доступа в Интернет: Конфигурация локальной сети	48
Табл. 10 Пароль	50
Табл. 11 LAN Setup	58
Табл. 12 Настройка подключения к глобальной сети	64
Табл. 13 Резервное подключение к глобальной сети	69
Табл. 14 Определения NAT	71
Табл. 15 Типы отображения NAT	75
Табл. 16 Службы и номера портов	77
Табл. 17 Режим NAT	78
Табл. 18 Редактировать набор серверов SUA/NAT	80
Табл. 19 Правила отображения адресов	81
Табл. 20 Редактирование правил отображения адресов	83
Табл. 21 Динамическая система доменных имен	86
Табл. 22 Время и дата	88
Табл. 23 Удаленное управление	92
Табл. 24 Настройка UPnP	95
Табл. 25 Состояние системы	108
Табл. 26 Состояние системы: Показать статистику	110
Табл. 27 Таблица DHCP	112
Табл. 28 Таблица Any IP (Любой IP)	113
Табл. 29 Диагностика: Общая	114
Табл. 30 Диагностика: DSL линия	115
Табл. 31 Обновление микропрограммы	117
Табл. 32 Работа с интерфейсом SMT	121
Табл. 33 Главное меню SMT	122
Табл. 34 Сводка Главного меню	122
Табл. 35 Меню 1 - Настройка общих параметров	125
Табл. 36 Меню 1.1 - Настройка динамической DNS	126

Табл. 37 Меню 2 - Настройка резервного подключения к глобальной сети	129
Табл. 38 Меню 2.1 - Настройка перенаправления трафика	130
Табл. 39 Настройка DHCP Ethernet	133
Табл. 40 Настройка TCP/IP порта Ethernet	134
Табл. 41 Меню 3.2.1 - Настройка псевдонима IP	137
Табл. 42 Меню 4 - Настройка доступа в Интернет	139
Табл. 43 Меню 11.1 - Профиль удаленного узла	143
Табл. 44 Меню 11.3 - Параметры сетевого уровня удаленного узла	146
Табл. 45 Меню 11.8 - Параметры дополнительной настройки	155
Табл. 46 Меню 12.1.1 - Редактирование статического маршрута IP	158
Табл. 47 Параметры сетевого уровня удаленного узла: Поля для настройки моста ..	160
Табл. 48 Меню 12.3.1 - Редактировать статический маршрут для моста	161
Табл. 49 Применение NAT в Меню 4 и Меню 11.3	165
Табл. 50 Правила отображения адресов SUA	166
Табл. 51 Меню 15.1.1 - Первый набор	169
Табл. 52 Меню 15.1.1.1 - Редактирование/Создание конкретного правила в наборе ..	170
Табл. 53 Сокращения, используемые в меню Filter Rules Summary (Сводка правил фильтра)	184
Табл. 54 Сокращения, используемые в правилах	185
Табл. 55 Меню 21.x.1 - Правило фильтра TCP/IP	187
Табл. 56 Меню 21.1.5.1 - Правило общего фильтра	190
Табл. 57 Таблица наборов фильтров	194
Табл. 58 Меню 22 - Настройка SNMP	198
Табл. 59 Прерывания SNMP	199
Табл. 60 Порты и постоянные виртуальные каналы	199
Табл. 61 Меню 24.1 - Сопровождение системы: Состояние	201
Табл. 62 Меню 24.2.1 - Сопровождение системы: Информация	204
Табл. 63 Меню 24.3.2 - Сопровождение системы: Системный журнал и учет ресурсов 207	
Табл. 64 Меню 24.4 - Сопровождение системы: Диагностика	210
Табл. 65 Структура имен файлов	212
Табл. 66 Основные команды для клиентов FTP на основе GUI	214
Табл. 67 Основные команды клиентов TFTP на основе GUI	216
Табл. 68 Меню 24.9.1 - Сопровождение системы: Управление бюджетом	224
Табл. 69 Меню 24.10 - Сопровождение системы: Установка времени и даты	226
Табл. 70 Меню 24.11 - Контроль удаленного управления	229
Табл. 71 Меню 25.1 - Настройка стратегии маршрутизации IP	233
Табл. 72 Меню 25.1.1 - Стратегия маршрутизации IP	234
Табл. 73 Меню 26.1 - Создание расписания	242
Табл. 74 Поиск и устранение неисправностей при запуске модема	245
Табл. 75 Устранение неисправностей светодиода LAN	245
Табл. 76 Устранение неисправностей светодиода DSL	246
Табл. 77 Устранение неисправности интерфейса LAN	246

Табл. 78 Устранение неисправности интерфейса WAN	246
Табл. 79 Устранение неисправностей при доступе в Интернет	247
Табл. 80 Устранение неисправностей, связанных с паролем	247
Табл. 81 Устранение неисправностей, связанных Web-конфигуратором	248
Табл. 82 Устранение неисправностей при удаленном управлении	248
Табл. 83 Классы IP-адресов	265
Табл. 84 Допустимые диапазоны IP-адресов для каждого класса	266
Табл. 85 “Естественные” маски	266
Табл. 86 Альтернативные варианты записи маски подсети	267
Табл. 87 Пример организации 2-х подсетей	268
Табл. 88 Подсеть 1	268
Табл. 89 Подсеть 2	269
Табл. 90 Подсеть 1	269
Табл. 91 Подсеть 2	270
Табл. 92 Подсеть 3	270
Табл. 93 Подсеть 4	270
Табл. 94 Восемь подсетей	271
Табл. 95 Организация подсетей класса С	271
Табл. 96 Организация подсетей класса В	272
Табл. 97 Сообщения по обслуживанию системы	278
Табл. 98 Записи системных ошибок	279
Табл. 99 Записи фильтра пакетов	279
Табл. 100 Записи ICMP	279
Табл. 101 Записи CDR	280
Табл. 102 Записи PPP	280
Табл. 103 Записи ICMP	280
Табл. 104 Записи системного журнала	282
Табл. 105 Типы данных сообщений RFC-2408 ISAKMP	282

Предисловие

Поздравляем с приобретением устройства P-660RT EE Модем ADSL2+ с портом Ethernet.



ПРИМЕЧАНИЕ: Зарегистрируйте ваше устройство в режиме он-лайн, чтобы иметь возможность получать по электронной почте извещения о последних обновлениях микропрограммы на сайте www.zyxel.ru.

Устройство легко устанавливается и настраивается.

О данном Руководстве пользователя

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



ПРИМЕЧАНИЕ: Для настройки модема используются Web-конфигуратор, SMT (System Management Terminal - системная консоль) и интерфейс интерпретатора команд. Не все интерфейсы обеспечивают настройку всех функций устройства.

Условные обозначения

- “Введите” означает, что Вам следует напечатать один или более символов. “Выберите” означает, что Вам следует использовать одну из стандартных опций.
- Заголовки и надписи меню SMT выполнены **полужирным шрифтом Times New Roman**. Стандартные пункты меню выполнены **полужирным шрифтом Arial**. Названия команд и клавиш со стрелками заключаются в квадратные скобки. [ENTER] обозначает клавишу "Enter" или клавишу возврата каретки. [ESC] обозначает клавишу "Escape", а [Space Bar] обозначает клавишу пробела.
- Действия в последовательности операций, выполняемых с помощью мыши, разделяются запятой. Например, “щелкните иконку Apple, **Control Panels (Панель Управления)** и затем **Modem (Модем)**” означает, что сначала нужно щелкнуть по иконке Apple, затем перевести указатель мыши на **Control Panels (Контрольная панель)** и затем щелкнуть **Modem (Модем)**.
- Для краткости в данном руководстве будет использоваться "например" вместо "например" и "т.е." вместо "то есть" и "другими словами".
- В данном руководстве устройство серии P-660RT EE может обозначаться как P-660RT.

Сопроводительная документация

- Справочный компакт-диск

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

- Краткое руководство

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

- Встроенная справка Web-конфигуратора

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

- Web-сайт корпорации ZyXEL

Для получения дополнительной документации обратитесь на сайт www.zyxel.ru.

Обратная связь с пользователем

Помогите нам помочь вам. Все комментарии, относящиеся к руководству пользователя, вопросы и предложения по улучшению отправляйте электронной почтой по адресу techwriters@zyxel.com.tw или отправляйте обычной почтой в отдел технической документации (Technical Writing Team) по адресу ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Спасибо.

Пояснения к графическим пиктограммам

Модем 	Компьютер 	Ноутбук 
Сервер 	DSL-коммутатор (DSLAM) 	Телефон 
Маршрутизатор 	Коммутатор 	

Введение в DSL

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

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

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

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

Введение в ADSL

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

ГЛАВА 1

Знакомство с P-660RT EE

В этой главе описываются основные функции и варианты применения модема.

1.1 Знакомство с P-660RT EE

P-660RT EE идеально подходит для высокоскоростного доступа в Интернет, а также организации соединения между локальными и удаленными сетями. Этот модем может работать в режиме моста или маршрутизатора. В модеме интегрированы функции высокоскоростного интерфейса 10/100 Мбит/с с автоматическим определением типа и скорости подключения по локальной сети и высокоскоростного ADSL порта, совместимого со стандартами ADSL/ADSL2/ADSL2+. Максимальные скорости передачи, достигаемые P-660RT EE для каждого стандарта, представлены в следующей таблице.

Табл. 1 Стандарты ADSL

СТАНДАРТ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ	ПЕРЕДАЧА ДАННЫХ	ПРИЕМ ДАННЫХ
ADSL	832 Kbps	8 Мбит/с
ADSL2	3,5 Мбит/с	12 Мбит/с
ADSL2+	3,5 Мбит/с	24 Мбит/с



ПРИМЕЧАНИЕ: Стандарт, который поддерживает ваш Интернет-провайдер, определяет максимальную скорость исходящего и входящего потока данных. Фактические скорости передачи будут зависеть от расстояния до вашего Интернет-провайдера, качества линии, тарифа и т.д.

Использование в P-660RT EE технологий DSL и NAT обеспечивает простоту установки и организации доступа в Интернет. При подключении через порт Ethernet, компьютеры смогут совместно использовать локальные ресурсы (такие как принтеры и файлы), а также одновременно иметь доступ в Интернет.

Графический интерфейс пользователя (GUI) на основе технологии Web-браузера обеспечивает простое управление устройством.

1.1.1 Функции модема

В следующих разделах описываются функции модема.

Высокоскоростной доступ в Интернет

Модем P-660RT EE поддерживает стандарты ADSL/ADSL2/ADSL2+ со скоростью приема данных до 24 Мбит/с и скорость передачи данных до 3,5 Мбит/с. Фактически достижимые скорости зависят от условий работы оборудования Интернет-провайдера.

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

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

Any IP (Любой IP)

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

Перенаправление трафика

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

Универсальная функция "Plug and Play" (UPnP)

При помощи стандартного протокола TCP/IP модем и другие устройства с поддержкой функции UPnP могут динамически подключаться к сети, получать IP-адрес и предоставлять свои ресурсы другим устройствам в сети.

Поддержка PPPoE (RFC2516)

PPPoE (Протокол "точка-точка" поверх Ethernet) эмулирует коммутируемое соединение. Он позволяет Интернет-провайдеру использовать существующую конфигурацию сети совместно с новейшими широкополосными технологиями, такими как ADSL. Драйвер PPPoE в устройстве P-660RT EE является "прозрачным" для компьютеров в локальной сети, которые работают только по Ethernet и не поддерживают протокол PPPoE, что устраняет необходимость настраивать PPPoE клиенты на отдельных компьютерах.

Трансляция сетевых адресов (NAT)

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

Интерфейс Fast Ethernet 10/100 Мбит/с с автоматическим выбором скорости передачи

Функция автоматического выбора скорости передачи позволяет P-660RT EE определять скорость входящего потока данных и производить соответствующую настройку без ручного вмешательства. Эта функция обеспечивает передачу данных со скоростью 10 или 100 Мбит/с в полудуплексном или дуплексном режиме передачи в зависимости от параметров сети Ethernet.

Интерфейс Fast Ethernet 10/100 Мбит/с с автоматическим распознаванием типа кабеля (MDI/MDI-X)

Интерфейс модема автоматически настраиваются либо на перекрестный, либо на прямой тип кабеля витая пара.

Поддержка динамической DNS

Поддержка динамической система доменных имен позволяет иметь постоянное имя для узла с динамическим IP-адресом, что упрощает доступ к этому узлу с любого места в Интернете. Для использования этой услуги необходимо зарегистрироваться у провайдера услуг службы динамической DNS.

Поддержка нескольких PVC (Permanent Virtual Circuit - постоянный виртуальный канал)

Устройство P-660RT EE поддерживает до 8-ми PVC.

Стандарты ADSL

- Полный диапазон скоростей передачи (ANSI T1.413, Issue 2; G.dmt (G.992.1)) с поддержкой скорости линии до 8 Мбит/с для входящего трафика и 832 кбит/с для исходящего трафика.
- Стандарт G.lite (G.992.2) с поддержкой скорости линии до 1,5 Мбит/с для входящего трафика и 512 кбит/с для исходящего трафика.
- Поддержка многорежимного стандарта (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.lite (G992.2)).
- TCP/IP (Протокол управления передачей/Протокол Internet) - протокол сетевого уровня.
- ATM Forum UNI 3.1/4.0 PVC.
- Поддержка до 8-ми PVC (UBR, CBR, VBR).
- Multiple Protocol over AAL5 (RFC 1483).

- PPP over AAL5 (RFC 2364).
- PPP over Ethernet over AAL5 (RFC 2516).
- RFC 1661.
- PPP over PAP (RFC 1334).
- PPP over CHAP (RFC 1994).

Поддержка протоколов

- Поддержка DHCP

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

- Псевдоним IP (IP Alias)

Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей с использованием одного интерфейса Ethernet. P-660RT EE поддерживает три логических интерфейса локальной сети на одном физическом интерфейсе Ethernet, при этом сам модем выступает в качестве шлюза для каждой логической сети.

- Маршрутизация на основе IP политики (IP Policy Routing - IPPR)

Обычно маршрутизация основана только на адресе получателя, и маршрутизатор выбирает самый короткий путь для пересылки пакета. Маршрутизация на базе IP политики (IPPR) обеспечивает механизм замены схемы маршрутизации по умолчанию, и позволяет изменить правила для пересылки пакета на основе стратегии, определяемой сетевым администратором.

- PPP (Point-to-Point Protocol - Протокол "точка-точка") - протокол канального уровня.
- Прозрачная передача (Transparent bridging) для неподдерживаемых протоколов сетевого уровня.
- Протокол RIP I/RIP II (Routing Information Protocol - Протокол обмена информацией о маршрутизации)
- Проxy-сервер IGMP (Internet Group Management Protocol - Протокол управления группами сети Интернет)
- Поддержка протокола ICMP (Internet Control Message Protocol - Протокол межсетевых управляющих сообщений)
- Поддержка ATM QoS (Quality of Service - Качество обслуживания предоставляемых услуг передачи данных)
- Поддержка MIB II (Management Information Base - База управляющей информации) (RFC 1213)

Совместимость с сетями

Устройство P-660RT EE совместимо с DSL-коммутаторами, использующими ADSL, большинства провайдеров, что максимально упрощает его настройку.

Мультиплексирование

Модем поддерживает мультиплексирование на базе VC и LLC.

Инкапсуляция

Модем поддерживает протокол PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), инкапсуляцию RFC 1483 поверх ATM, маршрутизацию с инкапсуляцией MAC (инкапсуляция ENET), а также PPP over Ethernet (RFC 2516).

Управление сетью

- Управление с помощью команд меню SMT (System Management Terminal - Системная консоль)
- Встроенный Web-конфигуратор
- CLI (Command Line Interpreter - Интерпретатор командной строки)
- Удаленное управление по протоколу Telnet или Web
- Управление по протоколу SNMP
- Сервер/Клиент/Ретранслятор DHCP
- Встроенные средства диагностики
- Системный журнал
- Поддержка протокола Telnet (защищенный паролем доступ по протоколу telnet к внутреннему конфигуратору)
- Сервер TFTP/FTP, поддержка обновления микропрограммы и резервное копирование/восстановление конфигурации
- Поддержка теста обратная петля OAM F4/F5, ячеек OAM AIS и RDI

Другие функции PPPoE

- Время неактивности PPPoE
- Установление PPPoE соединения по требованию

Возможности диагностики

Модем выполняет тесты самодиагностики. Эти тесты проверяют работоспособность следующих схем:

- Флэш-память
- Блок ADSL
- ОЗУ
- Порт локальной сети

Фильтры пакетов

Функции фильтрации пакетов P-660RT EE обеспечивают дополнительные возможности защиты и управления сетью.

Простота установки

Устройство P-660RT EE спроектировано с целью обеспечить быструю, интуитивно понятную и простую установку.

Корпус

Компактный, не требующий принудительной вентиляции корпус модема занимает мало места и легко помещается в любом месте. Предусмотрена возможность разместить его на столе или повесить на стену.

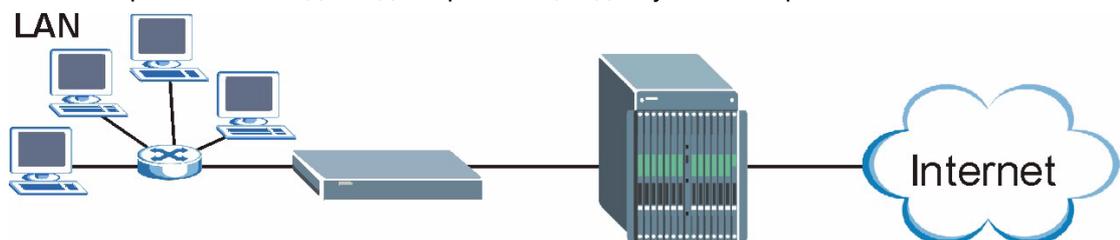
1.1.2 Применение модема

Далее приведено несколько примеров наиболее подходящего применения устройства P-660RT EE.

1.1.2.1 Доступ в Интернет

P-660RT EE является идеальным решением для высокоскоростного доступа в Интернет. Модем поддерживает протокол TCP/IP, повсеместно используемый в Интернет. Устройство совместимо с DSL-коммутаторами, использующими ADSL, большинства провайдеров. DSL-коммутатор представляет собой стойку с установленными линейными DSL-картами, данные с которых мультиплексируются в магистральный сетевой интерфейс/соединение (например, T1, OC3, DS3, ATM или Frame Relay). Его можно представить как стойку из DSL модемов. Типичная схема применения для доступа в Интернет показана на рисунке ниже.

Рис. 1 Применение модема для организации доступа в Интернет



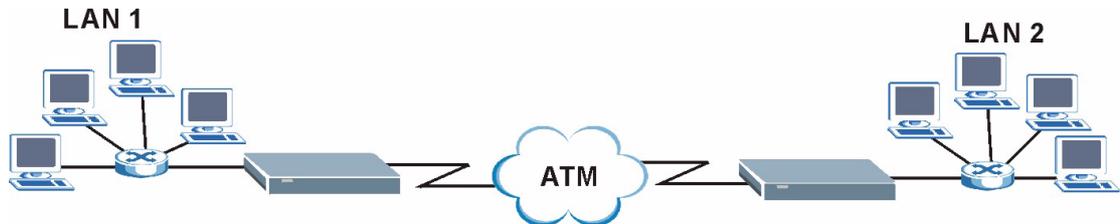
Учетная запись одиночного пользователя для доступа в Интернет

Для домашнего или офисного применения в модем встроена функция SUA (Single User Account - Учетная запись одиночного пользователя), что позволяет нескольким пользователям локальной сети иметь одновременный доступ в Интернет с использованием одного IP-адреса от провайдера и за ту же цену.

1.1.2.2 Организация соединения между локальными сетями

Модем можно использовать для соединения двух географически разнесенных сетей по ADSL линиям. Типичное применение модема для связи локальных сетей отображено ниже.

Рис. 2 Организация соединения между локальными сетями



1.1.3 Установка и подключение оборудования

Для выполнения установки и подключения оборудования см. *Краткое руководство*.

1.1.4 Светодиоды на передней панели

В следующей таблице приводится описание светодиодов, расположенных на передней панели.

Табл. 2 Описание светодиодов передней панели

СВЕТОДИОД	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
PWR/SYS	Зеленый	Горит	Электропитание модема включено и устройство нормально работает.
		Мигает	Модем перезагружается.
		Не горит	Модем не готов или не исправен.
10/100M	Зеленый	Горит	Соединение Ethernet 10 Мбит/с успешно установлено.
		Мигает	Модем принимает или передает данные.
	Желтый	Горит	Соединение Ethernet 100 Мбит/с успешно установлено.
		Мигает	Модем принимает или передает данные.
		Не горит	Локальная сеть не подключена.
DSL	Зеленый	Горит	Соединение с DSL-коммутатором успешно установлено.
		Мигает (медленно)	Модем инициализирует линию DSL.
		Мигает (быстро)	Модем передает или принимает не-PPP трафик.
		Не горит	Канал DSL не работает.

Табл. 2 Описание светодиодов передней панели

СВЕТОДИ ОД	ЦВЕТ	СОСТОЯН ИЕ	ОПИСАНИЕ
PPP	Желтый	Горит	Установлено PPP соединение (PPPoA или PPPoE).
		Мигает	Модем передает или принимает трафик PPPoA или PPPoE.
		Не горит	PPP соединение (PPPoA или PPPoE) не установлено.

ГЛАВА 2

Знакомство с Web-конфигуратором

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

2.1 Описание Web-конфигуратора

Web-конфигуратор - это интерфейс управления на основе технологии HTML, который позволяет выполнять настройку и управление модемом с помощью браузера Интернет. Необходимо использовать Internet Explorer версии 6.0 и выше или Netscape Navigator версии 7.0 и выше с включенной функцией JavaScript. Рекомендуемое разрешение экрана - 1024 на 768 пикселей.

2.1.1 Доступ к Web-конфигуратору модема

- 1 Убедитесь, что оборудование подключено правильно (см. *Краткое руководство*).
- 2 Подготовьте компьютер/компьютерную сеть для подключения к модему (см. [Приложение D, "PPPoE"](#)).
- 3 Запустите Web-браузер.
- 4 Введите в качестве адреса Web-сайта "192.168.1.1".
- 5 Появляется окно с запросом на ввод пароля. Введите пароль (по умолчанию "1234"). Щелкните **Login (Вход)** для перехода к окну, где предлагается изменить существующий пароль. Щелкните **Cancel (Отменить)**, чтобы сохранить пароль по умолчанию в поле ввода пароля.

Рис. 3 Окно ввода пароля



- 6 Настоятельно рекомендуется изменить пароль по умолчанию! Введите пароль, введите его еще раз для подтверждения и щелкните **Apply (Применить)**; в другом

случае, если в настоящее время вы не хотите изменять пароль, щелкните **Ignore (Пропустить)** для перехода к Главному меню.



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

Рис. 4 Изменение пароля при входе

Use this screen to change the password.

We recommend that you personalize the system administrator password by changing it to something besides the default '1234'.

The administrator password should must be between 1 - 30 characters.

New Password:

Retype to Confirm:

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



ПРИМЕЧАНИЕ: Модем автоматически завершает сеанс после пяти минут бездействия. Если это произойдет, просто повторно подключитесь к модему через сеть и войдите в систему.

2.1.2 Сброс модема к заводским установкам

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

2.1.2.1 Использование кнопки сброса к заводским установкам

- 1 Убедитесь, что светодиод **PWR/SYS** горит (не мигает).
- 2 Нажмите и удерживайте кнопку **RESET (СБРОС)** в течение десяти секунд или до тех пор, пока светодиод **PWR/SYS** не начнет мигать, тогда отпустите ее. Когда светодиод **PWR/SYS** начинает мигать, происходит восстановление настроек по умолчанию, и модем перезагружается.

2.1.3 Интерфейс Web-конфигуратора модема

Далее описывается, как работать с интерфейсом Web-конфигуратора из окна **SITE MAP (КАРТА САЙТА)**.

- Щелкните **Wizard Setup (Мастер установки)** для запуска мастера, который поможет Вам произвести первоначальную настройку модема.
- Для выставления параметров дополнительных функциональных возможностей модема, щелкните по ссылке **Advanced Setup (Дополнительная настройка)**.
- Щелкните по ссылке **Maintenance (Сопровождение)** для просмотра статистики о работе модема, информации о версии микропрограммы, создания резервной копии настроек системы или их восстановления из сохраненного файла.
- По завершении операций в рамках сеанса связи по управлению модемом, щелкните по ссылке **Logout (Выход)**, расположенной на панели навигации.

Рис. 5 Web-конфигуратор: Окно Site Map (Карта сайта)



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

Табл. 3 Сводная таблица окон Web-конфигуратора

РАЗДЕЛ	ПОДРАЗДЕЛ	ФУНКЦИЯ
Wizard Setup (Мастер установки)		
Wizard Setup (Мастер установки)		Эти окна используются для первоначальной настройки, включая настройку общих параметров, параметров Интернет-провайдера для доступа в Интернет и назначения IP-адреса в глобальной сети, сервера DNS, MAC-адреса.
Advanced Setup (Дополнительная настройка)		
Password (Пароль)		Это окно используется для изменения пароля.
LAN (Локальная сеть)		Это окно используется для настройки параметров DHCP и TCP/IP локальной сети.

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

РАЗДЕЛ	ПОДРАЗДЕЛ	ФУНКЦИЯ
WAN (Глобальная сеть)	WAN Setup (Настройка глобальной сети)	Это окно используется для изменения в модеме параметров удаленного узла глобальной сети.
	WAN Backup (Резервное подключение к глобальной сети)	Это окно используется для настройки параметров перенаправления трафика и настройки резервного подключения к глобальной сети.
NAT	SUA Only (Только SUA)	Это окно используется для настройки серверов, расположенных за устройством.
	Full Feature (Полный набор функциональных возможностей)	Это окно используется для настройки правил отображения сетевых адресов.
Security (Безопасность)		Это окно используется для настройки безопасности работы с Интернет и применения предустановленных правил фильтров.
Dynamic DNS (Динамическая система доменных имен)		Это окно используется для установки динамического сервера DNS.
Time and Date (Время и дата)		Это окно используется для установки времени и даты в модеме.
Remote Management (Удаленное управление)		Это окно используется для настройки интерфейсов и IP-адреса(ов), с которых пользователям разрешается выполнять управление модемом по протоколу Telnet/FTP/Web.
UPnP		Это окно используется для включения в модеме функции UPnP.
Maintenance (Сопровождение)		
System Status (Состояние системы)		В этом окне содержится административная и общесистемная информация.
DHCP Table (Таблица DHCP)		В этом окне отображается информация DHCP (Протокол динамической конфигурации узлов) в режиме ТОЛЬКО ДЛЯ ЧТЕНИЯ.
Any IP Table (Таблица Any IP)		В этом окне отображается текущая информация в режиме ТОЛЬКО ДЛЯ ЧТЕНИЯ обо всех сетевых устройствах, которые используют функцию Any IP для доступа к модему.
Diagnostic (Диагностика)	General (Общая)	Информация в этих окнах предназначена помочь определить неисправность основного подключения модема.
	DSL Line (DSL линия)	Информация в этих окнах предназначена помочь определить неисправность DSL линии.
Firmware (Микропрограмма)		Это окно используется для загрузки микропрограммы в модем.
Logout (Конец сеанса)		Эта ссылка используется для выхода из Web-конфигуратора.

ГЛАВА 3

Мастер установки

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

3.1 Введение

Wizard Setup (Мастер установки) используется для настройки системы с целью получения доступа в Интернет посредством ввода параметров (предоставленных вашим Интернет-провайдером) в таблицу 3 с настройками ADSL подключения, которая представлена в *Кратком руководстве*. Некоторые поля в мастере установки могут быть уже настроены вашим Интернет-провайдером.

3.1.1 Инкапсуляция

Убедитесь, что используется метод инкапсуляции, который требуется для вашего Интернет-провайдера. Модем поддерживает следующие методы инкапсуляции.

3.1.1.1 ENET ENCAP

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

3.1.1.2 PPP over Ethernet (протокол "точка-точка" поверх Ethernet)

Протокол PPPoE обеспечивает функции управления доступом и учета аналогично услуге доступа по коммутируемой линии с использованием протокола PPP. P-660RT EE образует мост для сеанса PPP поверх Ethernet (PPP over Ethernet, RFC 2516) от вашего компьютера к постоянному виртуальному каналу ATM (Permanent Virtual Circuit - PVC), до DSL-коммутатора, на котором PPP сеанс завершается. Один постоянный виртуальный канал (PVC) может поддерживать любое количество сеансов PPP из вашей локальной сети. Для получения дополнительной информации по PPPoE, см. Приложения.

3.1.1.3 PPPoA (протокол "точка-точка" поверх ATM)

PPPoA означает Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) (Протокол "точка-точка" по уровню 5 адаптации ATM). Соединение PPPoA функционирует подобно коммутируемому соединению Интернет. Модем инкапсулирует сеанс связи PPP на основе RFC1483 и пересылает его по постоянному виртуальному каналу ATM (PVC) к DSL-коммутатору Интернет-провайдера. Для получения дополнительной информации по PPPoA см. комментарий RFC 2364. Для информации по PPP см. комментарий RFC 1661.

3.1.1.4 RFC 1483

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

3.1.2 Мультиплексирование

Существует два способа определить, какие протоколы используются для передачи по виртуальному каналу (VC). Убедитесь, что вы используете метод мультиплексирования, который требуется для вашего Интернет-провайдера.

3.1.2.1 Мультиплексирование на базе VC

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

3.1.2.2 Мультиплексирование на базе LLC

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

3.1.3 VPI и VCI

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

3.1.4 Мастер установки доступа в Интернет: Первое окно

В окне **SITE MAP (КАРТА САЙТА)** щелкните **Wizard Setup (Мастер установки)** для отображения первого окна мастера.

Рис. 6 Мастер установки доступа в Интернет: Первое окно

The screenshot shows a window titled "Wizard Setup - ISP Parameters for Internet Access". It contains the following fields and values:

- Mode:** Routing (dropdown menu)
- Encapsulation:** RFC 1483 (dropdown menu)
- Multiplex:** LLC (dropdown menu)
- Virtual Circuit ID:**
 - VPI:** 8 (text input)
 - VCI:** 35 (text input)

A "Next" button is located at the bottom right of the window.

В следующей таблице даны описания полей этого окна.

Табл. 4 Мастер установки доступа в Интернет: Первое окно

ПОЛЕ	ОПИСАНИЕ
Mode (Режим)	Из раскрывающегося списка поля Mode (Режим) выберите Routing (Маршрутизация) (установлено по умолчанию), если ваш Интернет-провайдер позволяет использовать одни учетные данные для подключения к Интернету для нескольких компьютеров. В другом случае выберите Bridge (Мост) .
Encapsulation (Инкапсуляция)	Выберите тип инкапсуляции, используемый вашим Интернет-провайдером, из раскрывающегося списка поля Encapsulation (Инкапсуляция) . Опции в списке зависят от значения, установленного в поле Mode (Режим) . Если в поле Mode (Режим) вы установили Bridge (Мост) , то выберите PPPoA или RFC 1483 . Если в поле Mode (Режим) вы установили Routing (Маршрутизация) , то выберите PPPoA , RFC 1483 , ENET ENCAP или PPPoE .

Табл. 4 Мастер установки доступа в Интернет: Первое окно

ПОЛЕ	ОПИСАНИЕ
Multiplex (Мультиплексирование)	Выберите метод мультиплексирования, который использует ваш Интернет-провайдер, из раскрывающегося списка поля Multiplex (Мультиплексирование) : VC-based или LLC-based.
Virtual Circuit ID (Идентификатор виртуальной линии передачи)	VPI (Virtual Path Identifier - Идентификатор виртуального пути) и VCI (Virtual Channel Identifier - Идентификатор виртуального канала) определяют виртуальную линию передачи. Более подробно см. в приложении.
VPI	Введите назначенный вам номер VPI. Это поле может быть уже заполнено.
VCI	Введите назначенный вам номер VCI. Это поле может быть уже заполнено.
Next (Далее)	Щелкните по этой кнопке для перехода к следующему окну Мастера. Вид следующего окна зависит от выбранного выше протокола. Щелкните по ссылке протокола для перехода к следующему окну мастера для этого протокола.

3.2 IP-адрес и маска подсети

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

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

Если Интернет-провайдер не предоставляет явным образом адрес сети, то, скорее всего, вы используете учетную запись одиночного пользователя, и Интернет-провайдер будет назначать динамический IP-адрес при каждом установлении соединения. В этом случае необходимо выбрать IP-адрес из диапазона 192.168.0.0 - 192.168.255.0 и включить функцию NAT (Network Address Translation - Трансляция сетевых адресов) в устройстве P-660RT EE. Этот диапазон IP-адресов специально зарезервирован Агентством по назначению имен и уникальных параметров протоколов Интернет (IANA) для частного использования. Если не предписано иное, не следует использовать номера за пределами этого диапазона. Если выбрать адрес 192.168.1.0 в качестве номера сети, то получится 254 индивидуальных адреса от 192.168.1.1 до 192.168.1.254 (числа ноль и 255 зарезервированы). Иными словами, первые три числа в адресе задают номер сети, а остальные определяют конкретный компьютер в этой сети.

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

Маска подсети определяет сетевую часть IP-адреса. Модем вычисляет маску подсети автоматически на основе введенного IP-адреса. Если не указано иное, не следует изменять маску подсети, вычисленную модемом.

3.2.1 Назначение IP-адреса

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

3.2.1.1 Назначение IP с инкапсуляцией PPPoA или PPPoE

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

3.2.1.2 Назначение IP с инкапсуляцией RFC 1483

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

3.2.1.3 Назначение IP с инкапсуляцией ENET ENCAP

В этом случае можно иметь как статический, так и динамический IP-адрес. Для статического IP-адреса необходимо заполнить оба поля **IP Address (IP-адрес)** и **ENET ENCAP Gateway (Шлюз ENET ENCAP)**, параметры для которых предоставляются вашим Интернет-провайдером. Однако при назначении динамического IP-адреса, модем функционирует как клиент DHCP через порт WAN и, следовательно, поля **IP Address (IP-адрес)** и **ENET ENCAP Gateway (Шлюз ENET ENCAP)** являются недоступными (N/A), так как эти параметры для модема назначает сервер DHCP.

3.2.1.4 IP-адреса для частных сетей

Каждая машина в сети Интернет должна иметь уникальный адрес. Если сеть изолирована от Интернета, например, соединяет между собой локальные сети двух филиалов, можно без проблем назначать произвольные IP-адреса узлам

. Тем не менее, Агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало следующие три блока IP-адресов специально для частных сетей:

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

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



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

3.2.2 Постоянное соединение (PPP)

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

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

3.2.3 NAT

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

3.2.4 Мастер установки доступа в Интернет: Второе окно

Вид второго окна Мастера установка зависит от выбранного режима и типа инкапсуляции. Далее показаны окна для режима маршрутизации. Заполните поля и щелкните по кнопке **Next (Далее)** для продолжения.

Рис. 7 Подключение к Интернету по PPPoE

Wizard Setup - ISP Parameters for Internet Access

Service Name

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout sec

Nailed-Up Connection

Network Address Translation

В следующей таблице даны описания полей этого окна.

Табл. 5 Подключение к Интернету с использованием PPPoE

ПОЛЕ	ОПИСАНИЕ
Service Name (Имя услуги)	Введите имя провайдера услуг PPPoE.
User Name (Имя пользователя)	Введите имя пользователя в том же виде, как оно назначено Интернет-провайдером. Если имя назначается в виде user@domain , где domain означает имя услуги, необходимо ввести оба элемента именно так, как назначено провайдером.
Password (Пароль)	Введите пароль для данного имени пользователя.
IP Address (IP-адрес)	Статический IP-адрес представляет собой фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является постоянным. При каждом подключении к Интернету Интернет-провайдер будет назначать новый адрес. Выберите Obtain an IP Address Automatically (Получать IP-адрес автоматически) , если у вас динамический IP-адрес; в другом случае выберите Static IP Address (Статический IP-адрес) и введите IP-адрес, предоставленный Интернет-провайдером, в расположенном ниже текстовом поле.

Табл. 5 Подключение к Интернету с использованием PPPoE (продолжение)

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

Рис. 8 Подключение к Интернету по RFC 1483

The screenshot shows a window titled "Connection Setup- ISP Parameters for Internet Access". It contains the following elements:

- An "IP Address" text box containing the value "0.0.0.0".
- A "Network Address Translation" section with a dropdown menu currently set to "SUA Only".
- At the bottom of the window, there are two buttons: "Back" and "Next".

В следующей таблице даны описания полей этого окна.

Табл. 6 Подключение к Интернету с использованием RFC 1483

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Это поле доступно, если в поле Mode (Режим) выбран режим Routing (Маршрутизация) . Введите в это поле IP-адрес, предоставленный Интернет-провайдером.
Network Address Translation (Трансляция сетевых адресов)	Из раскрывающегося списка выберите None (Нет) , SUA Only (Только SUA) или Full Feature (Полный набор функциональных возможностей) . Более подробно см. Глава 7, на стр. 71 .
Back (Назад)	Для возврата к первому окну Мастера щелкните по кнопке Back (Назад) .
Next (Далее)	Для перехода к следующему окну Мастера щелкните по кнопке Next (Далее) .

Рис. 9 Подключение к Интернету с использованием ENET ENCAP

Connection Setup-ISP Parameters for Internet Access

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Subnet Mask

ENET ENCAP Gateway

Network Address Translation

▾

В следующей таблице даны описания полей этого окна.

Табл. 7 Подключение к Интернету с использованием ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Статический IP-адрес представляет собой фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является постоянным. При каждом подключении к Интернету Интернет-провайдер будет назначать новый адрес. Выберите Obtain an IP Address Automatically (Получать IP-адрес автоматически) , если у вас динамический IP-адрес; в другом случае выберите Static IP Address (Статический IP-адрес) и введите IP-адрес, предоставленный Интернет-провайдером, в расположенном ниже текстовом поле.
Subnet Mask (Маска подсети)	Введите маску подсети в десятичном формате с разделительными точками. Если требуется создание подсетей, см. Приложение С для расчета маски подсети.
ENET ENCAP Gateway (Шлюз ENET ENCAP)	Необходимо указать IP-адрес шлюза (предоставленный вашим Интернет-провайдером), если в предыдущем окне в поле Encapsulation (Инкапсуляция) установлен тип инкапсуляции ENET ENCAP .
Network Address Translation (Трансляция сетевых адресов)	Из раскрывающегося списка выберите None (Нет) , SUA Only (Только SUA) или Full Feature (Полный набор функциональных возможностей) . Более подробно см. главу NAT.
Back (Назад)	Для возврата к первому окну Мастера щелкните по кнопке Back (Назад) .
Next (Далее)	Для перехода к следующему окну Мастера щелкните по кнопке Next (Далее) .

Рис. 10 Подключение к Интернету с использованием PPPoA

Connection Setup- ISP Parameters for Internet Access

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout sec

Nailed-Up Connection

Network Address Translation

▾

В следующей таблице даны описания полей этого окна.

Табл. 8 Подключение к Интернету с использованием PPPoA

ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите регистрационное имя пользователя, предоставленное Интернет-провайдером.
Password (Пароль)	Введите пароль для данного имени пользователя.
IP Address (IP-адрес)	<p>Это поле доступно, если в поле Mode (Режим) выбран режим Routing (Маршрутизация).</p> <p>Статический IP-адрес представляет собой фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является постоянным. При каждом подключении к Интернету Интернет-провайдер будет назначать новый адрес.</p> <p>Выберите Obtain an IP Address Automatically (Получать IP-адрес автоматически), если у вас динамический IP-адрес; в другом случае выберите Static IP Address (Статический IP-адрес) и введите IP-адрес, предоставленный Интернет-провайдером, в расположенном ниже текстовом поле.</p>

Табл. 8 Подключение к Интернету с использованием PPPoA (продолжение)

ПОЛЕ	ОПИСАНИЕ
Connection (Подключение)	Выберите Connect on Demand (Подключение по требованию) , если постоянное соединение не требуется, и укажите в поле Max. Idle Timeout (Максимальное время неактивности) время неактивности (в секундах). По умолчанию для режима Подключение по требованию время неактивности установлено на 0, что означает, что сеанс связи Интернет не будет разрываться. Выберите Nailed-Up Connection (Постоянное соединение) , если требуется постоянное соединение. При разрыве соединения модем будет автоматически пытаться его восстановить. Правило(а) расписания связи в меню SMT 26 имеет приоритет над настройками полей Connection (Подключение) .
Network Address Translation (Трансляция сетевых адресов)	Это поле доступно, если в поле Mode (Режим) выбран режим Routing (Маршрутизация) . Из раскрывающегося списка выберите None (Нет) , SUA Only (Только SUA) или Full Feature (Полный набор функциональных возможностей) . Более подробно см. Глава 7, на стр. 71 .
Back (Назад)	Для возврата к первому окну Мастера щелкните по кнопке Back (Назад) .
Next (Далее)	Для перехода к следующему окну Мастера щелкните по кнопке Next (Далее) .

3.2.5 Настройка DHCP

DHCP (Dynamic Host Configuration Protocol - Протокол динамической конфигурации узлов, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получать с сервера конфигурацию TCP/IP при начальной загрузке. Можно настроить модем как сервер DHCP или отключить эту функцию. При настроенной функции сервера DHCP, модем предоставляет клиентам конфигурацию TCP/IP. При отключении службы DHCP требуется наличие другого сервера DHCP в локальной сети, или установка конфигурации компьютера вручную.

3.2.5.1 Настройка диапазона IP

Модем имеет предварительно настроенный диапазон из 32 IP-адресов для клиентских машин, начиная с 192.168.1.33 до 192.168.1.64. Такая конфигурация обеспечивает 31 IP-адрес, от 192.168.1.2 до 192.168.1.32 (за исключением одного адреса для самого модема - 192.168.1.1) для назначения другим машинам-серверам, например почтовому серверу, FTP, telnet, web и серверам других служб, которые могут потребоваться.

3.2.6 Мастер установки доступа в Интернет: Третье окно

Проверьте сделанные установки в окне, представленном ниже. Для изменения параметров локальной сети в модеме, щелкните **Change LAN Configurations (Изменить конфигурацию локальной сети)**. В другом случае щелкните **Save Settings (Сохранить настройки)** для сохранения конфигурации и перехода к разделу 3.13.

Рис. 11 Мастер установки доступа в Интернет: Третье окно

Wizard Setup - ISP Parameters for Internet Access

WAN Information:
Mode: **Routing**
Encapsulation: **PPPoE**
Multiplexing: **LLC**
VPI/VCI: **8/35**
Service Name :
User Name : **user@icp.ch**
Password : *********
IP Address : **Obtain an IP Address Automatically**
Network Address Translation: **SUA Only**
Connect on Demand: **Max Idle Timeout 0 sec.**

LAN Information:
IP Address: **192.168.1.1**
IP Mask: **255.255.255.0**
DHCP: **ON**
Client IP Pool Starting Address: **192.168.1.33**
Size of Client IP Pool: **32**

Change LAN Configuration

Save Settings

Если необходимо изменить настройки локальной сети в модеме, щелкните **Change LAN Configuration (Изменить конфигурацию локальной сети)** для отображения окна, представленного ниже.

Рис. 12 Мастер установки доступа в Интернет: Конфигурация локальной сети

Connection Setup- ISP Parameters for Internet Access

LAN IP Address: 192.168.1.1

LAN Subnet Mask: 255.255.255.0

DHCP

DHCP Server: ON

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

Back Finish

В следующей таблице даны описания полей этого окна.

Табл. 9 Мастер установки доступа в Интернет: Конфигурация локальной сети

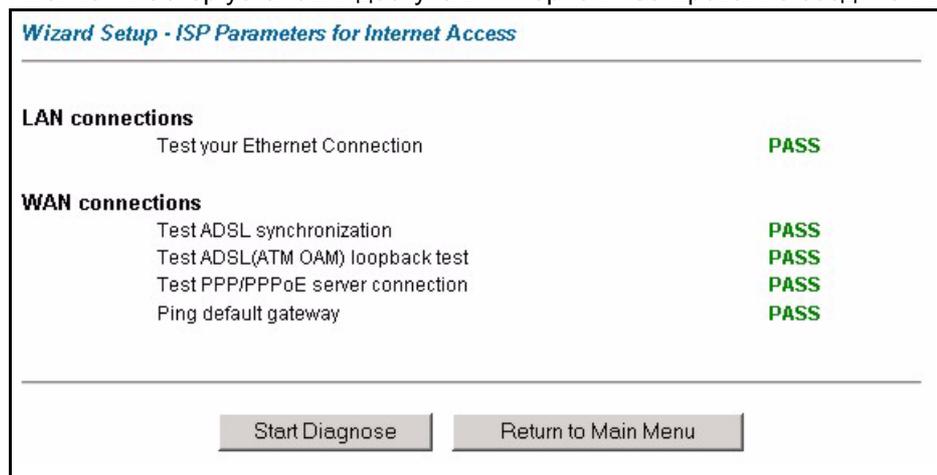
ПОЛЕ	ОПИСАНИЕ
LAN IP Address (IP-адрес в локальной сети)	Введите IP-адрес модема в десятичном формате с разделительными точками, например, 192.168.1.1 (установлено изготовителем по умолчанию). ПРИМЕЧАНИЕ: Если вы изменили IP-адрес модема в локальной сети, то для доступа к Web-конфигуратору необходимо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

Табл. 9 Мастер установки доступа в Интернет: Конфигурация локальной сети

ПОЛЕ	ОПИСАНИЕ
Secondary DNS Server (Дополнительный сервер DNS)	Аналогично записи предыдущей строки.
Back (Назад)	Для возврата к предыдущему окну щелкните по кнопке Back (Назад) .
Finish (Готово)	Щелкните по кнопке Finish (Готово) для сохранения настроек и перехода к следующему окну Мастера.

3.2.7 Мастер установки доступа в Интернет: Тестирование соединения

Модем автоматически тестирует соединение с компьютером(ами), подключенным к порту LAN. Для тестирования соединения от модема до Интернет-провайдера, щелкните по кнопке **Start Diagnose (Начать диагностику)**. В другом случае щелкните по кнопке **Return to Main Menu (Возврат в Главное меню)** для возврата к окну **Site Map (Карта сайта)**.

Рис. 13 Мастер установки доступа в Интернет: Тестирование соединения

3.2.7.1 Проверьте подключение к Интернету

Запустите Web-браузер и перейдите на сайт www.zyxel.ru. Теперь вы должны иметь доступ в Интернет. Для получения подробной информации по всем функциональным возможностям модема см. далее это *Руководство пользователя*. Если вы не можете получить доступ в Интернет, снова откройте Web-конфигуратор и проверьте, что установленные с помощью Мастера подключения настройки Интернет являются правильными.

ГЛАВА 4

Установка пароля

В этой главе описывается окно **Password (Пароль)**.

4.1 Введение

Настоятельно рекомендуется изменить пароль доступа к модему.

4.1.1 Изменение пароля

Для изменения пароля модема (настоятельно рекомендуется), в окне **Site Map (Карта сайта)** щелкните **Password (Пароль)**. Появляется окно, представленное ниже.

Рис. 14 Пароль

The screenshot shows a dialog box titled "Password". It contains three text input fields labeled "Old Password", "New Password", and "Retype to confirm". Below these fields is a red warning message: "Please record your new password whenever you change it. The system will lock you out if you have forgotten your password." At the bottom of the dialog are two buttons: "Apply" and "Cancel".

В следующей таблице даны описания полей этого окна.

Табл. 10 Пароль

ПОЛЕ	ОПИСАНИЕ
Old Password (Старый пароль)	Введите в данное поле пароль по умолчанию или текущий пароль, который используется для доступа к системе.
New Password (Новый пароль)	Введите в данное поле новый пароль.
Retype to Confirm (Повторный ввод для подтверждения)	Введите в данное поле новый пароль еще раз.

Табл. 10 Пароль

ПОЛЕ	ОПИСАНИЕ
Apply (Применить)	Щелкните по кнопке Apply (Применить) для сохранения настроек модема.
Cancel (Отменить)	Щелкните по кнопке Cancel (Отменить) , чтобы заново начать настройку в этом окне.

ГЛАВА 5

Настройка локальной сети

В этой главе описывается настройка параметров локальной сети.

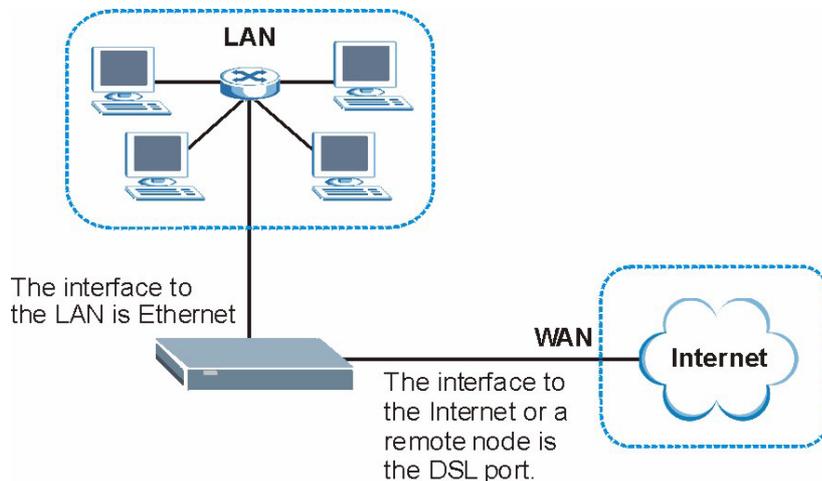
5.1 Обзор локальной сети

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

5.1.1 Локальные, глобальные сети и модем

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

Рис. 15 Локальные и глобальные IP-адреса



5.2 Адрес сервера DNS

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

Существует два способа распространения адресов серверов DNS Интернет-провайдером. Первый из них заключается в том, что Интернет-провайдер сообщает клиенту адреса серверов DNS, обычно в виде информационного листка, который клиент подписывает. Если Интернет-провайдер предоставил вам адреса серверов DNS, необходимо ввести их в поля **DNS Server (Сервер DNS)** в окне **LAN Setup (Настройка локальной сети)**, в противном случае оставьте это поле пустым.

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

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

Следует отметить, что проху-сервер DNS может работать, только если Интернет-провайдер использует серверные расширения DNS IPCP. Это не означает, что можно не включать серверы DNS при настройке DHCP при любых обстоятельствах. Если Интернет-провайдер предоставляет адреса серверов DNS в явной форме, убедитесь, что эти IP-адреса введены в окне **LAN Setup (Настройка локальной сети)**. Таким образом, модем может пересылать информацию от серверов DNS к компьютерам; а, компьютеры могут делать запрос непосредственно серверу DNS без вмешательства модема.

5.3 Назначение адреса сервера DNS

DNS (Система доменных имен) предназначена для отображения доменного имени на соответствующий ему IP-адрес и наоборот. Сервер DNS играет очень важную роль, так как без него нужно было бы точно знать IP-адрес компьютера, к которому необходимо получить доступ.

Существует два способа распространения адресов серверов DNS Интернет-провайдером.

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

5.4 Настройка TCP/IP локальной сети

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

5.4.1 Настройки локальной сети, установленные изготовителем по умолчанию

Изготовителем модема предустановлены следующие параметры локальной сети:

- IP-адрес of 192.168.1.1 с маской подсети of 255.255.255.0 (24 бита)
- Включена функция сервера DHCP с 32 IP-адресами для клиентов, начиная с адреса 192.168.1.33.

Данные параметры работоспособны в большинстве случаев. Если Интернет-провайдер предоставил адрес(а) сервера(ов) DNS в явной форме, см. встроенную справку Web-конфигуратора для настройки соответствующих полей.

5.4.2 IP-адрес и маска подсети

Для получения подробной информации, см. [Глава 3 Мастер установки](#) раздел [IP-адрес и маска подсети](#).

5.4.3 Настройка RIP

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

- **Both (Оба)** - модем осуществляет периодическую широковещательную рассылку своей маршрутной таблицы и принятых данных RIP.

- **In Only (Только входящие)** - модем не посылает пакеты RIP, но принимает поступающие пакеты RIP.
- **Out Only (Только исходящие)** - модем посылает пакеты RIP, но не принимает поступающие пакеты RIP.
- **None** - модем не посылает пакеты RIP и игнорирует поступающие пакеты RIP.

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

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

5.4.4 Многоадресная рассылка

Как правило, пакеты IP передаются одним из двух способов - одноадресная рассылка (1 отправитель - 1 получатель) или широковещательная рассылка (1 отправитель - все абоненты сети). При многоадресной рассылке IP-пакеты пересылаются конкретной группе компьютеров в сети, то есть, не одному компьютеру, но и не всем.

IGMP (Internet Group Multicast Protocol - Протокол многоадресной рассылки) - это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки - он не предназначен для передачи пользовательских данных. Версия 2 IGMP (RFC 2236) является усовершенствованным вариантом версии 1 (RFC 1112), однако версия 1 IGMP по-прежнему широко используется. Для получения более подробной информации о взаимодействии между IGMP версии 2 и версии 1, см. разделы 4 и 5 RFC 2236. Для идентификации групп узлов используются IP-адреса класса D, которые находятся в диапазоне от 224.0.0.0 до 239.255.255.255. Адрес 224.0.0.0 не назначается ни одной группе и используется компьютерами, выполняющими многоадресную рассылку. Адрес 224.0.0.1 используется для запросов и назначается постоянной группе, в которую входят все узлы (включая шлюзы). Чтобы участвовать в многоадресной рассылке IGMP, в группу 224.0.0.1 должны входить все узлы. Адрес 224.0.0.2 назначается группе маршрутизаторов, участвующих в многоадресной рассылке.

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

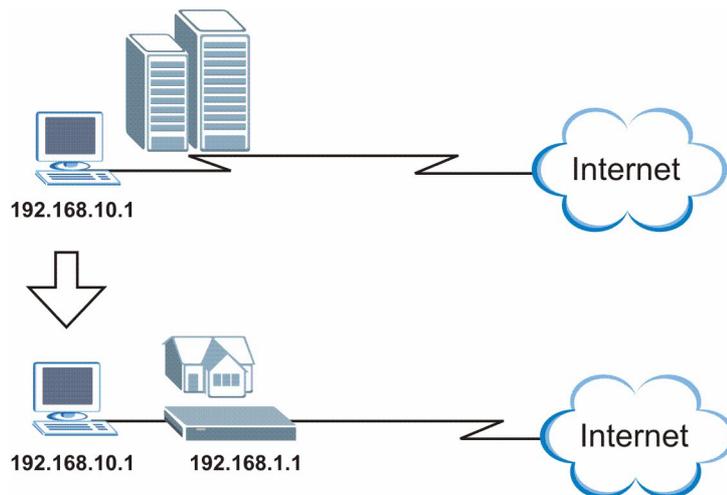
5.5 Any IP (Любой IP)

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

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

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

Рис. 16 Пример: Any IP



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



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

5.5.1 Как работает функция Any IP (Любой IP)

ARP (Address Resolution Protocol - Протокол разрешения адресов) служит для установления соответствия между адресом межсетевого протокола IP (IP-адрес) и аппаратным адресом машины в локальной сети, известного также как Media Access Control (Управление доступом к среде) или MAC-адрес. Таблица маршрутизации IP составляется в устройстве IP Ethernet (модеме) для принятия решения, какой следующий транзитный пункт необходимо использовать для пересылки данных конкретному адресату.

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

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

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

5.6 Настройка локальной сети

Щелкните **LAN (Локальная сеть)** и **LAN Setup (Настройка локальной сети)** для отображения следующего окна.

Рис. 17 Настройка локальной сети

LAN - LAN Setup

DHCP

DHCP

Client IP Pool Starting Address

Size of Client IP Pool

Primary DNS Server

Secondary DNS Server

Remote DHCP Server

TCP/IP

IP Address

IP Subnet Mask

RIP Direction

RIP Version

Multicast

В следующей таблице даны описания полей этого окна.

Табл. 11 LAN Setup

ПОЛЕ	ОПИСАНИЕ
DHCP	
DHCP	<p>Если в этом поле установлено значение Server (Сервер), модем может назначать IP-адреса, шлюз IP по умолчанию и серверы DNS для Windows 95, Windows NT и других систем, поддерживающих клиента DHCP.</p> <p>Если установлено значение None, функция сервера DHCP отключена.</p> <p>Если установлено значение Relay (Ретранслятор), Модем работает в качестве фиктивного сервера DHCP и ретранслирует запросы и ответы DHCP между удаленным сервером и клиентами. В этом случае следует ввести IP-адрес фактического удаленного сервера DHCP в поле Remote DHCP Server (Удаленный сервер DHCP).</p> <p>Если функция DHCP включена, необходимо установить следующие параметры:</p>
Client IP Pool Starting Address (Начальный адрес диапазона IP-адресов клиентов)	В этом поле вводится первый адрес непрерывного диапазона IP-адресов.
Size of Client IP Pool (Размер диапазона IP-адресов клиентов)	В этом поле устанавливается размер или счётчик непрерывного диапазона IP-адресов.

Табл. 11 LAN Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Primary DNS Server (Основной сервер DNS)	Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Secondary DNS Server (Дополнительный сервер DNS)	Аналогично предыдущей записи.
Remote DHCP Server (Удаленный сервер DHCP)	Если в поле DHCP выбрано значение Relay (Ретранслятор) , следует ввести IP-адрес фактического удаленного сервера DHCP.
TCP/IP	
IP Address (IP-адрес)	Введите IP-адрес модема в десятичном формате с разделительными точками, например, 192.168.1.1 (установлено изготовителем по умолчанию).
IP Subnet Mask (Маска IP подсети)	Введите маску подсети, назначенную вашим Интернет-провайдером (если задана).
RIP Direction (Направление RIP)	Выберите направление RIP из раскрывающего списка со значениями None (Нет) , Both (Оба) , In Only (Только входящие) и Out Only (Только исходящие) .
RIP Version (Версия RIP)	Выберите версию RIP, где возможны варианты: RIP-1 , RIP-2B и RIP-2M .
Multicast (Многоадресная рассылка)	IGMP (Internet Group Multicast Protocol - Протокол многоадресной рассылки) - это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Модем поддерживает обе версии IGMP: версию 1 (IGMP-v1) и IGMP-v2 . Для отключения выберите None (Нет) .
Any IP Setup (Any IP)	Поставьте флажок в окошке Active (Включить) для включения функции Any IP. Функция Any IP позволяет компьютеру получить доступ в Интернет без изменения сетевых настроек (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и модема находятся в разных подсетях. При отключении функции Any IP, только компьютеры с динамическими или статическими IP-адресами, находящимися в той же подсети, что и IP-адрес модема, смогут подключиться к модему или получить доступ в Интернет через модем.
Apply (Применить)	Щелкните по кнопке Apply (Применить) для сохранения настроек модема.
Cancel (Отменить)	Щелкните по кнопке Cancel (Отменить) , чтобы заново начать настройку в этом окне.

ГЛАВА 6

Настройка глобальной сети

В этой главе описывается настройка настроек глобальной сети.

6.1 Обзор глобальной сети

Интерфейс WAN (Wide Area Network - Глобальная вычислительная сеть) является внешним подключением к другой сети или Интернет.

Более подробно о настройке полей в окнах Глобальная сеть см. [Глава 3 Мастер установки](#).

6.2 Метрика

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

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

- Стандартный маршрут: назначается Интернет-провайдером (см. [раздел Доступ в Интернет с использованием Zero Configuration \(Автоматическая настройка на провайдера\)](#))
- Маршрут перенаправления трафика (см. [раздел Перенаправление трафика](#))
- Резервный маршрут WAN, называемый также резервное коммутируемое подключение (см. [раздел Настройка резервного подключения к глобальной сети](#))

Например, если стандартный маршрут имеет метрику "1", маршрут перенаправления трафика имеет метрику "2" и резервный маршрут имеет метрику "3", то стандартный маршрут используется как основной маршрут по умолчанию. Если по стандартному маршруту не удастся установить подключение к Интернету, тогда модем пытается использовать маршрут перенаправления трафика. Аналогичным образом, если соединение не удалось установить с помощью маршрута перенаправления трафика, модем использует резервный маршрут.

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



ПРИМЕЧАНИЕ: Маршрутизация на базе стратегии IP замещает схему маршрутизации по умолчанию и имеет приоритет над всеми маршрутами, описанными выше (см. [Глава 28 Маршрутизация на базе стратегии IP](#)).

6.3 Инкапсуляция PPPoE

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

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

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

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

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

6.4 Формирование трафика

Формирование трафика представляет собой соглашение между оператором связи и абонентом, предназначенное для регулирования средней скорости и колебаний скорости передачи данных по сети АТМ. Такое соглашение помогает устранить перегрузку каналов, что важно для передачи данных в реальном времени, таких как аудио- и видеоданные.

PCR (Peak Cell Rate - Пиковая скорость ячеек) - это максимальная скорость, с которой отправитель может передавать ячейки. Данный параметр может быть ниже (но не выше), чем максимальная скорость передачи в линии. Размер 1 ячейки ATM равен 53 байта (424 бита), таким образом, при максимальной скорости передачи 832 кбит/с, максимальная скорость PCR равна 1962 ячеек/с. Однако эта скорость не гарантирована, так как она зависит от скорости передачи в линии.

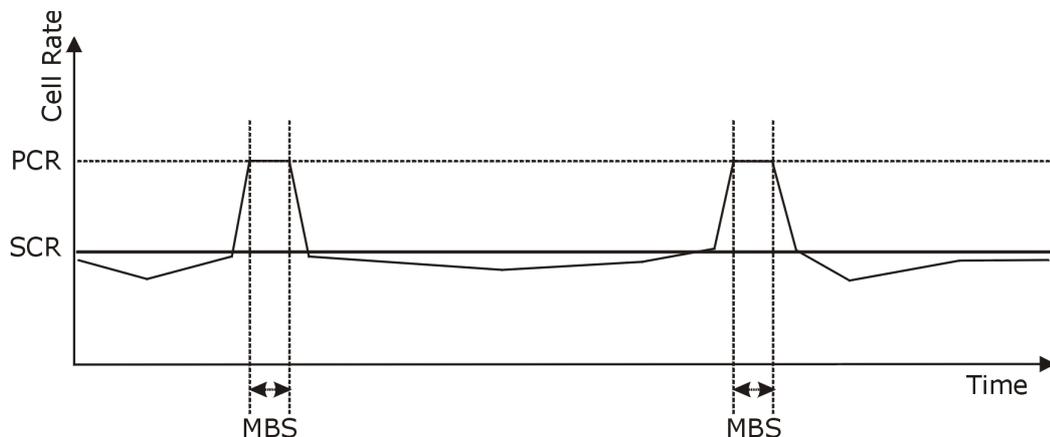
SCR (Sustained Cell Rate - Поддерживаемая скорость ячеек) - это средняя скорость ячеек каждого источника пульсирующего трафика. Она определяет максимальную среднюю скорость, с которой ячейки могут передаваться по виртуальному соединению. SCR не может быть больше, чем PCR.

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

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

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

Рис. 18 Пример формирования трафика



6.5 Доступ в Интернет с использованием Zero Configuration (Автоматическая настройка на провайдера)

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

Автоматическая настройка отключается, если:

- Модем находится в режиме моста
- Модем назначен статический (постоянный) IP-адрес в глобальной сети.

6.6 Настройка подключения к глобальной сети

Для изменения в модеме настроек удаленного узла глобальной сети, щелкните **WAN (Глобальная сеть)** и **WAN Setup (Настройка подключения к глобальной сети)**.

Появляется окно, вид которого зависит от типа инкапсуляции.

Рис. 19 Настройка подключения к глобальной сети (PPPoE)

WAN - WAN Setup

Name

Mode

Encapsulation

Multiplex

Virtual Circuit ID

VPI

VCI

ATM QoS Type

Cell Rate

Peak Cell Rate cell/sec

Sustain Cell Rate cell/sec

Maximum Burst Size

Login Information

Service Name

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Connection

Nailed-Up Connection

Connect on Demand

Max Idle Timeout sec

PPPoE Pass Through

PPPoE + PPPoE_Client_PC

В следующей таблице даны описания полей этого окна.

Табл. 12 Настройка подключения к глобальной сети

ПОЛЕ	ОПИСАНИЕ
Name (Имя)	Введите имя Интернет-провайдера, например, MyISP. (Эта информация используется только для идентификации).
Mode (Режим)	Из раскрывающегося списка поля Mode (Режим) выберите Routing (Маршрутизация) (установлено по умолчанию), если ваш Интернет-провайдер позволяет использовать одни учетные данные для подключения к Интернету для нескольких компьютеров. В другом случае, выберите Bridge (Мост) .

Табл. 12 Настройка подключения к глобальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
Encapsulation (Инкапсуляция)	Выберите из раскрывающегося списка метод инкапсуляции, используемый вашим Интернет-провайдером. Опции в списке зависят от режима, установленного в поле Mode (Режим) . Если в поле Mode (Режим) вы установили Bridge (Мост) , то выберите PPPoA или RFC 1483 . Если в поле Mode (Режим) вы установили Routing (Маршрутизация) , то выберите PPPoA , RFC 1483 , ENET ENCAP или PPPoE .
Multiplex (Мультиплексирование)	Выберите из раскрывающегося списка метод мультиплексирования, используемый вашим Интернет-провайдером. Вариантами являются VC или LLC .
Virtual Circuit ID (Идентификатор виртуальной линии передачи)	VPI (Virtual Path Identifier - Идентификатор виртуального пути) и VCI (Virtual Channel Identifier - Идентификатор виртуального канала) определяют виртуальную линию передачи. Более подробно см. в приложении.
VPI	Допустимый диапазон для VPI равен от 0 до 255. Введите назначенный вам номер VPI.
VCI	Допустимый диапазон для VCI равен от 32 до 65535 (номера от 0 до 31 зарезервированы для локального управления трафиком ATM). Введите назначенный вам номер VCI.
ATM QoS Type (Тип качества обслуживания ATM)	Выберите CBR (Постоянная скорость передачи) для установки постоянной (всегда доступной) пропускной способности для трафика речи или данных. Выберите UBR (Unspecified Bit Rate - Неопределенная скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите VBR (Variable Bit Rate - Переменная скорость передачи) для пульсирующего трафика и разделения пропускной способности с другими приложениями.
Cell Rate (Скорость ячеек)	Настройка скорости ячеек часто помогает устранить перегрузку в сети, которая снижает скорость передачи данных в реальном времени, таких как аудио и видео трафик.
Peak Cell Rate (Пиковая скорость ячеек)	Чтобы найти PCR (Peak Cell Rate - Пиковая скорость ячеек), разделите скорость DSL линии (бит/с) на 424 (размер ячейки ATM). Это максимальная скорость, с которой отправитель может передавать ячейки. Введите в это поле значение PCR.
Sustain Cell Rate (Поддерживаемая скорость ячеек)	Параметр SCR (Sustain Cell Rate - Поддерживаемая скорость ячеек) устанавливает среднюю скорость ячеек (установившаяся скорость), с которой они могут передаваться. Введите значение SCR, оно должно быть меньше, чем PCR. Следует отметить, что по умолчанию установлено 0 ячеек/с.
Maximum Burst Size (Максимальный размер пакета)	MBS (Maximum Burst Size - Максимальный размер пакета) - это максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите значение MBS (должно быть меньше 65535).
Login Information (Регистрационные данные)	(Только для инкапсуляции PPPoA и PPPoE)
Service Name (Имя услуги)	(Только для PPPoE). Введите имя услуги PPPoE в это поле.
User Name (Имя пользователя)	Введите имя пользователя точно так, как назначено Интернет-провайдером. Если имя назначается в формате user@domain, где domain означает имя услуги, то вводите оба элемента имени точно так, как назначено.

Табл. 12 Настройка подключения к глобальной сети (продолжение)

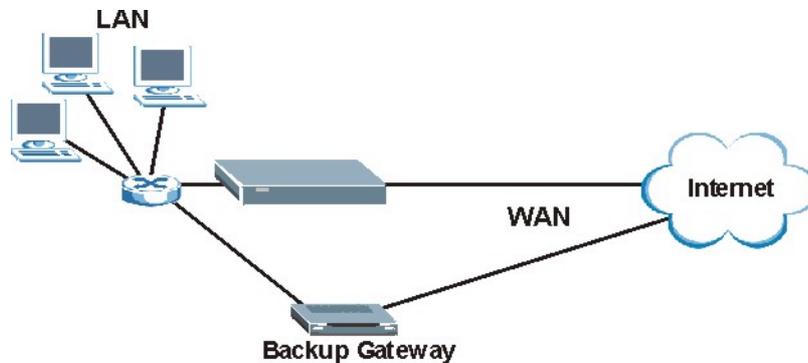
ПОЛЕ	ОПИСАНИЕ
Password (Пароль)	Введите пароль для данного имени пользователя.
IP Address (IP-адрес)	<p>Это поле доступно, если в поле Mode (Режим) выбран режим Routing (Маршрутизация).</p> <p>Статический IP-адрес представляет собой фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является постоянным. При каждом подключении к Интернету Интернет-провайдер будет назначать новый адрес.</p> <p>Выберите Obtain an IP Address Automatically (Получать IP-адрес автоматически), если у вас динамический IP-адрес; в другом случае выберите Static IP Address (Статический IP-адрес) и введите IP-адрес, предоставленный Интернет-провайдером, в расположенное ниже поле.</p>
Connection (Подключение) (Только для инкапсуляции PPPoA и PPPoE)	Правило(а) расписания связи в меню SMT 26 имеет приоритет над настройками полей Connection (Подключение) .
Nailed-Up Connection (Постоянное соединение)	Выберите Nailed-Up Connection (Постоянное соединение) , если требуется постоянное соединение. При разрыве соединения модем будет автоматически пытаться его восстановить.
Connect on Demand (Подключение по требованию)	Выберите Connect on Demand (Подключение по требованию) , если постоянное соединение не требуется, и введите в поле Max. Idle Timeout (Максимальное время неактивности) время неактивности (в секундах).
Max Idle Timeout (Максимальное время неактивности)	Если вы выбрали Connect on Demand (Подключение по требованию) введите интервал неактивности в поле Max Idle Timeout (Максимальное время неактивности) . По умолчанию установлено 0, что означает, что соединение с Интернет не будет разрываться.
PPPoE Pass Through (Сквозное пропускание PPPoE) (Только для инкапсуляции PPPoE)	<p>Это поле доступно, если вы выбрали инкапсуляцию PPPoE.</p> <p>В дополнение к встроенному в модем клиенту PPPoE, вы можете включить функцию сквозного пропускания PPPoE, чтобы разрешить до 10 узлам локальной сети использовать у себя программное обеспечение клиента PPPoE для подключения к Интернет-провайдеру через модем. Каждый узел может иметь свои учетные данные и общедоступный IP-адрес в глобальной сети.</p> <p>Сквозное пропускание PPPoE является альтернативой NAT для применений, где использование NAT нецелесообразно.</p> <p>Отключите функцию сквозного пропускания PPPoE, если не требуется, чтобы узлы в локальной сети использовали клиентское программное обеспечение PPPoE для подключения к Интернет-провайдеру.</p>
Subnet Mask (Маска подсети) (Только для инкапсуляции ENET ENCAP)	Введите маску подсети в десятичном формате с разделительными точками. Если требуется создание подсетей, см. Приложение С для расчета маски подсети.
ENET ENCAP Gateway (Шлюз ENET ENCAP) (Только для инкапсуляции ENET ENCAP)	Необходимо указать IP-адрес шлюза (предоставленный вашим Интернет-провайдером), если в поле Encapsulation (Инкапсуляция) установлен тип инкапсуляции ENET ENCAP .
Back (Назад)	Для возврата к предыдущему окну щелкните по кнопке Back (Назад) .

Табл. 12 Настройка подключения к глобальной сети (продолжение)

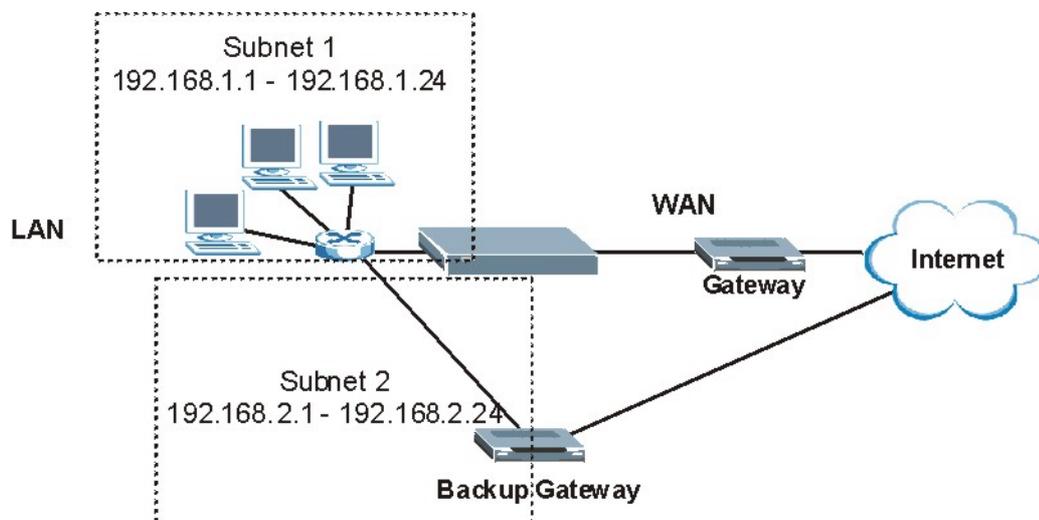
ПОЛЕ	ОПИСАНИЕ
Apply (Применить)	Щелкните Apply (Применить) для сохранения изменений.
Cancel (Отменить)	Щелкните по кнопке Cancel (Отменить) , чтобы заново начать настройку в этом окне.

6.7 Перенаправление трафика

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

Рис. 20 Пример перенаправления трафика

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

Рис. 21 Настройка локальной сети для перенаправления трафика

6.8 Настройка резервного подключения к глобальной сети

Для изменения настроек модема в отношении резервирования интерфейса WAN, щелкните **WAN (Глобальная сеть)**, затем **WAN Backup (Резервное подключение к глобальной сети)**. Появляется окно, представленное ниже.

Рис. 22 Резервное подключение к глобальной сети

WAN - WAN Backup Setup

Backup Type

Check WAN IP Address1

Check WAN IP Address2

Check WAN IP Address3

Fail Tolerance

Recovery Interval sec

Timeout sec

Traffic Redirect

Active

Metric

Backup Gateway

В следующей таблице даны описания полей этого окна.

Табл. 13 Резервное подключение к глобальной сети

ПОЛЕ	ОПИСАНИЕ
Backup Type (Тип резервирования)	<p>Выберите метод, который модем будет использовать для проверки соединения DSL.</p> <p>Выберите DSL Link (Канал DSL), чтобы модем проверял, установлено ли подключение к DSL-коммутатору. Выберите ICMP (Internet Control Message Protocol - Протокол межсетевых управляющих сообщений), чтобы модем периодически выполнял эхо-тестирование IP-адресов, установленных в полях Check WAN IP Address (Проверять IP-адреса глобальной сети).</p>
Check WAN IP Address1-3 (Проверять IP-адреса глобальной сети 1-3)	<p>Заполните эти поля, чтобы модем проверял доступность глобальной сети. Введите IP-адрес ближайшего надежного компьютера (например, адрес сервера DNS Интернет-провайдера).</p> <p>ПРИМЕЧАНИЕ: Если включена функция перенаправления трафика или резервного подключения, необходимо настроить по меньшей мере один IP-адрес.</p> <p>При использовании резервного подключения к глобальной сети, модем периодически проводит эхо-тестирование заданных в этом окне адресов и, если не получает ответа, использует другое резервное подключение к глобальной сети (если оно настроено).</p>
Fail Tolerance (Допустимое число отсутствий ответов)	<p>Введите число (рекомендуется 2), которое показывает сколько раз модем будет выполнять эхо-тестирование IP-адресов, установленных в поле Check WAN IP Address (Проверять IP-адреса глобальной сети) при отсутствии ответа, прежде чем переключиться на резервное подключение к глобальной сети (или другое резервное подключение к глобальной сети).</p>

Табл. 13 Резервное подключение к глобальной сети (продолжение)

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

ГЛАВА 7

Окна NAT (Трансляция сетевых адресов)

В данной главе описывается настройка функции NAT модема.

7.1 Обзор NAT

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

7.1.1 Определения NAT

Определение внутренний/внешний означает местоположение узла относительно модема, например, компьютеры абонентов являются внутренними узлами, тогда как web-серверы в Интернете являются внешними узлами.

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

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

Табл. 14 Определения NAT

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



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

7.1.2 Назначение NAT

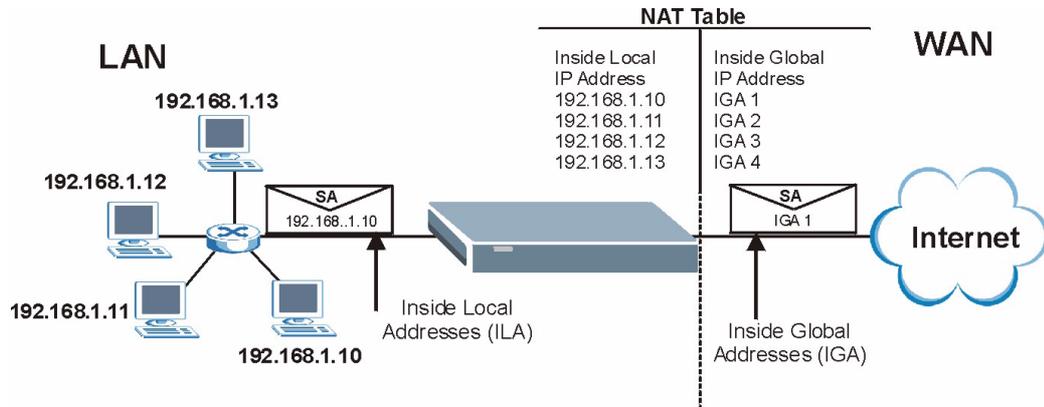
В простейшем случае, NAT изменяет IP-адрес источника в пакете, принятом от абонента (внутренний локальный адрес) на другой (внутренний глобальный адрес) перед передачей пакета в глобальную сеть. При получении ответа, NAT преобразовывает адрес назначения (внутренний глобальный адрес) обратно во внутренний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

Глобальные IP-адреса внутренних узлов могут быть статическими, или динамически назначаются Интернет-провайдером. Кроме того, вы можете определить серверы, например, web-сервер и сервер Telnet, находящиеся в вашей локальной сети, и сделать их доступными для внешних пользователей. Если вы не определили серверы (с отображением много-к-одному и много-ко-многим с перегрузкой – см. *Табл. 15*), NAT предлагает дополнительное преимущество защиты сети с помощью межсетевого экрана. Если серверы не определены, модем будет отфильтровывать все входящие запросы, предотвращая зондирование вашей сети злоумышленниками. Дополнительные сведения о трансляции IP-адресов см. Комментарий *RFC 1631, "Трансляция сетевых IP-адресов (NAT)"*.

7.1.3 Как работает NAT

Каждый пакет имеет два адреса – адрес источника и адрес назначения. Для исходящих пакетов, внутренний локальный адрес (ILA) является адресом источника в локальной сети, а внутренний глобальный адрес (IGA) - адресом источника в глобальной сети. Для входящих пакетов, ILA - это адрес назначения в локальной сети, а IGA - адрес назначения в глобальной сети. NAT преобразовывает частные (локальные) IP-адреса в уникальные глобальные, что необходимо для связи с узлами в других сетях. NAT заменяет исходный IP-адрес источника (и номера портов источника TCP или UDP на отображение много-к-одному и много-ко-многим с перегрузкой) в каждом пакете и затем пересылает его в Интернет. Модем сохраняет исходные адреса и номера портов, чтобы можно было восстановить исходные значения во входных ответных пакетах. Это проиллюстрировано на следующем рисунке.

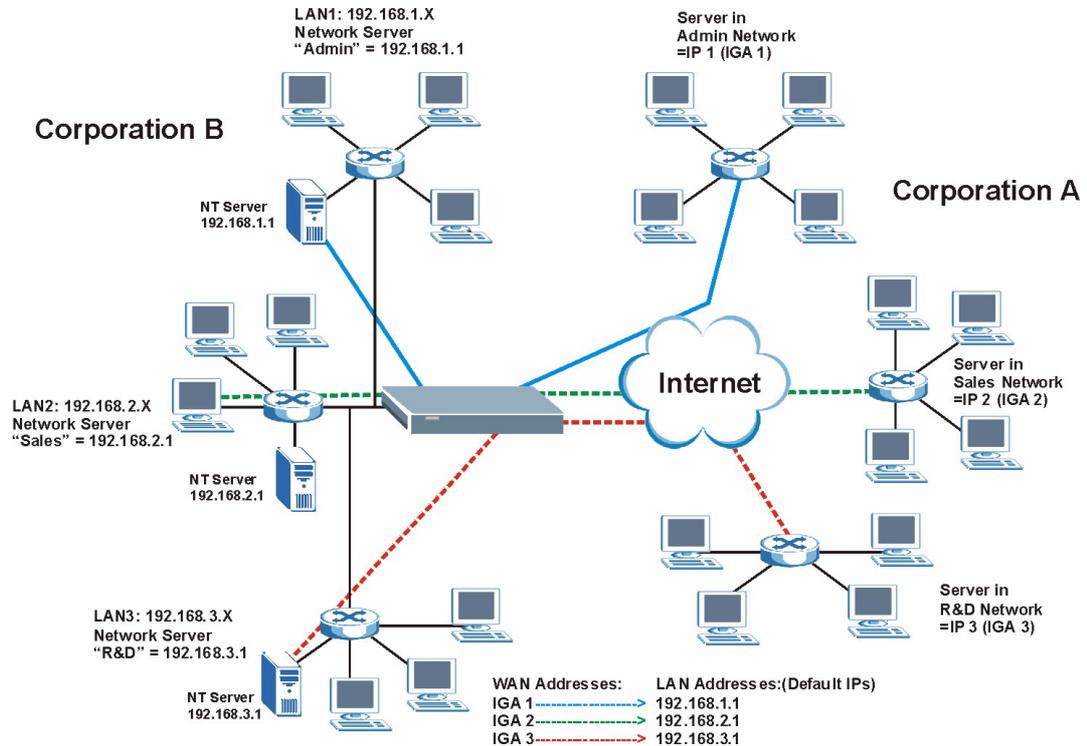
Рис. 23 Как работает NAT



7.1.4 Применение NAT

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

Рис. 24 Применение NAT с использованием псевдонимов IP



7.1.5 Типы отображения NAT

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

- **One to One (Один-к-одному):** В режиме один-к-одному, модем отображает один локальный IP-адрес на один глобальный IP-адрес.
- **Many to One (Много-к-одному):** В режиме много-к-одному, модем отображает несколько локальных IP-адресов на один глобальный IP-адрес. Эта функция эквивалентна SUA (например, PAT - Port Address Translation - Преобразование адресов портов), т.е. функции ZyXEL "Учетная запись одиночного пользователя", которая поддерживалась в предыдущих моделях маршрутизаторов ZyXEL (опция **SUA Only (Только SUA)** в современных маршрутизаторах).
- **Many to Many Overload (Много-ко-многим с перегрузкой):** В режиме много-ко-многим с перегрузкой, модем отображает множество локальных IP-адресов в несколько совместно используемых глобальных IP-адресов.
- **Many-to-Many No Overload (Много-ко-многим без перегрузки):** В режиме много-ко-многим без перегрузки, модем отображает каждый локальный IP-адрес в уникальный глобальный IP-адрес.

- **Server (Сервер)** Этот режим позволяет определить внутренние серверы для различных служб, находящихся за NAT, и сделать их доступными для внешних пользователей.



ПРИМЕЧАНИЕ: Номера портов **не** изменяются при использовании типов отображения NAT **один-к-одному** и **много-ко-многим без перегрузки**.

В следующей таблице приведена сводная информация о типах NAT.

Табл. 15 Типы отображения NAT

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

7.2 Сравнение SUA (Учетная запись одиночного пользователя) и NAT

SUA (Single User Account - Учетная запись одиночного пользователя) - это реализация в операционной системе ZyNOS подмножества NAT, которое поддерживает два типа отображения, **много-к-одному** и **сервер**. Модем кроме этого поддерживает **Full Feature (Полный набор функциональных возможностей)** NAT для отображения нескольких глобальных IP-адресов на несколько частных локальных IP-адресов клиентов или серверов с использованием типов отображения, как показано в [Табл. 15](#).



ПРИМЕЧАНИЕ: 1. Выбирайте **SUA Only (Только SUA)**, если модем имеет только один общедоступный IP-адрес в глобальной сети. 2. Выбирайте **Full Feature (Полный набор функциональных возможностей)**, если модем имеет несколько общедоступных IP-адресов в глобальной сети.

7.3 Сервер SUA

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

Вы можете указать для переадресации один номер порта или диапазон номеров портов, а также локальный IP-адрес требуемого сервера. Номер порта идентифицирует службу; например, служба web имеет порт 80, а FTP - порт 21. В некоторых случаях, когда служба неизвестна или один сервер поддерживает более одной службы (например, FTP и web), лучше указать диапазон номеров портов. Вы можете назначить IP-адрес сервера, который соответствует порту или диапазону портов.

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

7.3.1 IP-адрес сервера по умолчанию

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



ПРИМЕЧАНИЕ: Если вы не назначили IP-адрес для **Server Set 1 (Набор серверов 1)** (сервер по умолчанию) то модем будет отбрасывать все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

7.3.2 Переадресация портов: Службы и номера портов

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

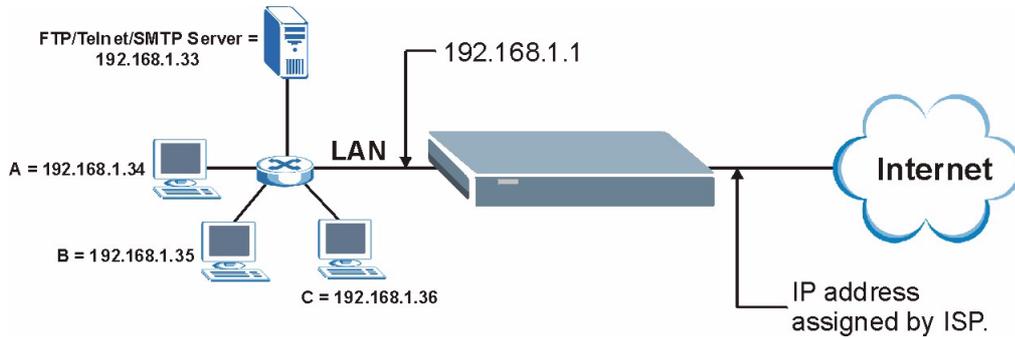
Табл. 16 Службы и номера портов

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

7.3.3 Настройка серверов, расположенных за SUA (Пример)

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

Рис. 25 Пример: Несколько серверов расположены за NAT



7.4 Выбор режима NAT

Щелкните **NAT** для отображения следующего окна.

Рис. 26 Режим NAT

NAT - Mode

Network Address Translation

None
 SUA Only [Edit Details](#)
 Full Feature [Edit Details](#)

В следующей таблице даны описания полей этого окна.

Табл. 17 Режим NAT

ПОЛЕ	ОПИСАНИЕ
None (Отключить)	Выберите эту опцию для отключения NAT.
SUA Only (Только SUA)	Выберите эту опцию, если модем имеет только один общедоступный IP-адрес в глобальной сети. Модем будет использовать Набор отображения адресов 1, установленный в окне NAT - Edit SUA/NAT Server Set (Редактировать набор серверов SUA/NAT) .
Edit Details (Редактировать параметры)	Щелкните по этой ссылке для перехода к окну NAT - Edit SUA/NAT Server Set (Редактировать набор серверов SUA/NAT) .

Табл. 17 Режим NAT (продолжение)

ПОЛЕ	ОПИСАНИЕ
Full Feature (Полный набор функциональных возможностей)	Выберите эту опцию, если модем имеет несколько общедоступных IP-адресов в глобальной сети.
Edit Details (Редактировать параметры)	Щелкните по этой ссылке для перехода к окну NAT - Address Mapping Rules (Правила отображения адресов) .
Apply (Применить)	Щелкните по кнопке Apply (Применить) для сохранения конфигурации.

7.5 Настройка сервера SUA



ПРИМЕЧАНИЕ: Если вы не назначили IP-адрес для **Набора серверов 1** (сервер по умолчанию), то модем будет отбрасывать все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

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

См. [Табл. 16](#) для справки по номерам портов, обычно используемых для конкретных служб.

Рис. 27 Редактировать набор серверов SUA/NAT

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

Save Cancel

В следующей таблице даны описания полей этого окна.

Табл. 18 Редактировать набор серверов SUA/NAT

ПОЛЕ	ОПИСАНИЕ
Start Port No. (Номер начального порта)	Введите в это поле номер порта. Для пересылки пакетов только одного порта, введите его номер еще раз в поле End Port No (Номер последнего порта) . Для пересылки пакетов ряда портов, введите здесь номер начального порта, а номер последнего порта в поле End Port No. (Номер последнего порта) .
End Port No. (Номер последнего порта)	Введите в это поле номер порта. Для пересылки пакетов только одного порта, введите его номер еще раз в поле Start Port No. (Номер начального порта) расположенное выше, и затем введите этот номер еще раз в это поле. Для пересылки пакетов ряда портов, введите здесь номер последнего порта в серии портов с начальным номером, указанным в поле Start Port No. (Номер начального порта) .
IP Address (IP-адрес)	Введите в этом поле IP-адрес сервера.
Save (Сохранить)	Щелкните по кнопке Save (Сохранить) для сохранения конфигурации модема.
Cancel (Отменить)	Щелкните по кнопке Cancel (Отменить) , чтобы вернуться к предыдущей конфигурации.

7.6 Настройка правил отображения адресов

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

Для изменения настроек отображения адресов модема, щелкните **NAT**, выберите **Full Feature (Полный набор функциональных возможностей)** и затем щелкните по ссылке **Edit Details (Редактировать параметры)**, чтобы отобразить следующее окно.

Рис. 28 Правила отображения адресов

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

Back

В следующей таблице даны описания полей этого окна.

Табл. 19 Правила отображения адресов

ПОЛЕ	ОПИСАНИЕ
Local Start IP (Начальный локальный IP-адрес)	Это начальный внутренний локальный IP-адрес (ILA). Локальные IP-адреса недоступны для типа отображения портов Server (Сервер) .
Local End IP (Конечный локальный IP-адрес)	Это конечный внутренний локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, то в поле Local Start IP (Начальный локальный IP-адрес) отображается 0.0.0.0, а в поле Local End IP (Конечный локальный IP-адрес) отображается 255.255.255.255. В этом поле отображается N/A (Не применяется) для типов отображения один-к-одному и сервер .

Табл. 19 Правила отображения адресов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Global Start IP (Начальный глобальный IP- адрес)	Это начальный внутренний глобальный IP-адрес (IGA). Если у вас динамический IP-адрес, назначаемый Интернет-провайдером, введите 0.0.0.0 в этом поле. В этом случае используются только отображения много-к-одному и сервер .
Global End IP (Конечный глобальный IP- адрес)	Это конечный внутренний глобальный IP-адрес (IGA). В этом поле индицируется N/A (Не применяется) для типов отображения один-к-одному , много-к-одному и сервер .
Типе (Тип)	<p>1-1: В режиме один-к-одному один локальный IP-адрес отображается на один глобальный IP-адрес. Следует отметить, что в режиме отображения NAT один-к-одному номера портов не изменяются.</p> <p>M-1: В режиме много-к-одному несколько локальных IP-адресов отображаются на один глобальный IP-адрес. Этот режим аналогичен SUA (т.е., PAT, port address translation - преобразование адресов портов), функции ZyXEL "Учетная запись одиночного пользователя", которую поддерживали предыдущие модели маршрутизаторов ZyXEL.</p> <p>M-M Ov (Overload): В режиме много-ко-многим с перегрузкой несколько локальных IP-адресов отображаются на несколько совместно используемых глобальных IP-адресов.</p> <p>MM No (No Overload): В режиме много-ко-многим без перегрузки каждый локальный IP-адрес отображается на уникальный глобальный IP-адрес.</p> <p>Server: Этот режим позволяет определить внутренние серверы для различных служб, находящихся за NAT, и сделать их доступными для внешних пользователей.</p>
Back (Назад)	Щелкните по кнопке Back (Назад) для возврата к окну NAT Mode (Режим NAT) .

7.7 Редактирование правил отображения адресов

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

Рис. 29 Редактирование правил отображения адресов

NAT - Edit Address Mapping Rule 1

Type: One-to-One

Local Start IP: 0.0.0.0

Local End IP: N/A

Global Start IP: 0.0.0.0

Global End IP: N/A

Server Mapping Set: N/A [Edit Details](#)

Apply Cancel Delete

В следующей таблице даны описания полей этого окна.

Табл. 20 Редактирование правил отображения адресов

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	<p>Выберите тип отображения портов из следующих вариантов.</p> <ul style="list-style-type: none"> • One-to-One (Один-к-одному): В режиме один-к-одному один локальный IP-адрес отображается на один глобальный IP-адрес. Следует отметить, что в режиме отображения NAT один-к-одному номера портов не изменяются. • Many-to-One (Много к одному): В режиме много-к-одному несколько локальных IP-адресов отображаются на один глобальный IP-адрес. Этот режим аналогичен SUA (т.е., PAT, port address translation - преобразование адресов портов), функции ZyXEL "Учетная запись одиночного пользователя", которую поддерживали предыдущие модели маршрутизаторов ZyXEL. • Many-to-Many Overload (Много-ко-многим с перегрузкой): В режиме много-ко-многим с перегрузкой несколько локальных IP-адресов отображаются на несколько совместно используемых глобальных IP-адресов. • Many-to-Many No Overload (Много-ко-многим без перегрузки): В режиме много-ко-многим без перегрузки каждый локальный IP-адрес отображается на уникальный глобальный IP-адрес. • Server (Сервер): Этот режим позволяет определить внутренние серверы для различных служб, находящихся за NAT, и сделать их доступными для внешних пользователей.
Local Start IP (Начальный локальный IP-адрес)	Это начальный локальный IP-адрес (ILA). Локальные IP-адреса недоступны для типа отображения портов Server (Сервер) .
Local End IP (Конечный локальный IP-адрес)	<p>Это конечный локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, то в поле Local Start IP (Начальный локальный IP-адрес) введите 0.0.0.0, а в поле Local End IP (Конечный локальный IP-адрес) введите 255.255.255.255.</p> <p>В этом поле индицируется N/A (Не применяется) для типов отображения один-к-одному и сервер.</p>

Табл. 20 Редактирование правил отображения адресов (продолжение)

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

ГЛАВА 8

Настройка динамической DNS

В этой главе описывается настройка модема для использования динамической DNS.

8.1 Динамическая система доменных имен

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

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

8.1.1 Шаблоны DYNDNS

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



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

8.2 Настройка динамической DNS

Для изменения функции DDNS модема, щелкните **Dynamic DNS (Динамическая DNS)**. Появляется окно, представленное ниже.

Рис. 30 Динамическая система доменных имен (Dynamic DNS)

Dynamic DNS

Active

Service Provider: WWW.DynDNS.ORG

Host Name: _____

E-mail Address: _____

User: _____

Password: _____

Enable Wildcard

Apply Cancel

В следующей таблице даны описания полей этого окна.

Табл. 21 Динамическая система доменных имен

ПОЛЕ	ОПИСАНИЕ
Active (Включить)	Установите флажок в этом окошке для использования динамической службы доменных имен.
Service Provider (Провайдер услуг)	Это имя провайдера услуг динамической DNS.
Host Names (Имя узла)	Введите доменное имя, назначенное модему провайдером услуг динамической DNS.
E-mail Address (Адрес электронной почты)	Введите адрес электронной почты.
User (Пользователь)	Введите имя пользователя.
Password (Пароль)	Введите назначенный пароль.
Enable Wildcard (Включить шаблоны)	Установите флажок в этом окошке для включения шаблонов DYNDNS.
Apply (Применить)	Щелкните по кнопке Apply (Применить) для сохранения конфигурации модема.
Cancel (Отменить)	Щелкните по кнопке Cancel (Отменить) , чтобы заново начать настройку в этом окне.

ГЛАВА 9

Время и дата

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

9.1 Установка времени и даты

Для изменения времени и даты в модеме, щелкните **Time And Date (Время и дата)**. Появляется окно, представленное ниже. Это окно используется для установки времени в модеме в соответствии с вашим часовым поясом.

Рис. 31 Время и дата

Time and Date

Time Server

Use Protocol when Bootup: None

IP Address or URL: N/A

Time and Date: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Daylight Savings

Start Date: 1 month 1 day

End Date: 1 month 1 day

Synchronize system clock with Time Server now.
(This may take up to 60 seconds.)

Date

Current Date: 2000-01-01

New Date (yyy-mm-dd): 2000-01-01

Time

Current Time: 01:10:51

New Time: 01:10:51

Apply Cancel

В следующей таблице даны описания полей этого окна.

Табл. 22 Время и дата

ПОЛЕ	ОПИСАНИЕ
Time Server (Сервер точного времени)	
Use Protocol when Bootup (Использовать протокол при загрузке)	<p>Введите сервисный протокол, с помощью которого ваш сервер времени посылает данные при включении модема. Не все серверы времени поддерживают все протоколы, поэтому следует проконсультироваться с Интернет-провайдером/сетевым администратором, или попытаться определить работающий протокол методом проб и ошибок.</p> <p>Основные различия между ними заключаются в формате представления времени.</p> <p>Формат Daytime (RFC 867) содержит день/месяц/год/часовой пояс сервера.</p> <p>Формат Time (RFC 868) представляет собой 4-байтовое целое число, означающее общее количество секунд, истекшее с даты 1970/1/1 на 0:0:0.</p> <p>Формат NTP (RFC 1305) аналогичен формату Time (RFC 868).</p> <p>Выберите None (Нет) для установки времени и даты вручную.</p>
IP Address or URL (IP-адрес или URL)	Введите IP-адрес или URL сервера времени. Если вы не обладаете этой информацией, следует обратиться к Интернет-провайдеру/сетевому администратору.
(Time and Date) Время и дата	Выберите часовой пояс вашего местонахождения. Это поле устанавливает разницу между вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time - GMT).
Daylight Savings (Переход на летнее время)	Выберите эту опцию, если вы используете переход на летнее время. Летнее время - это период с поздней весны до ранней осени, когда во многих странах стрелки часов переводятся на час вперед, чтобы добавить час светлого времени суток.
Start Date (Начальная дата)	Введите месяц и день, когда начинается летнее время, если выбрана опция Daylight Savings (Переход на летнее время) .
End Date (Конечная дата)	Введите месяц и день, когда заканчивается летнее время, если выбрана опция Daylight Savings (Переход на летнее время) .
Synchronize system clock with Time Server now (Синхронизировать системные часы с сервером времени).	Выберите эту опцию, чтобы модем использовал время от сервера времени (настроенного выше) для установки своих внутренних системных часов. Пожалуйста, подождите около 60 секунд, пока модем обнаружит сервер времени. Если модем не смог обнаружить сервер времени, проверьте используемый сервисный протокол и IP-адрес сервера времени. Если IP-адрес установлен правильно, протестируйте соединение, например, с помощью команды "ping".
Date (Дата)	
Current Date (Текущая дата)	В этом поле отображается дата в модеме. Каждый раз при загрузке этой страницы, модем синхронизирует время с сервером времени.
New Date (уууу-мм-дд) (Новая дата (гггг-мм-дд))	В этом поле отображается последняя обновленная дата от сервера времени. Если в поле Use Protocol when Bootup (Использовать протокол при загрузке) установлено None (Нет) , введите вручную новую дату в этом поле и затем щелкните Apply (Применить) .
Time (Время)	
Current Time (Текущее время)	В этом поле отображается время в модеме. Каждый раз при загрузке этой страницы, модем синхронизирует время с сервером времени.

Табл. 22 Время и дата (продолжение)

ПОЛЕ	ОПИСАНИЕ
New Time (Новое время)	В этом поле отображается последнее обновленное время от сервера времени. Если в поле Use Protocol when Bootup (Использовать протокол при загрузке) установлено None (Нет) , введите ручную новое время в этом поле и затем щелкните Apply (Применить) .
Apply (Применить)	Щелкните по кнопке Apply (Применить) для сохранения конфигурации модема.
Cancel (Отменить)	Щелкните по кнопке Cancel (Отменить) , чтобы заново начать настройку в этом окне.

ГЛАВА 10

Настройка удаленного управления

В этой главе предоставлена информация для настройки удаленного управления модемом.

10.1 Обзор удаленного управления

Функция удаленного управления позволяет определить компьютеры и протоколы, по которым разрешен доступ к интерфейсу управления модема.

Вы можете удаленно управлять модемом:

- через Интернет (только через глобальную сеть)
- отовсюду (через локальную и глобальную сеть)
- только через локальную сеть
- никак (функция отключена).

Для отключения удаленного управления с использованием конкретной службы, выберите **Disable (Отключить)** в поле **Server Access (Доступ к серверу)** при использовании SMT или **Access Status (Состояние доступа)** при использовании Web-конфигуратора для соответствующей службы.

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

- 1 Telnet
- 2 HTTP

10.1.1 Ограничения на удаленное управление

Удаленное управление со стороны локальной или глобальной сети не будет работать, если:

- Применен фильтр для блокировки службы Telnet, FTP или Web в меню SMT 3.1 (локальная сеть) или в меню 11.5 (глобальная сеть).

- Эта служба отключена в окне настройки удаленного управления.
- IP-адрес, установленный в поле **Secured Client IP (IP-адрес доверенного клиента)** не совпадает с IP-адресом клиента. В случае несовпадения адресов модем немедленно завершает сеанс управления.
- Уже выполняется другой сеанс удаленного управления, имеющий равный или более высокий приоритет. Одновременно допускается проведение только одного сеанса удаленного управления.

10.1.2 Удаленное управление и NAT

При включении функции NAT:

- Если удаленное управление осуществляется через глобальную сеть, необходимо использовать IP-адрес модема в глобальной сети.
- Если удаленное управление осуществляется через локальную сеть, необходимо использовать IP-адрес модема в локальной сети.

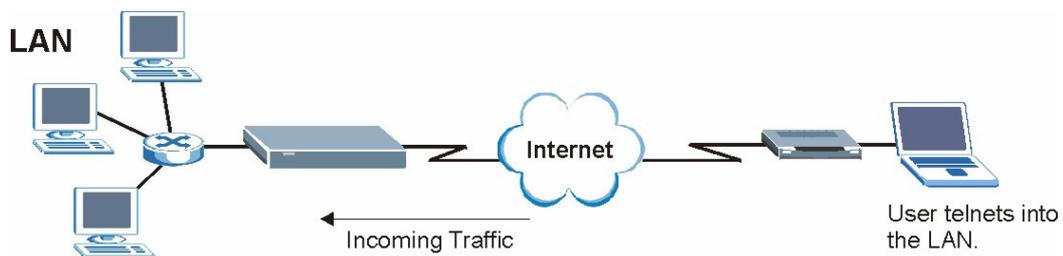
10.1.3 Время бездействия системы

Интервал бездействия системы во время сеанса управления по умолчанию установлен 5 минут (300 секунд). Модем автоматически завершает сеанс управления при бездействии более этого периода. Сеанс управления не разрывается, если в окне статистики проводится опрос системы.

10.2 Управление с помощью Telnet

Можно настроить удаленный доступ к модему с использованием протокола Telnet, как показано ниже.

Рис. 32 Настройка Telnet в сети TCP/IP



10.3 FTP

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

10.4 Web

Для настройки и управления файлами можно использовать встроенный Web-конфигуратор модема. Более подробно см. встроенную справку.

10.5 Настройка удаленного управления

Щелкните **Remote Management (Удаленное управление)** для отображения следующего окна.

Рис. 33 Удаленное управление

Server Type	Access Status	Port	Secured Client IP
Telnet	All	23	0.0.0.0
FTP	All	21	0.0.0.0
Web	All	80	0.0.0.0

Apply Cancel

В следующей таблице даны описания полей этого окна.

Табл. 23 Удаленное управление

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

ГЛАВА 11

Универсальная функция Plug and Play (UPnP)

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

11.1 Описание универсальной функции Plug and Play

Универсальная функция Plug and Play (UPnP) - это распределенный открытый сетевой стандарт, использующий TCP/IP для обеспечения взаимодействия между устройствами в одноранговой сети. Устройство UPnP может динамически подключаться к сети, получать IP-адрес, предоставлять свои ресурсы и собирать информацию о других устройствах сети. Кроме того, устройство может беспрепятственно и автоматически покидать сеть, если оно больше не используется.

11.1.1 Как узнать, используется ли UPnP?

Оборудование UPnP идентифицируется иконкой в папке Network Connections (Сетевые подключения) (Windows XP). Каждое совместимое с UPnP устройство, установленное в сети, появляется в виде отдельной иконки. Выбор иконки устройства UPnP позволяет получить доступ к информации и свойствам данного устройства.

11.1.2 NAT Traversal

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

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

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

Для получения более подробной информации о NAT см. [Глава 7 Окна NAT \(Трансляция сетевых адресов\)](#).

11.1.3 Предупреждения по использованию UPnP

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

Все устройства с включенной функцией UPnP могут свободно взаимодействовать друг с другом без дополнительной настройки. Отключите функцию UPnP, если это не входит в ваши намерения.

11.2 UPnP и ZyXEL

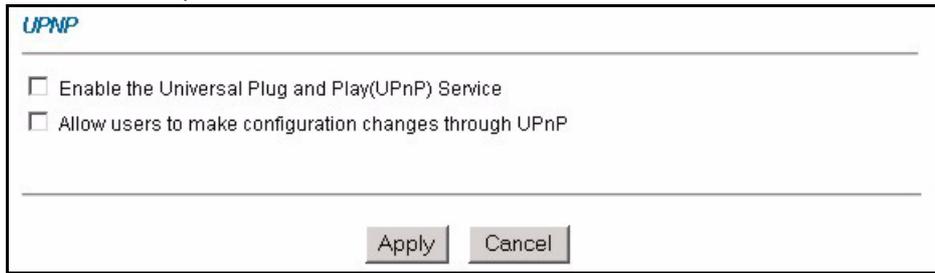
Корпорация ZyXEL получила сертификат UPnP от форума Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). Реализация UPnP ZyXEL поддерживает функцию IGD 1.0 (Internet Gateway Device - устройство-шлюз Интернет). На момент написания документа реализация ZyXEL UPnP поддерживает Windows Messenger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

Широковещательные рассылки UPnP допускаются только внутри локальной сети.

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

11.2.1 Настройка UPnP

В окне **Site Map (Карта сайта)** в Главном меню, щелкните **UPnP** под разделом **Advanced Setup (Дополнительная настройка)** для отображения представленного ниже окна.

Рис. 34 Настройка UPnP

В следующей таблице даны описания полей этого окна.

Табл. 24 Настройка UPnP

ПОЛЕ	ОПИСАНИЕ
Enable the Universal Plug and Play (UPnP) Service (Включить службу UPnP)	Установите флажок в этом окошке для включения UPnP. Помните, что каждый может использовать приложение UPnP, чтобы открыть окно регистрации Web-конфигуратора, не вводя IP-адрес модема (хотя для доступа к Web-конфигуратору необходимо ввести пароль).
Allow users to make configuration changes through UPnP (Разрешить пользователям вносить изменения в конфигурацию через UPnP)	Установите флажок в этом окошке, чтобы разрешить приложениям UPnP автоматически настраивать модем с целью взаимодействия через него. Например, при использовании NAT Transversal, приложения UPnP автоматически резервируют порт переадресации NAT, чтобы иметь возможность взаимодействовать с другим устройством UPnP; это предотвращает необходимость ручной настройки переадресации портов для приложения UPnP.
Apply (Применить)	Щелкните Apply (Применить) для сохранения конфигурации модема.
Cancel (Отменить)	Щелкните по кнопке Cancel (Отменить) для возврата к предыдущим сохраненным настройкам.

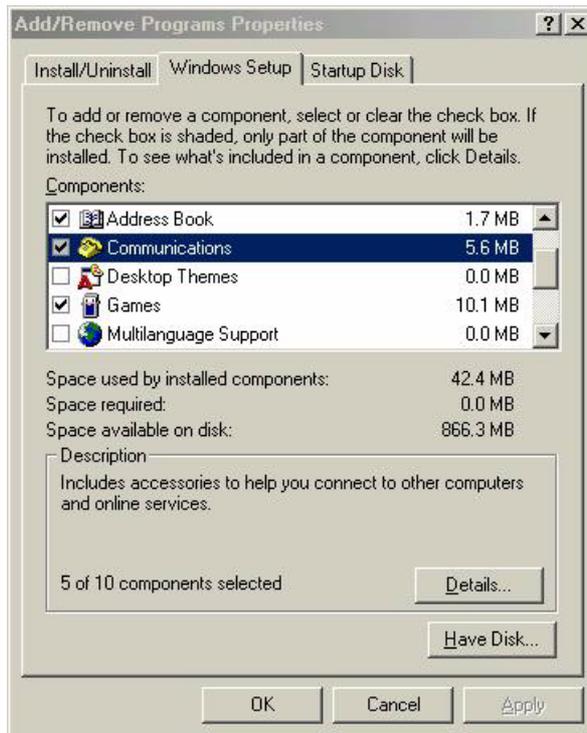
11.3 Пример установки UPnP в Windows

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

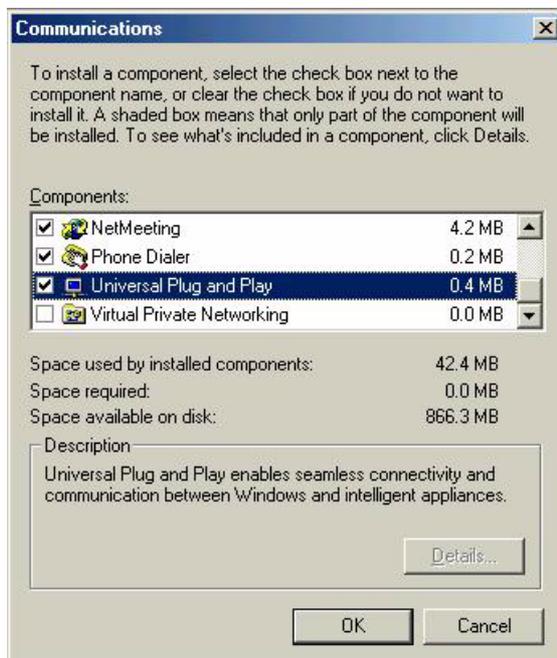
Установка UPnP в Windows Me

Выполните следующие действия для установки UPnP в Windows Me.

- 1 Щелкните **Start (Пуск)**, **Control Panel (Панель управления)**. Дважды щелкните **Add/Remove Programs (Установка и удаление программ)**.
- 2 Щелкните закладку **Windows Setup (Установка Windows)** и выберите **Communication (Связь)** в поле **Components (Компоненты)**. Щелкните **Details (Дополнительно)**.

Рис. 35 Установка и удаление программ: Установка Windows: Связь

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

Рис. 36 Установка и удаление программ: Установка Windows: Связь: Компоненты

4 Щелкните **ОК** для возврата в окно **Add/Remove Programs Properties (Свойства установки/удаления программ)** и щелкните **Next (Далее)**.

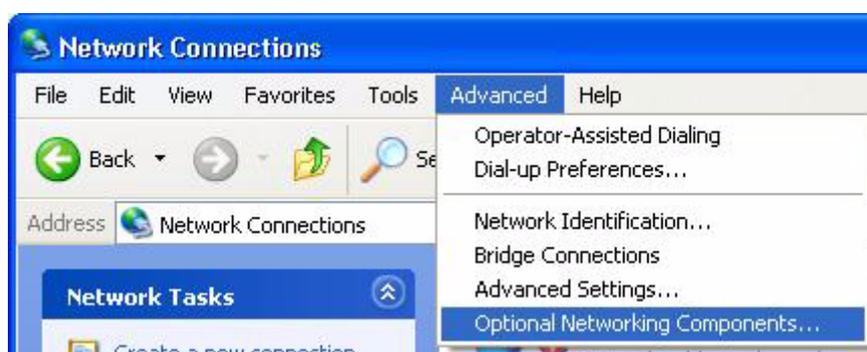
5 При появлении запроса перезагрузите компьютер.

Установка UPnP в Windows XP

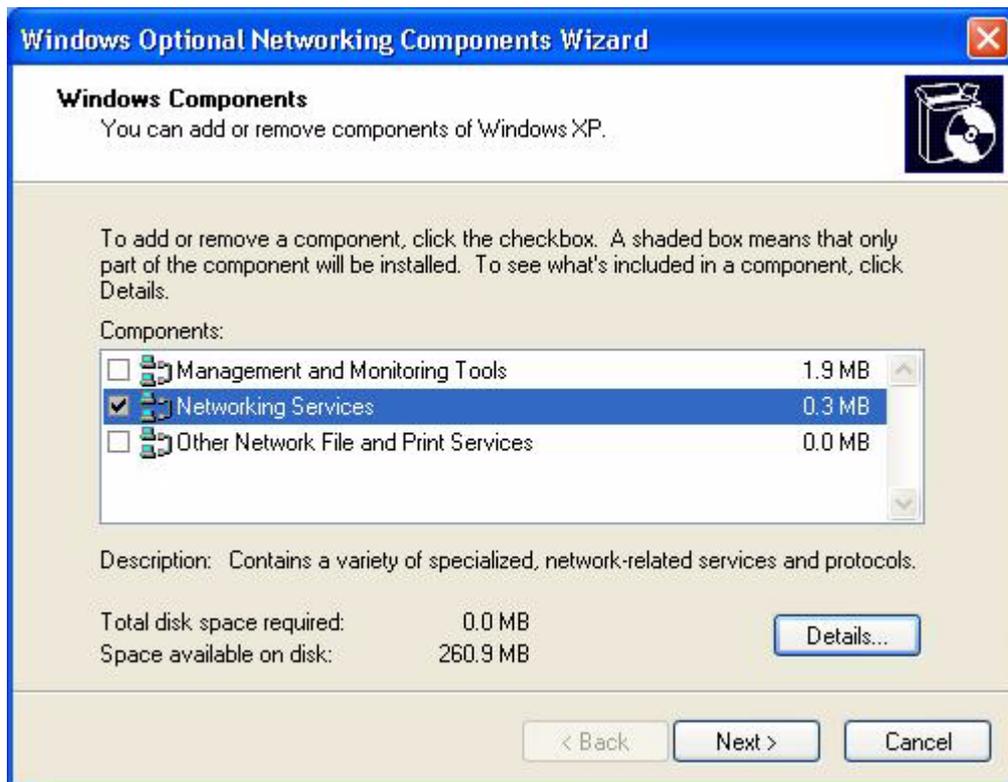
Выполните следующие действия для установки UPnP в Windows XP.

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

Рис. 37 Сетевые подключения

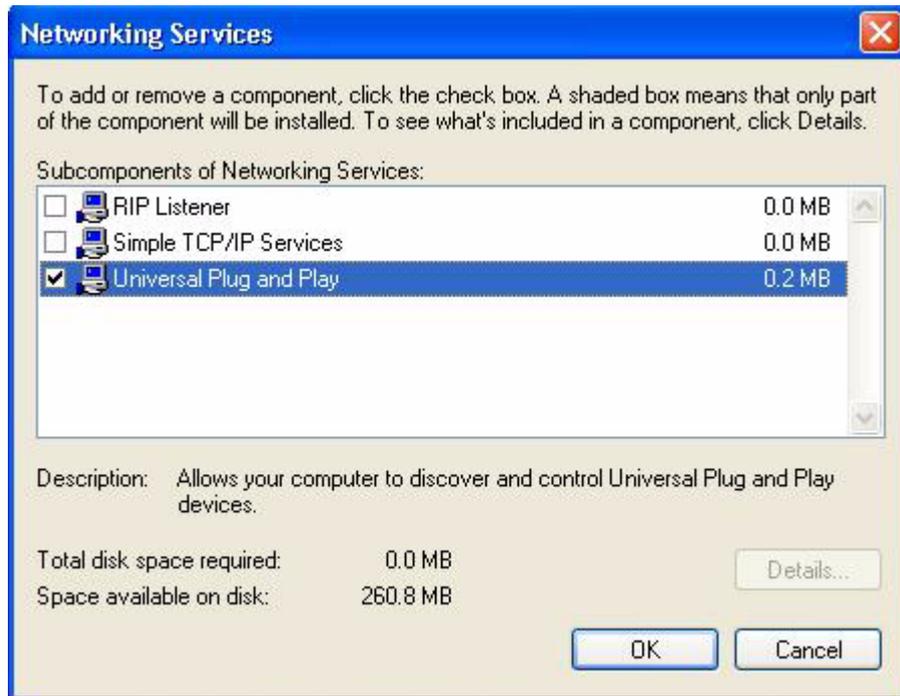


- 4 Появляется окно **Windows Optional Networking Components Wizard (Мастер установки дополнительных сетевых компонентов Windows)**. Выберите **Networking Services (Сетевые службы)** в поле **Components (Компоненты)** и щелкните **Details (Дополнительно)**.

Рис. 38 Мастер установки дополнительных компонентов Windows

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

Рис. 39 Сетевые службы



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

11.4 Пример использования UPnP в Windows XP

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

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

Автоматическое обнаружение сетевого устройства UPnP

- Щелкните **Start (Пуск)**, **Control Panel (Панель управления)**. Дважды щелкните **Network Connections (Сетевые подключения)**. В разделе Internet Gateway (Шлюз в Интернет) отображается иконка.
- Щелкните правой кнопкой мыши на этой иконке и выберите **Properties (Свойства)**.

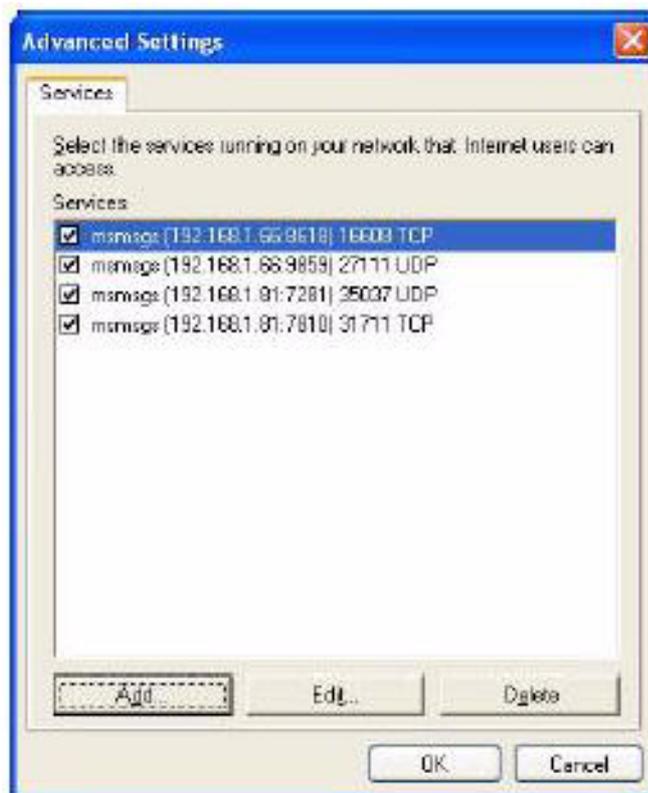
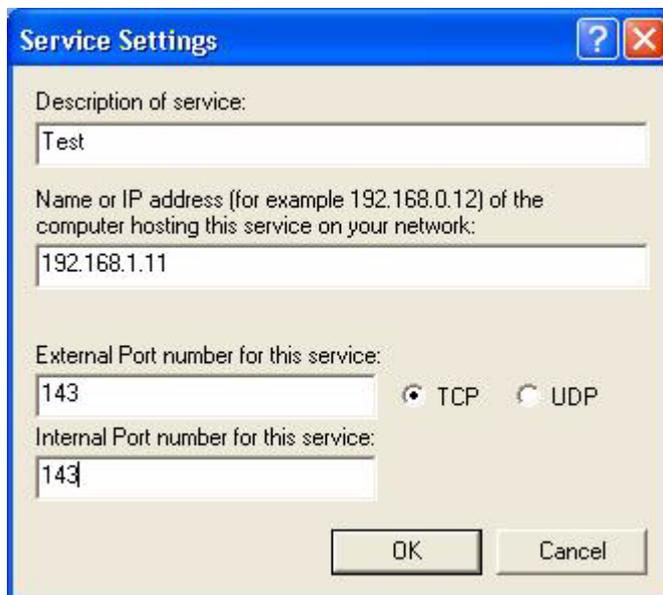
Рис. 40 Сетевые подключения



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

Рис. 41 Свойства подключения к Интернет

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

Рис. 42 Свойства подключения к Интернет: Дополнительные настройки**Рис. 43** Свойства подключения к Интернет: Дополнительные настройки: Добавить

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

- 6** Выберите **Show icon in notification area when connected (Отображать значок в строке состояния при подключении)** и щелкните **ОК**. В системной панели отображается значок.

Рис. 44 Значок в системной панели



- 7** Дважды щелкните иконку для отображения текущего состояния подключения к Интернету.

Рис. 45 Состояние подключения к Интернет



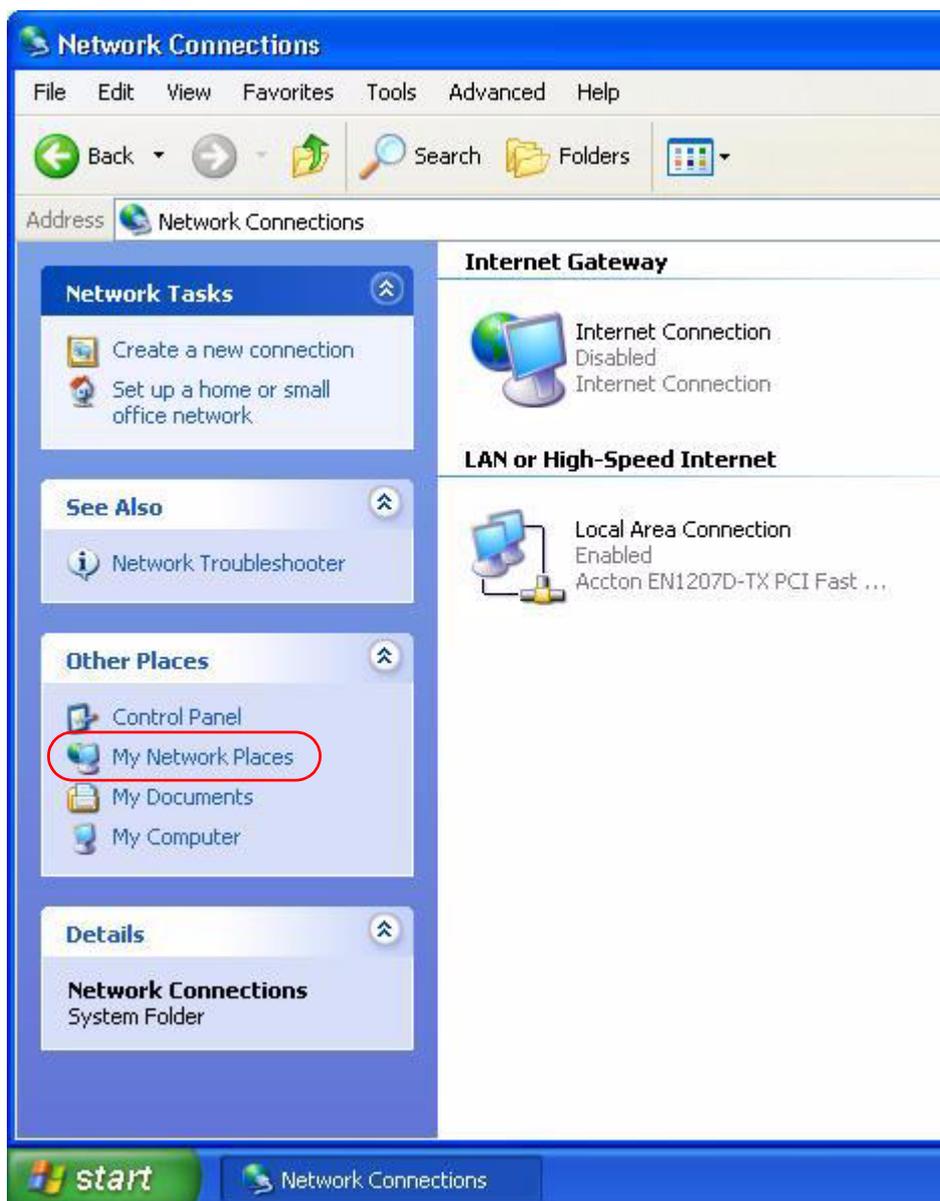
Простой доступ к Web-конфигуратору

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

Выполните следующие действия для доступа к Web-конфигуратору.

- 1** Щелкните **Start (Пуск)**, **Control Panel (Панель управления)**.
- 2** Дважды щелкните на **Network Connections (Сетевые подключения)**.
- 3** Выберите **My Network Places (Мое сетевое окружение)** в разделе **Other Places (Другие места)**.

Рис. 46 Сетевые подключения



- 4 В разделе **Local Network (Локальная сеть)** для каждого UPnP-совместимого устройства отображается иконка с описанием.
- 5 Щелкните правой кнопкой мыши на иконке модема и выберите **Invoke (Запуск)**. Появится окно регистрации Web-конфигуратора.

Рис. 47 Сетевые подключения: Мое сетевое окружение

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

Рис. 48 Сетевые подключения: Мое сетевое окружение: Свойства: Пример

ГЛАВА 12

Сопровождение

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

12.1 Описание обслуживания

Окна для обслуживания устройства служат для просмотра информации о системе, загрузки новой микропрограммы, управления конфигурацией и перезапуска модема.

12.2 Окно Состояние системы

Щелкните **System Status (Состояние системы)** для отображения представленного ниже окна, которое используется для контроля текущего состояния модема. Следует отметить, что поля в этом окне отображаются в режиме ТОЛЬКО ДЛЯ ЧТЕНИЯ и используются только в целях диагностики.

Рис. 49 Состояние системы

System Status

System Status

System Name:
 ZyNOS FW Version: V3.40(UF.0)b1 | 9/28/2004
 DSL FW Version: TI AR7 01.01.08.00
 Standard: NORMAL

WAN Information

IP Address: 0.0.0.0
 IP Subnet Mask: 0.0.0.0
 Default Gateway: 0.0.0.0
 VPI/VCI: 8/ 35

LAN Information

MAC Address: 00:a0:c5:01:23:45
 IP Address: 192.168.1.1
 IP Subnet Mask: 255.255.255.0
 DHCP: Server
 DHCP Start IP: 192.168.1.33
 DHCP Pool Size: 32

В следующей таблице даны описания полей этого окна.

Табл. 25 Состояние системы

ПОЛЕ	ОПИСАНИЕ
System Status (Состояние системы)	
System Name (Системное имя)	В этом поле отображается имя модема, которое используется в целях идентификации.
ZyNOS Firmware Version (Версия ПО ZyNOS)	Здесь отображается версия микропрограммы ZyNOS, а также дата ее создания. ZyNOS - это собственная разработка сетевой операционной системы ZyXEL.
DSL FW Version (Версия ПО DSL)	Здесь отображается версия микропрограммы DSL для модема.
Standard (Стандарт)	Здесь отображается стандарт, используемый модемом.

Табл. 25 Состояние системы (продолжение)

ПОЛЕ	ОПИСАНИЕ
WAN Information (Параметры глобальной сети)	
IP Address (IP-адрес)	Здесь отображается IP-адрес порта WAN.
IP Subnet Mask (Маска IP подсети)	Здесь отображается маска IP подсети для порта WAN.
Default Gateway (Шлюз по умолчанию)	Здесь отображается IP-адрес шлюза по умолчанию, если он применяется.
VPI/VCI	Здесь отображаются номера Идентификатора виртуального пути (VPI) и Идентификатора виртуального канала (VCI), которые установлены в первом окне Мастера установки.
LAN Information (Параметры локальной сети)	
MAC Address (MAC-адрес)	В этом поле отображается уникальный MAC-адрес (Media Access Control - Управление доступом к среде) или Ethernet адрес модема.
IP Address (IP-адрес)	Здесь отображается IP-адрес порта LAN.
IP Subnet Mask (Маска IP подсети)	Здесь отображается маска IP подсети для порта LAN.
DHCP	Здесь отображается режим DHCP порта WAN - Server (Сервер) , Relay (Ретранслятор) (не во всех моделях) или None (Отключить) .
DHCP Start IP (Начальный IP-адрес диапазона DHCP)	Здесь устанавливается первый адрес из непрерывного диапазона IP-адресов.
DHCP Pool Size (Размер диапазона DHCP)	Здесь устанавливается количество IP-адресов диапазона DHCP.
Show Statistics (Показать статистику)	Щелкните по кнопке Show Statistics (Показать статистику) для просмотра статистики производительности, например, количества пакетов, переданных и принятых через каждый порт.

12.2.1 Статистика системы

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

Рис. 50 Состояние системы: Показать статистику

System up Time: 1:47:45
CPU Load: 0.29%

WAN Port Statistics:
Link Status: **Down**
Upstream Speed: **0 kbps**
Downstream Speed: **0 kbps**

Node-Link	Status	TxPkts	RxPkts	Errors	Tx B/s	Rx B/s	Up Time
1-PPPoE	Idle	0	0	0	0	0	0:00:00

LAN Port Statistics:

Interface:	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full Duplex	20847	20602	0

Poll Interval(s) :

В следующей таблице даны описания полей этого окна.

Табл. 26 Состояние системы: Показать статистику

ПОЛЕ	ОПИСАНИЕ
System up Time (Время работы системы)	Здесь отображается время, истекшее с момента запуска системы.
CPU Load (Загрузка CPU)	В этом поле отображается процент загрузки процессора модема.
LAN or WAN Port Statistics (Статистика порта LAN или WAN)	Здесь отображается статистика порта глобальной или локальной сети.
Link Status (Состояние канала связи)	Здесь отображается состояние подключения к глобальной сети.
Upstream Speed (Скорость передачи данных)	В этом поле отображается скорость исходящего от модема трафика
Downstream Speed (Скорость приема данных)	В этом поле отображается скорость входящего в модем трафика
Node-Link (Номер - вид соединения)	В этом поле отображается порядковый номер удаленного узла и вид соединения. Виды соединения: PPPoA, ENET, RFC 1483 и PPPoE.
Interface (Интерфейс)	В данном поле отображается тип порта.

Табл. 26 Состояние системы: Показать статистику (продолжение)

ПОЛЕ	ОПИСАНИЕ
Status (Состояние)	Для порта WAN здесь отображается скорость порта и режим передачи, если используется инкапсуляция Ethernet, а также Down (Не работает) (канал не работает), Idle (Ожидание) (неактивность канала (ppp), Dial (Установка соединения) (выполняется вызов) и Drop (Завершение соединения) (разрыв соединения), если используется инкапсуляция PPPoE. Для порта LAN здесь отображается скорость порта и режим передачи.
TxPkts (Передано пакетов)	В этом поле отображается количество пакетов, переданных через этот порт.
RxPkts (Принято пакетов)	В этом поле отображается количество пакетов, принятых через этот порт.
Errors (Ошибки)	В этом поле отображается количество пакетов с ошибками, принятых через этот порт.
Tx B/s (Скорость передачи)	В этом поле отображается количество байтов, переданных в последнюю секунду.
Rx B/s (Скорость приема)	В этом поле отображается количество байтов, принятых в последнюю секунду.
Up Time (Время соединения)	В этом поле отображается время, прошедшее с момента установления соединения через этот порт.
Collision (Конфликт)	Здесь отображается количество конфликтов при передаче через данный порт.
Poll Interval(s) (Интервал(ы) опроса)	Введите интервал времени, через который браузер будет обновлять информацию о системе.
Set Interval (Установить интервал)	Щелкните по этой кнопке для применения нового интервала опроса, который вы установили в поле Poll Interval (Интервал опроса) .
STOP (Остановить)	Щелкните по этой кнопке для прекращения обновления информации о системе.

12.3 Окно Таблица DHCP

DHCP (Dynamic Host Configuration Protocol - Протокол динамической конфигурации узлов, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получать с сервера конфигурацию TCP/IP при начальной загрузке. Можно настроить модем как сервер DHCP или отключить эту функцию. При включенной функции сервера DHCP, модем предоставляет клиентам параметры TCP/IP. При установке значения **None (Отключить)**, служба DHCP будет отключена, следовательно, необходимо иметь другой сервер DHCP в локальной сети, или изменять параметры компьютера вручную.

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

Рис. 51 Таблица DHCP

<i>DHCP Table</i>		
Host Name	IP Address	MAC Address
tw	192.168.1.33	00-00-E8-7C-14-80

В следующей таблице даны описания полей этого окна.

Табл. 27 Таблица DHCP

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

12.4 Окно Таблица Any IP

Щелкните **Maintenance (Сопровождение)**, **Any IP (Любой IP)**. В таблице Any IP отображается текущая информация в режиме только для чтения (включая IP-адрес и MAC-адрес) для всех сетевых устройств, которые используют функцию Any IP для подключения к модему. Более подробно см. [раздел Any IP \(Любой IP\)](#).

Рис. 52 Таблица Any IP (Любой IP)

Any IP Table		
#	IP Address	MAC Address
1	192.168.10.1	00:50:ba:ad:4f:81

Refresh

В следующей таблице даны описания полей этого окна.

Табл. 28 Таблица Any IP (Любой IP)

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер.
IP Address (IP-адрес)	В этом поле отображается IP-адрес сетевого устройства.
MAC Address (MAC-адрес)	В этом поле отображается MAC-адрес (Media Access Control - Управление доступом к среде) компьютера с данным IP-адресом. Каждое устройство Ethernet имеет уникальный MAC-адрес. MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатиричных символов, например, 00:A0:C5:00:00:02.
Refresh (Обновить)	Щелкните по кнопке Refresh (Обновить) для обновления информации в этом окне.

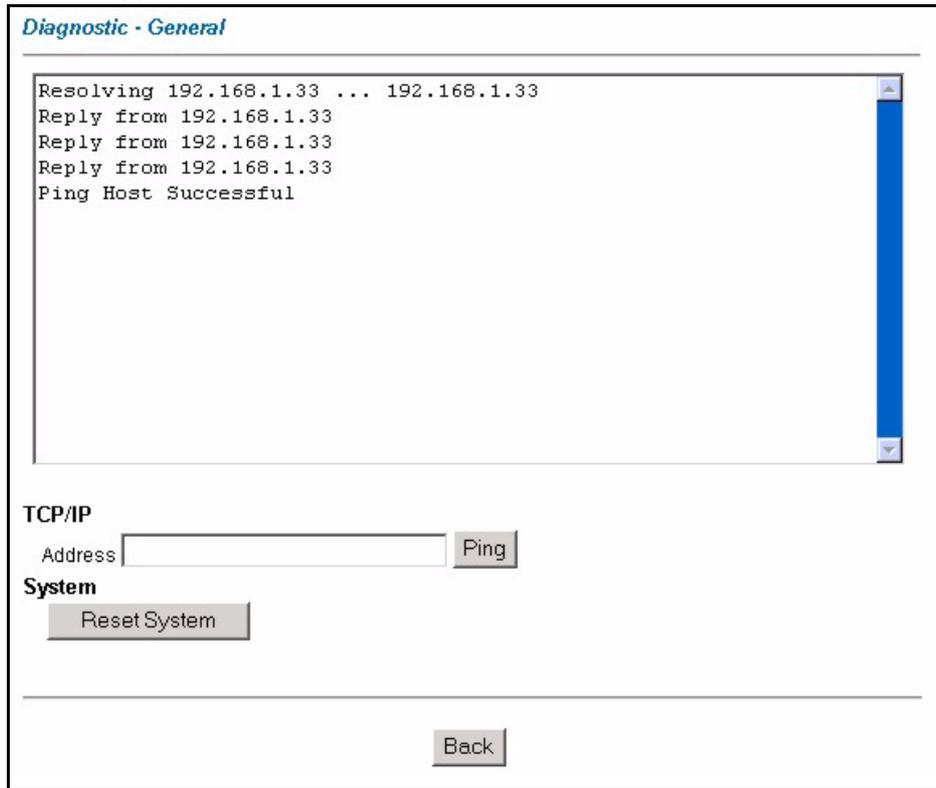
12.5 Окна диагностики

Информация в этих окнах представлена в режиме только для чтения и предназначена помочь определить неисправность модема.

12.5.1 Окно общей диагностики

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

Рис. 53 Диагностика: Общая



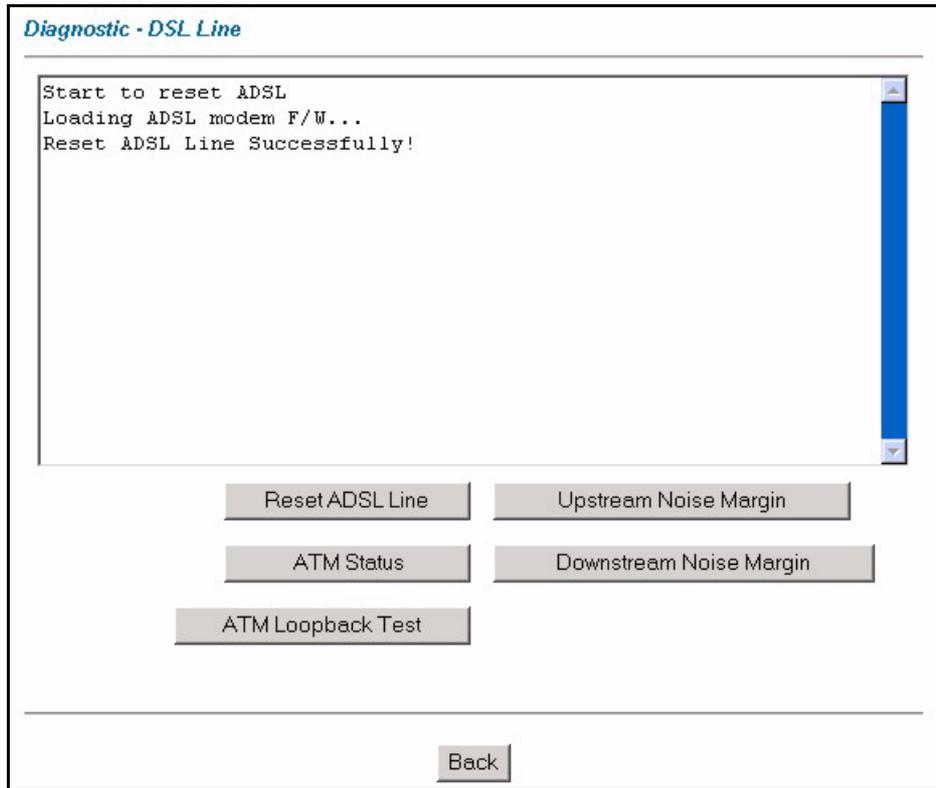
В следующей таблице даны описания полей этого окна.

Табл. 29 Диагностика: Общая

ПОЛЕ	ОПИСАНИЕ
TCP/IP Address (Адрес TCP/ IP)	Введите IP-адрес компьютера, который необходимо протестировать с помощью команды "ping", чтобы проверить соединение.
Ping (Эхо- тестирование)	Щелкните по этой кнопке для тестирования устройства с введенным IP-адресом с помощью команды "ping".
Reset System (Перезапуск системы)	Щелкните по этой кнопке для перезапуска модема. Появляется диалоговое окно с предупреждением: уверены ли вы, что хотите выполнить перезапуск системы. Щелкните ОК для продолжения.
Back (Назад)	Щелкните по этой кнопке для перехода обратно к главному окну Diagnostic (Диагностика) .

12.5.2 Окно диагностики DSL линии

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

Рис. 54 Диагностика: DSL линия

В следующей таблице даны описания полей этого окна.

Табл. 30 Диагностика: DSL линия

ПОЛЕ	ОПИСАНИЕ
Reset ADSL Line (Сброс ADSL линии)	Щелкните по этой кнопке, чтобы заново инициализировать ADSL линию. Тогда в большом текстовом поле сверху будет отображаться прохождение и результаты этой операции, например,: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
ATM Status (Состояние ATM)	Щелкните по этой кнопке для отображения состояния ATM.
ATM Loopback Test (Тест петля ATM)	Щелкните по этой кнопке для запуска кольцевого тестирования ATM. Прежде чем начать выполнение теста, убедитесь, что вы настроили хотя бы один PVC с соответствующими VPI/VCI. Модем посылает пакет OAM F5 на ATM/DSL-коммутатор, после чего он возвращается обратно в модем. Кольцевое тестирование ATM используется для поиска и устранения неисправностей в сети ATM.
Upstream Noise Margin (Запас помехоустойчивости при передаче)	Щелкните по этой кнопке для отображения запаса помехоустойчивости при передаче.

Табл. 30 Диагностика: DSL линия (продолжение)

ПОЛЕ	ОПИСАНИЕ
Downstream Noise Margin (Запас помехоустойчивости при приеме)	Щелкните по этой кнопке для отображения запаса помехоустойчивости при приеме.
Back (Назад)	Щелкните по этой кнопке для перехода обратно к главному окну Diagnostic (Диагностика) .

12.6 Окно микропрограммы

Найдите микропрограмму на сайте www.zyxel.ru, которое содержится в файле, имя которого (обычно) содержит наименование модели системы с расширением .bin, например, "P-660RT.bin". Для загрузки используется протокол HTTP (Hypertext Transfer Protocol - Протокол передачи гипертекста), загрузка может занять до 2-х минут времени. После успешной загрузки микропрограммы система перезапускается. См. [Глава 25 Сопровождение файлов конфигурации и микропрограммы](#) в разделах этого документа по SMT для обновления в микропрограммы с использованием команд FTP/TFTP.



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

Щелкните **Firmware (Микропрограмма)** для отображения следующего окна. Следуйте указаниям в этом окне для загрузки микропрограммы в модем.

Рис. 55 Обновление микропрограммы

FIRMWARE

Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click UPLOAD.

File Path:

CONFIGURATION FILE

Click **Reset** to clear all user-defined configurations and return to the factory defaults.

В следующей таблице даны описания полей этого окна.

Табл. 31 Обновление микропрограммы

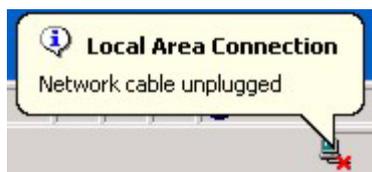
ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите путь к файлу, который вы хотите загрузить, или щелкните по кнопке Browse (Просмотр) ... для определения местонахождения файла.
Browse (Просмотр). ..	Щелкните по кнопке Browse (Просмотр)... для определения местонахождения файла с расширением .bin, который вы хотите загрузить. Необходимо помнить, что архивированные файлы (.zip) необходимо распаковать, прежде чем выполнять загрузку.
Upload (Загрузить)	Щелкните по кнопке Upload (Загрузить) для запуска процесса загрузки. Процесс загрузки может занять до 2 минут.
Reset (Сброс)	Щелкните по этой кнопке для полного удаления пользовательской конфигурации и возвращения параметров модема к заводским настройкам по умолчанию. См. раздел <i>Сброс настроек модема</i> .



ПРИМЕЧАНИЕ: Нельзя выключать питание модема во время загрузки микропрограммы обеспечения!

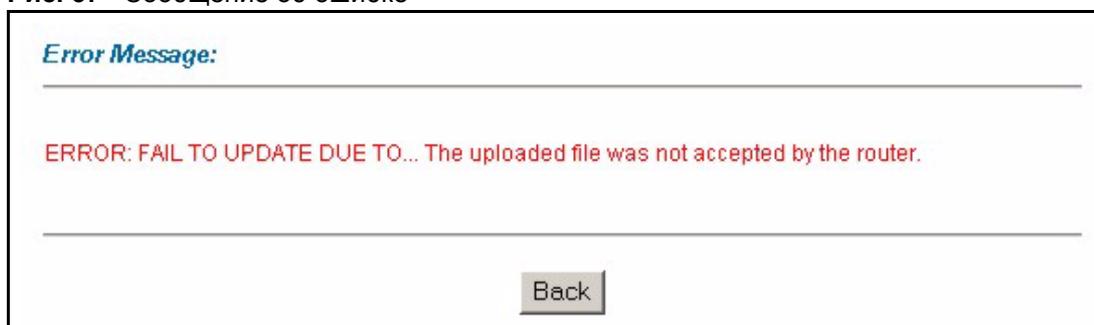
После того как вы увидите окно **Firmware Upload in Process (Выполняется загрузка микропрограммы)**, подождите 2 минуты, прежде чем повторно подключиться к модему по сети и войти в систему.

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

Рис. 56 Временное отключение сети

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

Если загрузку не удалось завершить успешно, появляется следующее окно. Щелкните по кнопке **Back (Назад)** для возврата к окну **Firmware (Микропрограмма)**.

Рис. 57 Сообщение об ошибке

ГЛАВА 13

Знакомство с SMT

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

13.1 Описание SMT

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

13.1.1 Процедура настройки при помощи SMT через соединение Telnet

Далее представлен порядок подключения к модему с помощью Telnet.

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

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

13.1.2 Ввод пароля

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

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

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

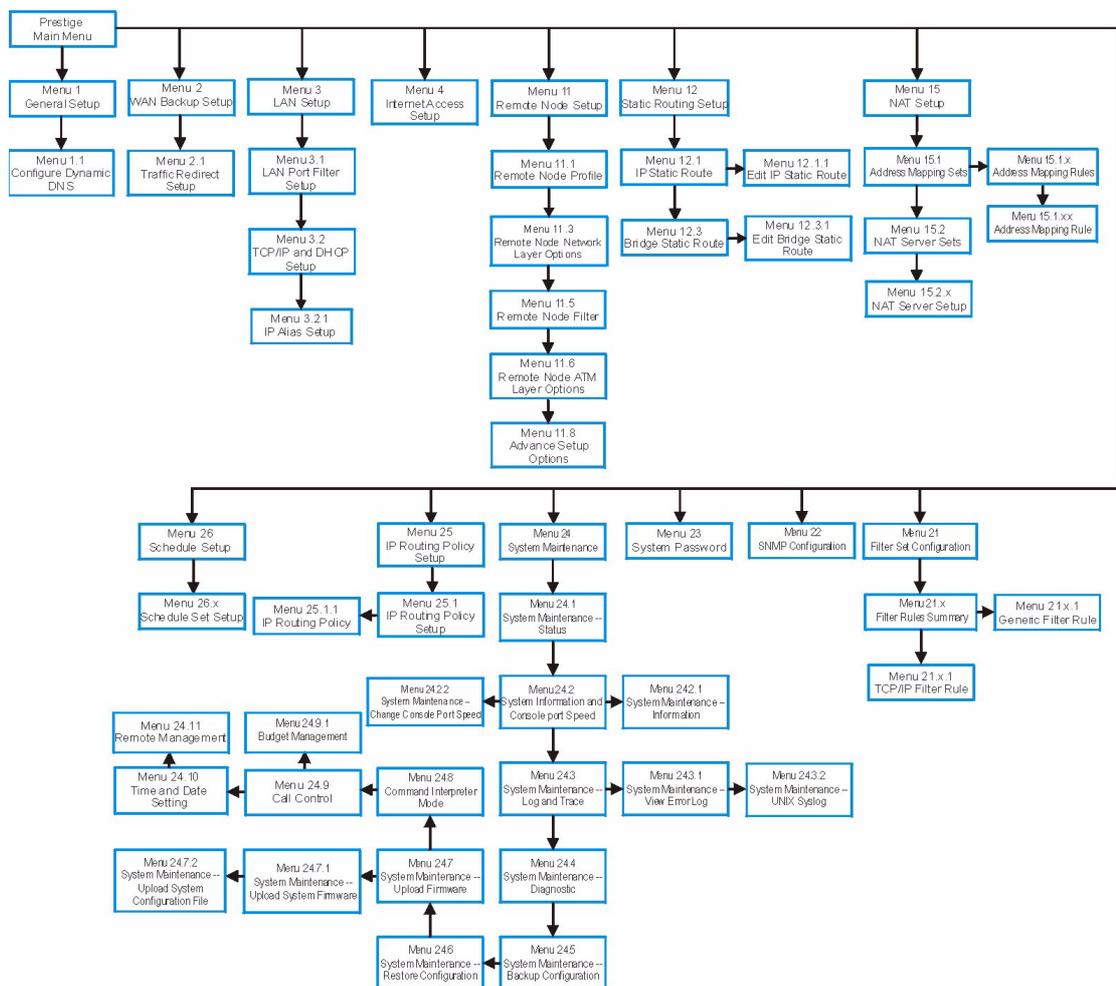
Рис. 58 Окно регистрации

Enter Password : ****

13.1.3 Обзор меню SMT модема

На следующем рисунке представлена сводная схема меню SMT модема.

Рис. 59 Обзор меню SMT модема



13.2 Работа с интерфейсом SMT

SMT (System Management Terminal - Системная консоль) является интерфейсом, предназначенным для настройки параметров модема.

Прежде, чем выполнять изменения в конфигурации, необходимо ознакомиться с некоторыми операциями, приведенными в представленной ниже таблице.

Табл. 32 Работа с интерфейсом SMT

ОПЕРАЦИЯ	НАЖАТИЕ КЛАВИШИ	ОПИСАНИЕ
Переход к меню нижнего уровня	[Enter]	Для перехода в подменю введите его номер и нажмите клавишу [ENTER].
Переход к меню верхнего уровня	[Esc]	Для возврата к предыдущему меню нажмите клавишу [ESC].
Переход к "скрытому" меню	Нажмите клавишу [ПРОБЕЛ] для изменения No на Yes , а затем нажмите клавишу [ENTER].	Поля, начинающиеся с "Edit", ведут к "скрытым" меню и имеют значение по умолчанию No . Чтобы перейти к "скрытому" меню нажмите клавишу [ПРОБЕЛ] для изменения No на Yes , затем нажмите клавишу [ENTER].
Перемещение курсора	Клавиша [ENTER] или клавиши со стрелками "вверх/вниз".	Находясь в меню, для перемещения к следующему полю нажмите клавишу [ENTER]. Для перемещения к предыдущему/следующему полю можно также использовать клавиши со стрелками "вверх/вниз". Если курсор находится вверху меню, то для перемещения вниз меню, нажмите клавишу со стрелкой "вверх".
Ввод данных	Введите данные или нажмите клавишу [ПРОБЕЛ], затем нажмите клавишу [ENTER].	Меню содержат два типа полей. В поле первого типа следует напечатать требуемые данные. Поля второго типа предназначены для ввода параметров, просмотр вариантов которых производится с помощью клавиши [ПРОБЕЛ].
Обязательные поля	<? > или ChangeMe (Измени меня)	Все поля с символом <? > подлежат обязательному заполнению, чтобы иметь возможность сохранения новой конфигурации. Чтобы иметь возможность сохранения новой конфигурации, поля ChangeMe (Измени меня) нельзя оставлять пустыми.
Недоступные пол	<N/A>	В некоторых полях SMT отображается <N/A> (недоступно). Это означает, что данное поле недоступно.
Сохранение конфигурации	[Enter]	Для сохранения конфигурации нажмите клавишу [ENTER] при появлении сообщения "Press ENTER to confirm or ESC to cancel". После сохранения данных, как правило, происходит возврат к предыдущему меню. Необходимо сохранять настройки в каждом окне, которое вы настраивали.
Выход из SMT		Введите 99 и затем нажмите клавишу [ENTER]. Ввод символов 99 в строке приглашения Главного меню и нажатие [ENTER] используются для выхода из интерфейса SMT.

После ввода пароля на экране отображается Главное меню SMT, как показано ниже.

Табл. 33 Главное меню SMT

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.	
Prestige 660R-63/67C Main Menu	
Getting Started	Advanced Management
1. General Setup	21. Filter Set Configuration
2. WAN Backup Setup	22. SNMP Configuration
3. LAN Setup	23. System Password
4. Internet Access Setup	24. System Maintenance
	25. IP Routing Policy Setup
	26. Schedule Setup
Advanced Applications	
11. Remote Node Setup	
12. Static Routing Setup	
15. NAT Setup	99. Exit
Enter Menu Selection Number:	

13.2.1 Описание интерфейса SMT

Табл. 34 Сводка Главного меню

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
1	General Setup (Общие настройки)	Данное меню используется для ввода общих параметров.
2	WAN Backup Setup (Настройка резервного подключения к глобальной сети)	Данное меню используется для настройки перенаправления трафика.
3	LAN Setup (Настройка локальной сети)	Данное меню используется для настройки подключения к локальной сети.
4	Internet Access Setup (Настройка доступа в Интернет)	Простой и быстрый способ настройки подключения к Интернету.
11	Remote Node Setup (Настройка удаленного узла)	Данное меню используется для настройки удаленного узла для соединения между локальными сетями, включая подключение к Интернету.
12	Static Routing Setup (Настройка статической маршрутизации)	Данное меню используется для настройки статических маршрутов.
15	NAT Setup (Настройка NAT)	Данное меню используется для определения внутренних серверов, когда включена служба NAT.
21	Filter Set Configuration (Создание набора фильтров)	Данное меню используется для настройки фильтров.
22	SNMP Configuration (Настройка SNMP)	Данное меню используется для настройки параметров SNMP.

Табл. 34 Сводка Главного меню

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
23	System Password (Системный пароль)	Данное меню используется для изменения пароля.
24	System Maintenance (Сопровождение системы)	Данное меню обеспечивает просмотр информации о состоянии системы, диагностику, загрузку микропрограммы и т. д.
25	IP Routing Policy Setup (Настройка стратегии маршрутизации IP)	Данное меню используется для настройки стратегии маршрутизации IP.
26	Schedule Setup (Настройка расписания)	Данное меню используется для составления расписания исходящих вызовов.
99	Exit (Выход)	Данное меню используется для выхода из SMT и перехода к пустому экрану.

13.3 Изменение системного пароля

Для изменения пароля модема, заданного по умолчанию, выполните следующие действия.

- 1 В Главном меню введите 23 для отображения **Menu 23 - System Password (Системный пароль)**, как показано ниже.
- 2 Введите текущий системный пароль в поле **Old Password (Старый пароль)**, например, "1234" и нажмите клавишу [ENTER].

Рис. 60 Меню 23 - Изменение пароля

```

Menu 23 - System Password

Old Password= ?
New Password= ?
Retype to confirm= ?

Enter here to CONFIRM or ESC to CANCEL:

```

- 3 Введите новый системный пароль в поле **New Password (Новый пароль)** (до 30 символов) и нажмите клавишу [ENTER].
- 4 Для подтверждения повторите ввод нового системного пароля в поле **Retype to Confirm (Повторный ввод для подтверждения)** и нажмите клавишу [ENTER].



ПРИМЕЧАНИЕ: При вводе пароля каждый символ на экране отображается символом звездочка "*".

ГЛАВА 14

Меню 1 - Настройка общих параметров

Меню 1 - Настройка общих параметров содержит административную и общесистемную информацию.

14.1 Настройка общих параметров

Меню 1 - Настройка общих параметров содержит административную и общесистемную информацию (см. ниже). Поле **System Name** (Имя системы) служит только для идентификации. Однако, поскольку некоторые Интернет-провайдеры проверяют это имя, следует вводить имя вашего компьютера.

- В Windows 95/98 щелкните **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления), **Network** (Сеть и удаленный доступ к сети). Щелкните на закладке **Identification** (Идентификация), запишите имя, указанное в поле **Computer Name** (Имя компьютера) и введите его как **Системное имя** модема.
- В Windows 2000 щелкните **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления) и дважды щелкните **System** (Система). Щелкните на закладке **Network Identification** (Сетевая идентификация), а затем на кнопке **Properties** (Свойства). Запишите имя, указанное в поле **Computer Name** (Имя компьютера) и введите его как **Системное имя** модема.
- В Windows XP щелкните на **Start** (Пуск), **My Computer** (Мой компьютер) - **View system information** (Информация о системе), а затем щелкните на закладке **Computer Name** (Имя компьютера). Запишите имя, указанное в поле **Full Computer Name** (Полное имя компьютера), и введите его как **Системное имя** модема.

Запись **Domain Name** (Имя домена) передается клиентам DHCP в локальной сети. Если вы оставите это поле незаполненным, будет использоваться имя домена, полученное протоколом DHCP от Интернет-провайдера. В отличие от имени узла (системное имя), которое необходимо вводить на каждом конкретном компьютере, имя домена может быть назначено модемом с помощью DHCP.

14.2 Процедура настройки в Меню 1

В Главном меню введите 1 для перехода в Меню 1 — **Настройка общих параметров**, как показано ниже.

Рис. 61 Меню 1 - Настройка общих параметров

```

Menu 1 General Setup

System Name= ?
Location=
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No

Route IP= Yes
Bridge= No

Press ENTER to Confirm or ESC to Cancel:

```

Заполните обязательные поля. Подробная информация по этим полям представлена в таблице ниже.

Табл. 35 Меню 1 - Настройка общих параметров

ПОЛЕ	ОПИСАНИЕ
System Name (Системное имя)	Введите описательное имя в целях идентификации. Имя может включать до 30 буквенно-цифровых символов. Использование пробелов не допускается. Допускается использование тире "-" и символа подчеркивания "_".
Location (Местонахождение) (необязательное поле)	Введите географическое местонахождение модема (до 31 символа).
Contact Person's Name (Имя ответственного лица) (необязательное поле)	Введите имя ответственного за модем лица (до 30 символов).
Domain Name (Имя домена)	Введите имя домена (если известно). Если это поле оставлено пустым, Интернет-провайдер может назначить имя домена с помощью DHCP. Чтобы увидеть текущее имя домена, используемое вашим шлюзом, нужно перейти в меню 24.8 и ввести команду "sys domainname". Чтобы очистить это поле, просто нажмите клавишу [ПРОБЕЛ]. Имя домена, введенное вручную, имеет более высокий приоритет, чем имя домена, назначенное Интернет-провайдером.
Edit Dynamic DNS (Редактировать динамическую DNS)	Нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да) или No (Нет) (по умолчанию). Выберите Yes (Да) для настройки Меню 1.1 — Configure Dynamic DNS (Настройка динамической DNS) (описано далее).
Route IP (Маршрутизация IP)	Установите значение этого поля Yes (Да) для включения или No (Нет) для отключения маршрутизации IP. Для доступа в Интернет, необходимо включить маршрутизацию IP.

Табл. 35 Меню 1 - Настройка общих параметров

ПОЛЕ	ОПИСАНИЕ
Bridge (Мост)	Включение/выключение межсетевого моста для передачи неподдерживаемых протоколов (например, SNA) или протоколов, которые не включены в предыдущем поле Route IP (Маршрутизация IP) . Выберите Yes (Да), чтобы включить межсетевой мост; выберите No (Нет), чтобы отключить его.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

14.2.1 Процедура настройки динамической DNS



ПРИМЕЧАНИЕ: Если вы имеете частный IP-адрес в глобальной сети, то динамическая DNS не используется.

Для настройки динамической DNS перейдите в **Меню 1 — Настройка общих параметров** и выберите **Yes** (Да) в поле **Edit Dynamic DNS (Редактировать динамическую DNS)**. Нажмите клавишу [ENTER] для отображения **Меню 1.1— Настройка динамической DNS**, как показано ниже.

Рис. 62 Меню 1.1 - Настройка динамической DNS

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= Yes
Host= me.dyndns.org
EMAIL= mail@mailserver
User= username
Password= *****
Enable Wildcard= No

Press ENTER to Confirm or ESC to Cancel:

```

Для настройки параметров динамической DNS выполните действия, приведенные в следующей таблице.

Табл. 36 Меню 1.1 - Настройка динамической DNS

ПОЛЕ	ОПИСАНИЕ
Service Provider (Провайдер услуг)	Это имя провайдера услуг динамической DNS.
Active (Включить)	Чтобы включить динамическую DNS, нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да) и затем нажмите клавишу [ENTER].

Табл. 36 Меню 1.1 - Настройка динамической DNS

ПОЛЕ	ОПИСАНИЕ
Host (Имя узла)	Введите имя домена, назначенное модему провайдером услуг динамической DNS.
EMAIL (Адрес электронной почты)	Введите адрес электронной почты.
User (Пользователь)	Введите имя пользователя.
Password (Пароль)	Введите назначенный пароль.
Enable Wildcard (Включить шаблоны)	Модем поддерживает шаблоны DYNDNS. Нажмите клавишу [ПРОБЕЛ] и затем [ENTER], чтобы выбрать Yes (Да) или No (Нет). Данное поле имеет значение N/A (Не доступно), если вы выберете клиент DDNS в качестве провайдера услуг.
<p>После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.</p>	

ГЛАВА 15

Меню 2 - Настройка резервного подключения к глобальной сети

В этой главе описывается настройка функции перенаправления трафика с помощью меню 2 и 2.1.

15.1 Описание настройки резервного подключения к глобальной сети

В этой главе описывается настройка модема для перенаправления трафика и создания резервных соединений.

15.2 Настройка резервного подключения в Меню 2

Введите 2 в главном меню для перехода в меню 2.

Рис. 63 Меню 2 - Настройка резервного подключения к глобальной сети

```
Menu 2 - Wan Backup Setup

Check Mechanism = DSL Link
Check WAN IP Address1 = 0.0.0.0
Check WAN IP Address2 = 0.0.0.0
Check WAN IP Address3 = 0.0.0.0
  KeepAlive Fail Tolerance = 0
  Recovery Interval(sec) = 0
  ICMP Timeout(sec) = 0
Traffic Redirect = No

Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описаны поля данного меню.

Табл. 37 Меню 2 - Настройка резервного подключения к глобальной сети

ПОЛЕ	ОПИСАНИЕ
Check Mechanism (Проверить алгоритм)	Нажмите [ПРОБЕЛ], затем нажмите [ENTER] для выбора способа, который используется модемом для проверки соединения DSL. Выберите DSL Link (Канал DSL) , чтобы модем проверял соединение DSL на физическом уровне. Выберите ICMP (Internet Control Message Protocol - Протокол управляющих сообщений в сети Интернет) , чтобы модем периодически выполнял эхо-тестирование IP-адресов, установленных в полях Check WAN IP Address (Проверять IP-адреса глобальной сети) .
Check WAN IP Address1-3 (Проверять IP-адреса глобальной сети 1-3)	Заполните эти поля, чтобы модем проверял доступность глобальной сети. Введите IP-адрес ближайшего надежного компьютера (например, адрес сервера DNS Интернет-провайдера). При использовании резервного подключения к глобальной сети, модем периодически проводит эхо-тестирование установленных здесь адресов и, если не получает ответа, использует другое резервное подключение к глобальной сети (если настроено).
KeepAlive Fail Tolerance (Допуск на отказы)	Введите число (рекомендуется 2), которое показывает сколько раз модем будет выполнять эхо-тестирование IP-адресов, установленных в поле Check WAN IP Address (Проверять IP-адреса глобальной сети) при отсутствии ответа, прежде чем переключиться на резервное подключение к глобальной сети (или другое резервное подключение к глобальной сети).
Recovery Interval (sec) (Интервал восстановления, с)	Когда модем использует соединение с более низким приоритетом (обычно резервное подключение к глобальной сети), устройство периодически проверяет, можно или нет перейти на соединение с более высоким приоритетом. Введите время в секундах (рекомендуется 30), которое модем выжидает между проверками. Увеличьте время, если в устройстве с IP-адресом получателя обрабатывается большой объем трафика.
ICMP Timeout (Время ожидания ICMP)	Введите интервал времени в секундах для ожидания ответа ICMP для сеанса ICMP.
Traffic Redirect (Перенаправление трафика)	Нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да) или No (Нет) . Выберите Yes (Да) и нажмите [ENTER] для настройки Меню 2.1 Traffic Redirect Setup (Настройка перенаправления трафика) . Выберите No (Нет) (по умолчанию), если не требуется настраивать эту функцию.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

15.2.1 Настройка перенаправления трафика

Меню 2.1 — Traffic Redirect Setup (Настройка перенаправления трафика)

используется для настройки параметров, которые определяют, в каком случае модем направляет трафик глобальной сети на резервный шлюз.

Рис. 64 Меню 2.1 - Настройка перенаправления трафика

```

Menu 2.1 - Traffic Redirect Setup

Active= No
Configuration:
Backup Gateway IP Address= 0.0.0.0
Metric= 15

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описаны поля данного меню.

Табл. 38 Меню 2.1 - Настройка перенаправления трафика

ПОЛЕ	ОПИСАНИЕ
Active (Включить)	Нажмите [ПРОБЕЛ] и выберите Yes (для включения) или No (для отключения) функции перенаправления трафика. По умолчанию установлено No .
Configuration (Конфигурация)	
Backup Gateway IP Address (IP- адрес резервного шлюза)	Введите IP-адрес резервного шлюза в десятичном формате с разделительными точками. Модем автоматически пересылает трафик на этот IP-адрес при завершении подключения к Интернету.
Metric (Метрика)	В этом поле устанавливается приоритет маршрутов, которые использует модем. Метрика представляет собой "стоимость передачи данных". Маршрутизатор определяет наилучший маршрут для передачи, выбирая путь с самой низкой "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве единицы "стоимости", минимальное значение которой равно 1 и соответствует прямому соединению между сетями. Число, определяющее стоимость, должно лежать в интервале от "1" до "15"; значение больше "15" означает, что канал не работает. Чем меньше число, тем ниже "стоимость".
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

ГЛАВА 16

Меню 3 - Настройка локальной сети

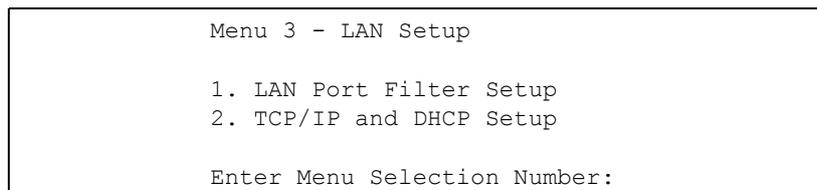
сети

В этой главе описывается настройка параметров проводной локальной сети.

16.1 Настройка локальной сети

В данном разделе описывается настройка сети Ethernet с помощью **Меню 3 — Настройка локальной сети**. В Главном меню, введите 3 для перехода в меню 3.

Рис. 65 Меню 3 - Настройка локальной сети



16.1.1 Общая настройка сети Ethernet

Данное меню позволяет установить набор(-ы) фильтров, которые необходимо применять к трафику Ethernet. Необходимость в фильтрации трафика Ethernet возникает редко; тем не менее, наборы фильтров могут быть полезными для блокировки определенных пакетов, снижения объема трафика и предотвращения несанкционированного доступа.

Рис. 66 Меню 3.1 - Настройка фильтра порта LAN

```
Menu 3.1 - LAN Port Filter Setup

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

Press ENTER to Confirm or ESC to Cancel:
```

Если требуется информация по созданию фильтров, то сначала следует ознакомиться с главой [Глава 22 Настройка фильтров](#), а затем вернуться к данному меню для настройки наборов фильтров.

16.2 Настройка Ethernet в зависимости от используемого протокола

В зависимости от протоколов, используемых для ваших задач, необходимо выполнить соответствующую настройку Ethernet, как описывается далее.

- Для настройки Ethernet с TCP/IP см. [раздел Настройка доступа в Интернет](#).
- Для настройки моста Ethernet см. [Глава 20 Настройка межсетевых мостов](#).

16.3 Настройка Ethernet с TCP/IP и DHCP

Меню 3.2 используется для настройки конфигурации TCP/IP в модеме.

Для редактирования меню 3.2, в Главном меню введите 3 для перехода в **Меню 3 — Настройка локальной сети**. В меню 3 нажмите клавишу "2" и затем нажмите [ENTER] для отображения **Меню 3.2 — TCP/IP and DHCP Ethernet Setup (Настройка Ethernet с TCP/IP и DHCP)**, как показано ниже:

Рис. 67 Меню 3.2 - Настройка Ethernet с TCP/IP и DHCP

```

Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup
DHCP= Server
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 32
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
Remote DHCP Server= N/A
TCP/IP Setup:
IP-address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-2B
Multicast= None
IP Policies=
Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

```

Для настройки полей DHCP выполните действия, представленные в следующей таблице.

Табл. 39 Настройка DHCP Ethernet

ПОЛЕ	ОПИСАНИЕ
DHCP Setup (Настройка DHCP)	
DHCP	<p>Если в этом поле установлено значение Server (Сервер), модем может назначать IP-адреса, шлюз IP по умолчанию и серверы DNS компьютерам с Windows 95, Windows NT и другими системами, поддерживающими клиента DHCP.</p> <p>Если установлено None (Нет), функция сервера DHCP отключена.</p> <p>Если установлено значение Relay (Ретранслятор), модем работает в качестве фиктивного сервера DHCP и ретранслирует запросы и ответы DHCP между удаленным сервером и клиентами. В данном случае необходимо ввести IP-адрес фактического удаленного сервера DHCP в поле Remote DHCP Server (Удаленный сервер DHCP).</p> <p>Если используется сервер DHCP, необходимо установить следующие параметры:</p>
Client IP Pool Starting Address (Начальный IP-адрес клиентского диапазона)	В этом поле вводится первый адрес из непрерывного диапазона IP-адресов.
Size of Client IP Pool (Размер клиентского IP-диапазона)	В этом поле устанавливается размер непрерывного диапазона IP-адресов.

Табл. 39 Настройка DHCP Ethernet (продолжение)

ПОЛЕ	ОПИСАНИЕ
Primary DNS Server (Основной сервер DNS) Secondary DNS Server (Дополнительный сервер DNS)	Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Remote DHCP Server (Удаленный сервер DHCP)	Если в поле DHCP выбрано значение Relay (Ретранслятор) , следует ввести IP-адрес фактического удаленного сервера DHCP.

Для настройки параметров TCP/IP порта Ethernet выполните действия, представленные в следующей таблице.

Табл. 40 Настройка TCP/IP порта Ethernet

ПОЛЕ	ОПИСАНИЕ
TCP/IP Setup (Настройка TCP/IP)	
IP Address (IP-адрес)	Введите IP-адрес (в локальной сети) модема в десятичном формате с разделительными точками.
IP Subnet Mask (Маска IP подсети)	Модем вычисляет маску подсети автоматически на основе назначенного IP-адреса. Если организация подсетей не требуется, следует использовать маску подсети, вычисленную модемом (более подробно см. Приложение С Организация подсетей IP).
RIP Direction (Направление RIP)	Нажмите клавишу [ПРОБЕЛ] для выбора направления RIP. Вариантами являются: None (Нет) , Both (Оба) , In Only (Только входящие) или Out Only (Только исходящие) .
Version (Версия)	Нажмите клавишу [ПРОБЕЛ] для выбора версии RIP. Вариантами являются: RIP-1 , RIP-2B или RIP-2M .
Multicast (Многоадресная рассылка)	IGMP (Internet Group Multicast Protocol - Протокол многоадресной рассылки) - это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Модем поддерживает как версию 1 (IGMP-v1), так и версию 2 (IGMP-v2). Нажмите клавишу [ПРОБЕЛ] для включения многоадресной рассылки IP или выберите None (Нет) для отключения этой функции.
IP Policies (Стратегии IP)	С помощью меню SMT 25 создайте стратегии IP (см. Глава 28 Маршрутизация на базе стратегии IP) и примените их к интерфейсу LAN модема, посредством ввода их номеров в это поле. Можно применить до четырех наборов стратегий IP (из двенадцати), номера вводятся через запятую.
Edit IP Alias (Редактирование псевдонима IP)	модем поддерживает три логических интерфейса локальной сети на одном физическом интерфейсе Ethernet, при этом сам модем является шлюзом для каждой логической сети. Нажмите клавишу [ПРОБЕЛ] для изменения No на Yes и затем нажмите [ENTER] для перехода в меню 3.2.1.

ГЛАВА 17

Доступ в Интернет

В данной главе описывается настройка в модеме параметров локальной и глобальной сети для доступа в Интернет.

17.1 Описание доступа в Интернет

Для более подробной информации по настройке полей в меню SMT, которые описываются в этой главе, см. главы с описанием Мастера установки Web-конфигуратора, а также окон настройки локальной и глобальной сети.

17.2 Стратегии IP

Обычно маршрутизация производится *только* на основе адреса получателя, поэтому маршрутизатор выбирает самый короткий путь для пересылки пакета. Маршрутизация на базе стратегии IP (IP Policy Routing - IPPR) обеспечивает механизм замены схемы маршрутизации по умолчанию и позволяет изменить алгоритм прохождения пакетов на основе стратегии, определяемой сетевым администратором. Применение маршрутизации на основе стратегии к входящим пакетам каждого интерфейса имеет приоритет перед стандартной маршрутизацией. В Меню 25 SMT (см. [Глава 28 Маршрутизация на базе стратегии IP](#)) можно создать стратегии маршрутизации и применить их к интерфейсам модема LAN и/или WAN с помощью меню 3.2 (LAN) и 11.3 (WAN).

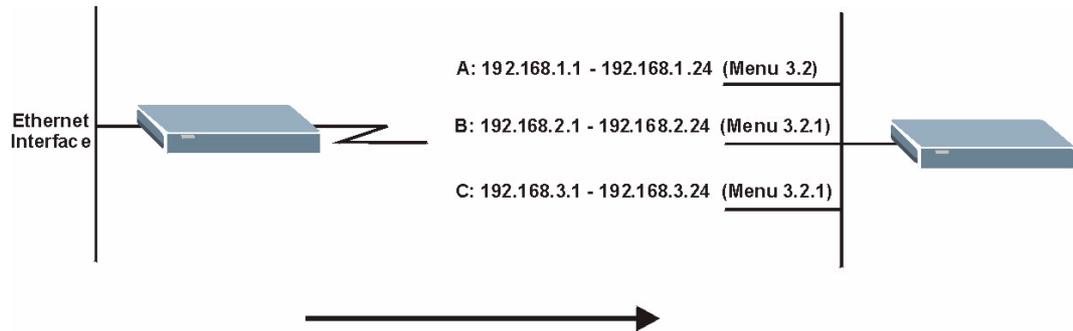
17.3 Псевдоним IP

Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей на основе одного интерфейса Ethernet. Модем поддерживает три логических интерфейса локальной сети на одном физическом интерфейсе Ethernet, при этом сам модем является шлюзом для каждой логической сети.



ПРИМЕЧАНИЕ: Необходимо следить, чтобы логические сети не перекрывались.

На следующем рисунке показано деление локальной сети на подсети А, В, и С.

Рис. 68 Пример сети с использованием псевдонимов IP

Для настройки псевдонимов IP в модеме используется Меню 3.2.1.

17.4 Создание псевдонимов IP

Настройте первую сеть с помощью Меню 3.2. Переместите курсор в поле **Edit IP Alias (Редактировать псевдоним IP)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**, затем нажмите [ENTER] для настройки второй и третьей сети.

Рис. 69 Меню 3.2 - Настройка TCP/IP и DHCP

```

Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup
DHCP= Server
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 32
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
Remote DHCP Server= N/A
TCP/IP Setup:
IP-address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= None
Version= RIP-2B
Multicast= None
IP Policies=
Edit IP Alias= Yes

Press ENTER to Confirm or ESC to Cancel:

```

При нажатии клавиши [ENTER] открывается **Меню 3.2.1 - Настройка псевдонима IP**, как показано ниже.

Рис. 70 Меню 3.2.1 - Настройка псевдонима IP

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= Yes
IP Address= 192.168.2.1
IP Subnet Mask= 255.255.255.0
RIP Direction= None
Version= RIP-1
Incoming protocol filters=
Outgoing protocol filters=
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
Incoming protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:

```

Для настройки параметров псевдонима IP выполните действия, приведенные в следующей таблице.

Табл. 41 Меню 3.2.1 - Настройка псевдонима IP

ПОЛЕ	ОПИСАНИЕ
IP Alias (Псевдоним IP)	Выберите Yes (Да) для настройки локальной сети в модеме.
IP Address (IP-адрес)	Введите IP-адрес модема в десятичном формате с разделительными точками.
IP Subnet Mask (Маска IP подсети)	Модем вычисляет маску подсети автоматически на основе назначенного IP-адреса. Если организация подсетей не требуется, следует использовать маску подсети, вычисленную модемом
RIP Direction (Направление RIP)	Нажмите клавишу [ПРОБЕЛ] для выбора направления RIP. Вариантами являются: None (Нет), Both (Оба), In Only (Только входящие) или Out Only (Только исходящие).
Version (Версия)	Нажмите клавишу [ПРОБЕЛ] для выбора версии RIP. Вариантами являются: RIP-1 , RIP-2B или RIP-2M .
Incoming Protocol Filters (Фильтры входных протоколов)	Введите набор(-ы) фильтров, которые должны применяться к входящему трафику между данным узлом и модемом.
Outgoing Protocol Filters (Фильтры выходных протоколов)	Введите набор(-ы) фильтров, которые должны применяться к исходящему трафику между данным узлом и модемом.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

17.5 Настройка маршрута IP

Сначала необходимо включить функцию маршрутизации IP в **Меню 1 - Настройка общих параметров**.

Для редактирования Меню 1, в Главном меню введите 1 и нажмите клавишу [ENTER]. Установите **Yes (Да)** в поле **Route IP (Маршрут IP)** с помощью нажатия клавиши [ПРОБЕЛ].

Рис. 71 Меню 1 - Настройка общих параметров

```
Menu 1 - General Setup

System Name= ?
Location= location
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No

Route IP= Yes
Bridge= No

Press ENTER to Confirm or ESC to Cancel:
```

17.6 Настройка доступа в Интернет

Меню 4 позволяет ввести все параметры доступа в Интернет в одном окне. Фактически, Меню 4 представляет собой упрощенную настройку для одного из удаленных узлов, к которым можно получить доступ через Меню 11. Прежде, чем выполнять настройку модема для доступа в Интернет, необходимо получить учетные данные для подключения к Интернету.

Используйте таблицу 3 в *Кратком руководстве* для внесения учетных данных Интернет. Если используется инкапсуляция PPPoA или PPPoE, то потребуются ввести только регистрационное имя и пароль, предоставляемые Интернет-провайдером. Если используется инкапсуляция ENET ENCAP, то потребуются ввести только IP-адрес шлюза инкапсуляции Ethernet.

В Главном меню, введите 4 для входа в **Меню 4 – Настройка доступа в Интернет**, как показано ниже.

Рис. 72 Меню 4 - Настройка доступа в Интернет

```

Menu 4 - Internet Access Setup

ISP's Name= myISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= CBR
    Peak Cell Rate (PCR)= 0
    Sustain Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
    IP Address= 0.0.0.0
Network Address Translation= SUA Only
    Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описываются действия по настройке модема для доступа в Интернет.

Табл. 42 Меню 4 - Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ
ISP's Name (Имя Интернет-провайдера)	Введите имя вашего Интернет-провайдера (Эта информация используется только в целях идентификации).
Encapsulation (Инкапсуляция)	Нажмите клавишу [ПРОБЕЛ] для выбора метода инкапсуляции, который используется вашим Интернет-провайдером. Вариантами являются: PPPoE , PPPoA , RFC 1483 или ENET ENCAP .
Multiplexing (Мультиплексирование)	Нажмите клавишу [ПРОБЕЛ] для выбора метода мультиплексирования, который используется вашим Интернет-провайдером. Вариантами являются: VC-based (на базе VC) или LLC-based (на базе LLC) .
VPI # (Номер VPI)	Введите назначенный номер VPI (Virtual Path Identifier - Идентификатор виртуального пути).
VCI # (Номер VCI)	Введите назначенный номер VCI (Virtual Channel Identifier - Идентификатор виртуального канала).
ATM QoS Type (Тип качества обслуживания ATM)	Нажмите клавишу [ПРОБЕЛ] и выберите CBR (Continuous Bit Rate - постоянная скорость передачи), чтобы установить постоянную (всегда доступную) пропускную способность. Выберите UBR (Unspecified Bit Rate - Неопределенная скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите VBR (Variable Bit Rate - Переменная скорость передачи) для пульсирующего трафика и разделения пропускной способности с другими приложениями.
Peak Cell Rate (PCR) (Пиковая скорость ячеек)	Это максимальная скорость, с которой отправитель может передавать ячейки. Введите пиковую скорость ячеек.

Табл. 42 Меню 4 - Настройка доступа в Интернет (продолжение)

ПОЛЕ	ОПИСАНИЕ
Sustain Cell Rate (SCR) (Поддерживаемая скорость ячеек)	SCR (Sustained Cell Rate - поддерживаемая скорость ячеек) это средняя скорость ячеек источника пульсирующего трафика типа "есть-нет", который может передаваться с пиковой скоростью, и является параметром пульсирующего трафика. Введите поддерживаемую скорость ячеек. SCR должно быть меньше, чем PCR.
Maximum Burst Size (MBS) (Максимальный размер пакета)	MBS - это максимальное количество ячеек, которое может быть передано с пиковой скоростью. Введите максимальный размер пакета. Значение должно быть меньше 65535.
My Login (Имя пользователя)	Поля My Login (Имя пользователя) и My Password (Пароль) заполняются только при использовании инкапсуляции PPPoA и PPPoE. Введите регистрационное имя, предоставленное Интернет-провайдером. Если используется инкапсуляция PPPoE, это поле имеет формат user@domain, где domain определяет имя услуги PPPoE.
My Password (Пароль)	Введите пароль для данного регистрационного имени.
ENET ENCAP Gateway (Шлюз ENET ENCAP)	Если используется инкапсуляция ENET ENCAP , введите IP-адрес шлюза, предоставленный Интернет-провайдером.
Idle Timeout (Время неактивности)	Значение в этом поле определяет интервал неактивности в секундах, по истечении которого модем автоматически завершает сеанс связи PPPoE.
IP Address Assignment (Назначение IP-адреса)	Нажмите клавишу [ПРОБЕЛ], чтобы выбрать Static (статический) или Dynamic (динамический) IP адрес.
IP Address (IP-адрес)	Введите IP-адрес, предоставленный Интернет-провайдером, (если требуется).
Network Address Translation (Трансляция сетевых адресов)	Нажмите клавишу [ПРОБЕЛ], чтобы выбрать режим NAT: None (Нет) , SUA Only (Только SUA) или Full Feature (Полный набор функциональных возможностей) . Более подробно о функции SUA (Single User Account - Учетная запись одиночного пользователя) см. Глава 21 Трансляция сетевых адресов (NAT) .
Address Mapping Set (Набор отображения адресов)	Введите номера наборов отображения (от 1 до 8) для использования с NAT. Более подробно см. Глава 21 Трансляция сетевых адресов (NAT) .
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

Если все настройки выполнены правильно, модем должен автоматически подключиться к Интернету. Если при подключении происходит сбой, на экран выводится сообщение об ошибке, с помощью которого необходимо предпринять соответствующие меры для устранения неисправности.

ГЛАВА 18

Настройка удаленного узла

В данной главе описывается настройка удаленного узла.

18.1 Описание настройки удаленного узла

В данном разделе описываются протольно-независимые параметры удаленного узла. Удаленный узел используется для отправки вызовов на удаленный шлюз. Удаленный узел функционирует как удаленный шлюз и как вход в сеть, которая за ним находится. При настройке доступа в Интернет в Меню 4 фактически настраиваются параметры одного из удаленных узлов.

Сначала выберите удаленный узел в **Меню 11- Настройка удаленного узла**. После этого можно редактировать профиль этого узла в Меню 11.1, а также настраивать конкретные параметры с помощью трех подменю: редактировать параметры IP и моста в Меню 11.3; редактировать параметры АТМ в Меню 11.6; и редактировать наборы фильтров в Меню 11.5.

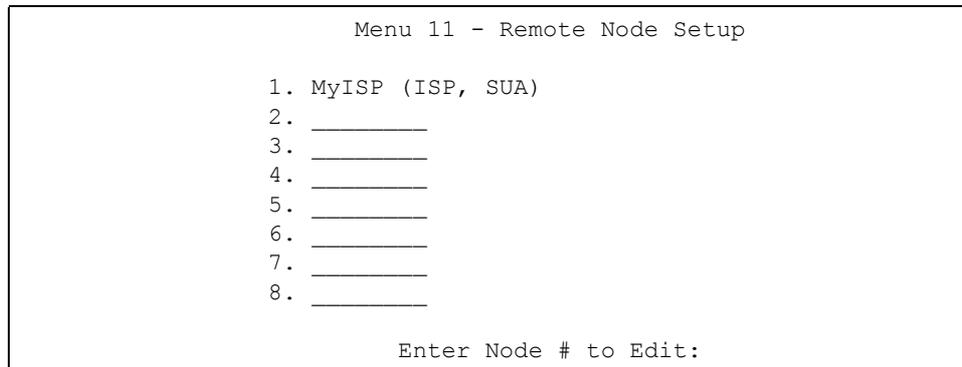
18.2 Настройка удаленного узла

В данном разделе описываются протольно-независимые параметры удаленного узла.

18.2.1 Профиль удаленного узла

Для настройки удаленного узла выполните следующие действия:

- 1** В Главном меню введите 11 для отображения **Меню 11 - Настройка удаленного узла**.
- 2** В Меню 11 введите номер удаленного узла, параметры которого необходимо настроить, как показано на следующем рисунке.

Рис. 73 Меню 11 - Настройка удаленного узла

18.2.2 Сценарии инкапсуляции и мультиплексирования

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

18.2.2.1 Сценарий 1: Один виртуальный канал, несколько протоколов

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

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

Инкапсуляция **RFC-1483** с мультиплексированием **на базе VC** требует минимального количества служебной информации (0 байт). Однако если имеется потенциальная потребность поддержки нескольких протоколов в будущем, то правильнее выбрать инкапсуляцию **PPPoA**, вместо **RFC-1483**, так как в этом случае не придется заново настраивать все компьютеры.

18.2.2.3 Сценарий 3: Несколько виртуальных каналов

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

Рис. 74 Меню 11.1 - Профиль удаленного узла

```

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                Route= IP
Active= Yes                          Bridge= No

Encapsulation= RFC 1483              Edit IP/Bridge= No
Multiplexing= LLC-based              Edit ATM Options= No
Service Name= N/A                    Edit Advance Options= N/A
Incoming:                             Telco Option:
  Rem Login= N/A                      Allocated Budget(min)= N/A
  Rem Password= N/A                  Period(hr)= N/A
Outgoing:                              Schedule Sets= N/A
  My Login= N/A                      Nailed-Up Connection= N/A
  My Password= N/A                   Session Options:
  Authen= N/A                         Edit Filter Sets= No
                                       Idle Timeout(sec)= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Заполните поля в **Меню 11.1 – Профиль удаленного узла**, как описывается в следующей таблице.

Табл. 43 Меню 11.1 - Профиль удаленного узла

ПОЛЕ	ОПИСАНИЕ
Rem Node Name (Имя удаленного узла)	Введите уникальное описательное имя для данного узла длиной до восьми символов.
Active (Включить)	Нажмите клавишу [ПРОБЕЛ], затем клавишу [ENTER] для выбора Yes (Да), чтобы включить, или No (Нет), чтобы отключить данный узел. Неактивные узлы отображаются в Меню 11 SMT со знаком минус ("-").
Encapsulation (Инкапсуляция)	PPPoA относится к RFC-2364 (Инкапсуляция PPP по уровню 5 адаптации ATM). Если выбрана инкапсуляция RFC-1483 (многопротокольная инкапсуляция по уровню 5 адаптации ATM) ENET ENCAP , то поля Rem Login (Имя пользователя удаленного узла), Rem Password (Пароль удаленного узла), My Login (Мое имя), My Password (Мой пароль) и Authen (Аутентификация) являются недоступными (N/A).
Multiplexing (Мультиплексирование)	Нажмите клавишу [ПРОБЕЛ], затем клавишу [ENTER] для выбора метода мультиплексирования, используемого Интернет-провайдером: на базе VC или на базе LLC .
Service Name (Имя услуги)	В случае использования инкапсуляции PPPoE , введите название услуги PPPoE.
Incoming: (Входящие вызовы)	
Rem Login (Регистрационное имя удаленного узла)	Введите регистрационное имя, которое данный удаленный узел будет использовать при вызове модема. Регистрационное имя и пароль удаленного узла (Rem Password) используются для аутентификации данного узла.

Табл. 43 Меню 11.1 - Профиль удаленного узла (продолжение)

ПОЛЕ	ОПИСАНИЕ
Rem Password (Пароль удаленного узла)	Введите пароль, который данный удаленный узел будет использовать при вызове модема.
Outgoing: (Исходящие вызовы)	
My Login (Мое имя пользователя)	Введите регистрационное имя, назначенное Интернет-провайдером, которое модем будет использовать при вызове данного удаленного узла.
My Password (Мой пароль)	Введите пароль, назначенный Интернет-провайдером, который модем будет использовать при вызове данного удаленного узла.
Authen (Аутентификация)	В данном поле устанавливается протокол аутентификации, используемый для исходящих вызовов. Возможны следующие варианты: CHAP/PAP – модем будет принимать вызовы по протоколу CHAP или PAP при запросе от данного удаленного узла. CHAP – принимается только CHAP (Challenge Handshake Authentication Protocol - Протокол аутентификации по методу "вызов-рукопожатие"). PAP – принимается только PAP (Password Authentication Protocol - Протокол аутентификации по паролю).
Route (Маршрут)	Данное поле определяет протокол, используемый при маршрутизации. Возможны варианты: IP и None (Нет) .
Bridge (Мост)	Если функция моста включена, модем будет пересылать все пакеты, которые он не маршрутизирует, на данный удаленный узел. В другом случае, пакеты будут отбрасываться. Выберите Yes (Да) для включения или No (Нет) для отключения моста.
Edit IP/Bridge (Редактировать IP/мост)	Нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да) , затем нажмите клавишу [ENTER] для вывода Меню 11.3 – Параметры сетевого уровня удаленного узла .
Edit ATM Options (Редактирование параметров ATM)	Нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да) , затем нажмите клавишу [ENTER] для вывода Меню 11.6 – Параметры уровня ATM удаленного узла .
Edit Advance Options (Редактировать дополнительные параметры)	Это поле доступно, только если в поле Encapsulation (Инкапсуляция) установлено значение PPPoE . Нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да) , затем нажмите клавишу [ENTER] для вывода Меню 11.8 – Настройка дополнительных параметров .
Telco Option (Параметры телефонной компании)	
Allocated Budget (min) (Выделенный бюджет, мин.)	В этом поле устанавливается предельное значение времени для исходящих вызовов данного удаленного узла. По умолчанию установлено 0, т.е. контроль бюджета не ведется.
Period (hr) (Интервал (ч))	В этом поле устанавливается интервал времени, через который сбрасывается выделенный бюджет. Например, чтобы разрешить вызов данного удаленного узла не более 10 минут каждый час, установите значение 10 (минут) в поле Allocated Budget (Выделенный бюджет) и значение 1 (час) в поле Period (Интервал) .
Schedule Sets (Расписание)	Это поле доступно только при инкапсуляции PPPoE и PPPoA . Можно применять до четырех расписаний. Более подробно см. Глава 29 Расписание вызовов .

Табл. 43 Меню 11.1 - Профиль удаленного узла (продолжение)

ПОЛЕ	ОПИСАНИЕ
Nailed up Connection (Постоянное соединение)	Это поле доступно только при инкапсуляции PPPoE и PPPoA . Данное поле определяет, является ли соединение с данным удаленным узлом постоянным соединением. Более подробная информация приведена ранее в этом разделе.
Session Options (Параметры сеанса связи)	
Edit Filter Sets (Редактирование наборов фильтров)	Нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да), а затем нажмите клавишу [ENTER] и перейдите в Меню 11.5 для редактирования наборов фильтров. Более подробно см. раздел Фильтр удаленного узла .
Idle Timeout (sec) (Время неактивности (с))	Введите интервал времени в секундах (0-9999), разрешенный для неактивности (трафик к удаленному узлу отсутствует), по истечении которого модем автоматически завершает соединение с удаленным узлом. Значение 0 означает, что сеанс связи не ограничен по времени.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

18.2.3 Протокол аутентификации исходящих вызовов

По очевидным причинам рекомендуется использовать максимально надежный протокол аутентификации. Однако, в некоторых исполнениях оборудования профиль пользователя включает специальный протокол аутентификации. Если для такого устройства используемый протокол аутентификации отличается от протокола в профиле пользователя, соединение будет разорвано, даже если используемый протокол является более надежным, чем специальный. Если соединение разрывается сразу после успешной аутентификации, убедитесь, что используется соответствующий протокол аутентификации при подключении к такому устройству.

18.3 Параметры сетевого уровня удаленного узла

Для настройки параметров TCP/IP необходимо в **Меню 11.3 – Параметры сетевого уровня удаленного узла** выполнить следующие действия.

- 1 В Меню 11.1 убедитесь, что **IP** входит в число протоколов в поле **Route (Маршрут)**.
- 2 Переместите курсор в поле **Edit IP/IPX/Bridge (Редактировать IP/IPX/мост)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**, а затем нажмите клавишу [Enter] для отображения **Меню 11.3 – Параметры сетевого уровня удаленного узла**.

Рис. 75 Меню 11.3 - Параметры сетевого уровня удаленного узла

```

Menu 11.3 - Remote Node Network Layer Options

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

Enter here to CONFIRM or ESC to CANCEL:

```

В следующей таблице описываются поля **Меню 11.3 – Параметры сетевого уровня удаленного узла**.

Табл. 44 Меню 11.3 - Параметры сетевого уровня удаленного узла

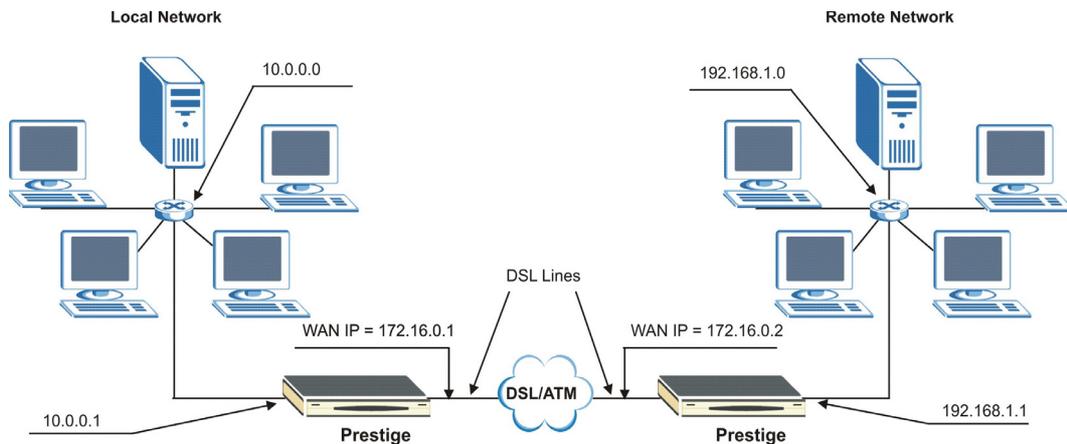
ПОЛЕ	ОПИСАНИЕ
IP Address Assignment (Назначение IP-адреса)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER], чтобы выбрать Dynamic (Динамический) , если удаленный узел использует динамически назначаемый IP-адрес, или Static (Статический) , если используется статический (постоянный) IP-адрес. Вы сможете настраивать этот параметр только в узле Интернет-провайдера (также можно использовать Меню 4), все остальные узлы установлены на использование Static (Статический) .
Rem IP Addr (IP-адрес удаленного узла)	IP-адрес, установленный в предыдущем меню.
Rem Subnet Mask (Маска подсети для удаленного узла)	Введите маску подсети, назначенную для удаленного узла.
My WAN Addr (Мой адрес в глобальной сети)	В некотором исполнении, главным образом, в реализации на базе UNIX, необходимо обеспечить отдельные номера сетей IP для соединений WAN и LAN, и каждое окончание должно иметь уникальный адрес внутри номера сети. В таком случае, введите IP-адрес, назначенный порту WAN модема. ПРИМЕЧАНИЕ: Это относится к локальному адресу модема, но не к адресу удаленного маршрутизатора.
NAT	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER], чтобы выбрать Full Feature (Полный набор функциональных возможностей) , если модем имеет несколько общедоступных IP-адресов в глобальной сети. Выберите SUA Only (Только SUA) , если модем имеет только один общедоступный IP-адрес в глобальной сети. В SMT используется набор отображения адресов 255 (Меню 15.1 - см. Рис.97). Выберите None (Нет) для отключения функции NAT.

Табл. 44 Меню 11.3 - Параметры сетевого уровня удаленного узла (продолжение)

ПОЛЕ	ОПИСАНИЕ
Address Mapping Set (Набор отображения адресов)	Если в поле NAT установлено значение Full Feature (Полный набор функциональных возможностей) , настройте наборы отображения адресов в Меню 15.1. Выберите один из наборов серверов NAT (от 2 до 10) в Меню 15.2 (более подробно см. Глава 21 Трансляция сетевых адресов (NAT)) и введите его номер в это поле. Если в поле NAT установлено значение SUA Only (Только SUA) , в SMT используется набор серверов NAT 1 в Меню 15.2 (более подробно см. Глава 21 Трансляция сетевых адресов (NAT)).
Metric (Метрика)	Метрика определяет "стоимость" передачи и используется для целей маршрутизации. При маршрутизации IP в качестве единицы "стоимости" используется счетчик переходов по сети. Минимальное значение "стоимости" равно 1 и соответствует прямому соединению между сетями. Введите число, которое будет приблизительно выражать "стоимость" трафика для данного канала. Число не обязательно должно быть точным, но должно находиться в диапазоне от 1 до 15. В большинстве случаев хорошо подходит значение 2 или 3.
Private (Частный)	Этот параметр определяет, будет ли модем включать маршрут к этому удаленному узлу в свою широковещательную рассылку RIP. Если установлено Yes (Да) , данный маршрут считается частным и не включается в широковещательную рассылку RIP. Если установлено No (Нет) , маршрут к этому удаленному узлу является доступным для других узлов через широковещательную рассылку RIP.
RIP Direction (Направление RIP)	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER] для выбора направления RIP. Вариантами являются: Both (Оба направления) , In Only (Только входящие) , Out Only (Только исходящие) или None (Нет) .
Version (Версия)	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER] для выбора версии RIP. Вариантами являются: RIP-1 , RIP-2B или RIP-2M .
Multicast (Многоадресная рассылка)	Значение IGMP-v1 устанавливает версию 1 IGMP, IGMP-v2 устанавливает версию 2 IGMP, а None (Нет) отключает IGMP.
IP Policies (Стратегии IP)	Можно применять до четырех наборов стратегий IP (из 12), номера которых вводятся через запятую. Сначала создайте наборы фильтров в Меню 25 (см. Глава 28 Маршрутизация на базе стратегии IP), а затем примените их в этом поле.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

18.3.1 IP-адреса в поле My WAN Addr (Мой адрес в глобальной сети)

На следующем рисунке показан пример использования IP-адресов, который разъясняет заполнение поля **My WAN Addr (Мой адрес в глобальной сети)** в Меню 11.3. См. ранее [Глава 5 Настройка локальной сети](#) на [Рис.15](#), где представлено краткое описание IP-адреса в глобальной сети. Поле **My WAN Addr (Мой адрес в глобальной сети)** показывает IP-адрес в глобальной сети локального устройства Prestige (172.16.0.1 на следующем рисунке), а поле **Rem IP Addr (IP-адрес удаленного узла)** показывает IP-адрес в глобальной сети такого же удаленного устройства (172.16.0.2 на следующем рисунке).

Рис. 76 Пример IP-адресов для соединения локальных сетей на базе TCP/IP

18.4 Фильтр удаленного узла

В Меню 11.1 переместите курсор в поле **Edit Filter Sets (Редактировать наборы фильтров)**, а затем нажмите клавишу [ПРОБЕЛ] для выбора **Yes (Да)**. Затем нажмите клавишу [ENTER] для вывода **Меню 11.5 – Фильтр удаленного узла**.

В **Меню 11.5 – Фильтр удаленного узла** установите набор(-ы) фильтров для применения к входящему и исходящему трафику между данным удаленным узлом и модемом, а также для предотвращения инициирования вызовов конкретными пакетами. Можно применять до 4 наборов фильтров для каждого типа фильтра, номера которых вводятся через запятую, например, 1, 5, 9, 12.

При заполнении данного поля допускается использование пробелов. Модем имеет готовый набор фильтров NetBIOS_WAN, который блокирует пакеты NetBIOS. Его можно включить в набор фильтров вызовов, если вы не хотите, чтобы пакеты NetBIOS инициировали вызовы удаленного узла.

Рис. 77 Меню 11.5 - Фильтр удаленного узла (инкапсуляция RFC 1483 или ENET)

```

Menu 11.5 - Remote Node Filter
  Input Filter Sets:
    protocol filters= 1, 5, 9, 12
    device filters=
  Output Filter Sets:
    protocol filters=
    device filters=

Enter here to CONFIRM or ESC to CANCEL:

```

Рис. 78 Меню 11.5 - Фильтр удаленного узла (инкапсуляция RFC или ENET)

```
Menu 11.5 - Remote Node Filter
Input Filter Sets:
  protocol filters= 1, 5, 9, 12
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Call Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

18.4.1 Правила фильтров безопасности Интернет в Web-конфигураторе

В Web-конфигураторе откройте окно Security (Безопасность), как показано ниже. Выберите стандартные правила фильтров и щелкните **Apply (Применить)**.

Рис. 79 Безопасность при работе в Интернет

Internet Security

Your device provides the following filter rules

<input checked="" type="checkbox"/> Telnet	Telnet traffic is blocked from the WAN to the LAN
<input checked="" type="checkbox"/> FTP	FTP traffic is blocked from the WAN to the LAN
<input checked="" type="checkbox"/> TFTP	TFTP traffic is blocked from the WAN to the LAN
<input checked="" type="checkbox"/> Web	Web traffic is blocked from the WAN to the LAN
<input checked="" type="checkbox"/> SNMP	SNMP traffic is blocked from the WAN
<input type="checkbox"/> Ping.	Ping traffic is blocked from the WAN

Apply Cancel

После применения правил фильтров в Web-конфигураторе, наборы фильтров 11 и 12 автоматически применяются в поле **protocol filters (фильтры протоколов)** в разделе **Input Filter Sets (Набор входных фильтров)** Меню SMT 11.5.



ПРИМЕЧАНИЕ: После применения правил фильтров **Internet Security (Безопасность в Интернет)** в Web-конфигураторе, номера наборов фильтров входных протоколов, примененные ранее в SMT, удаляются. Чтобы применить их снова или применить новые наборы фильтров, необходимо ввести номера наборов фильтров заново вместе с наборами фильтров 11 и 12. Например, чтобы применить наборы фильтров 1 и 2, введите 1, 2, 11, 12.

18.4.2 Наборы фильтров Web-конфигуратора

При применении правил фильтров с использованием Web-конфигуратора, наборы фильтров 11 и 12 автоматически создаются в Меню 21 SMT. Эта функция доступна не во всех моделях устройства.

Рис. 80 Меню 21 - Создание наборов фильтров

```

Menu 21 - Filter Set Configuration

Filter Set #      Comments      Filter Set #      Comments
-----
1                _____      7                _____
2                NetBIOS_WAN      8                _____
3                NetBIOS_LAN      9                _____
4                _____      10               _____
5                _____      11               WebSet1
6                _____      12               WebSet2

Enter Filter Set Number to Configure= 0
    
```

На следующих рисунках показаны правила фильтров в наборах фильтров 11 и 12.

Рис. 81 Меню 21.11 - Набор Web 11

```

Menu 21.11 - Filter Rules Summary
# A Type      Filter Rules      M m n
-----
1 Y IP      Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=161      N
D N
2 Y IP      Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=162      N
D F
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure:
    
```

Рис. 82 Меню 21.12 - Набор Web 12

Menu 21.12 - Filter Rules Summary			
#	A	Type	Filter Rules
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23
	D	N	
2	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21
	D	N	
3	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=69
	D	N	
4	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80
	D	N	
5	N		
6	N		

Enter Filter Rule Number (1-6) to Configure



ПРИМЕЧАНИЕ: Не редактируйте наборы фильтров 11 и 12. Они используются исключительно Web-конфигуратором. Все правила, созданные в наборах 11 и 12, будут удалены или заменены после применения правил фильтров, созданных Web-конфигуратором.

18.5 Редактирование параметров уровня АТМ

Для редактирования **Меню 11.6 – Параметры уровня АТМ удаленного узла** выполните следующие действия.

В Меню 11.1 переместите курсор в поле **Edit ATM Options (Редактирование параметров АТМ)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**. Нажмите клавишу [ENTER] для отображения **Меню 11.6 – Параметры уровня АТМ удаленного узла**.

Вид Меню 11.6 имеет два варианта в зависимости от выбранного в Меню 11.1 метода мультиплексирования: **на базе VC** или **на базе LLC** и инкапсуляции **PPP**.

18.5.1 Мультиплексирование на базе VC (не-PPP инкапсуляция)

При мультиплексировании **на базе VC** по предварительному соглашению каждому протоколу назначается отдельный виртуальный канал, например, по VC1 передается IP. Для каждого протокола должны быть заданы отдельные номера VPI и VCI.

Рис. 83 Меню 11.6 - Мультиплексирование на базе VC

```

Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (VC-Multiplexing)

VC Options for IP:                VC Options for Bridge:
VPI #= 8                        VPI #= 1
VCI #= 35                       VCI #= 36
ATM QoS Type= UBR                 ATM QoS Type= N/A
Peak Cell Rate (PCR)= 0           Peak Cell Rate (PCR)= N/A
Sustain Cell Rate (SCR)= 0        Sustain Cell Rate (SCR)= N/A
Maximum Burst Size (MBS)= 0       Maximum Burst Size (MBR)= N/A

Press ENTER to Confirm or ESC to Cancel:

```

18.5.2 Мультиплексирование на базе LLC или инкапсуляция PPP

При мультиплексировании **на базе LLC** или инкапсуляции **PPP** по одному виртуальному каналу передается несколько протоколов вместе с информацией идентификации протоколов, которая содержится в заголовке каждого пакета.

Рис. 84 Меню 11.6 - Мультиплексирование на базе LLC или инкапсуляция PPP

```

Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)

VPI #= 8
VCI #= 35
ATM QoS Type= UBR
Peak Cell Rate (PCR)= 0
Sustain Cell Rate (SCR)= 0
Maximum Burst Size (MBS)= 0

Enter here to CONFIRM or ESC to CANCEL:

```

В этом случае для всех протоколов нужно указать только один набор номеров VPI и VCI. Допустимый диапазон номеров VPI - от 0 до 255, а для VCI - от 32 до 65535 (номера от 1 до 31 зарезервированы для локального управления трафиком ATM).

18.5.3 Параметры дополнительной настройки

В Меню 11.1 в поле **Encapsulation (Инкапсуляция)** выберите **PPPoE**.

Рис. 85 Меню 11.1- Профиль удаленного узла

```
Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                Route= IP
Active= Yes                          Bridge= No

Encapsulation= PPPoE                Edit IP/Bridge= No
Multiplexing= LLC-based              Edit ATM Options= No
Service Name=                        Edit Advance Options= Yes
Incoming:                            Telco Option:
  Rem Login=                          Allocated Budget(min)= 0
  Rem Password= *****              Period(hr)= 0
Outgoing:                              Schedule Sets=
  My Login= ?                          Nailed-Up Connection= No
  My Password= ?                       Session Options:
  Authen= CHAP/PAP                     Edit Filter Sets= No
                                         Idle Timeout(sec)= 0

Press ENTER to Confirm or ESC to Cancel:
```

Переместите курсор в поле **Edit Advance Options (Редактировать дополнительные параметры)** и нажмите [ПРОБЕЛ] для выбора **Yes**, затем нажмите [ENTER] для отображения **Меню 11.8 – Параметры дополнительной настройки**.

Рис. 86 Меню 11.8 - Параметры дополнительной настройки

```

Menu 11.8 - Advance Setup Options

PPPoE pass-through= No

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описываются поля данного меню.

Табл. 45 Меню 11.8 - Параметры дополнительной настройки

ПОЛЕ	ОПИСАНИЕ
PPPoE pass-through (Сквозное пропускание PPPoE)	<p>Нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да), затем нажмите [ENTER] для включения функции сквозного пропускания PPPoE. В дополнение к встроенному в модем PPPoE клиенту, вы можете включить функцию сквозного пропускания PPPoE, чтобы разрешить до 10 узлам локальной сети использовать у себя программных PPPoE клиентов для подключения к Интернет-провайдеру через модем. Каждый узел может иметь отдельные учетные данные и индивидуальный общедоступный IP-адрес в глобальной сети.</p> <p>Сквозное пропускание PPPoE является альтернативой NAT для применений, где использование NAT нецелесообразно.</p> <p>Нажмите [ПРОБЕЛ] для выбора No и затем нажмите [ENTER] для отключения функции сквозного пропускания PPPoE, если вы не хотите разрешать узлам в локальной сети использовать программное обеспечение клиента PPPoE для подключения к Интернет-провайдеру.</p>
<p>После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.</p>	

ГЛАВА 19

Настройка статических маршрутов

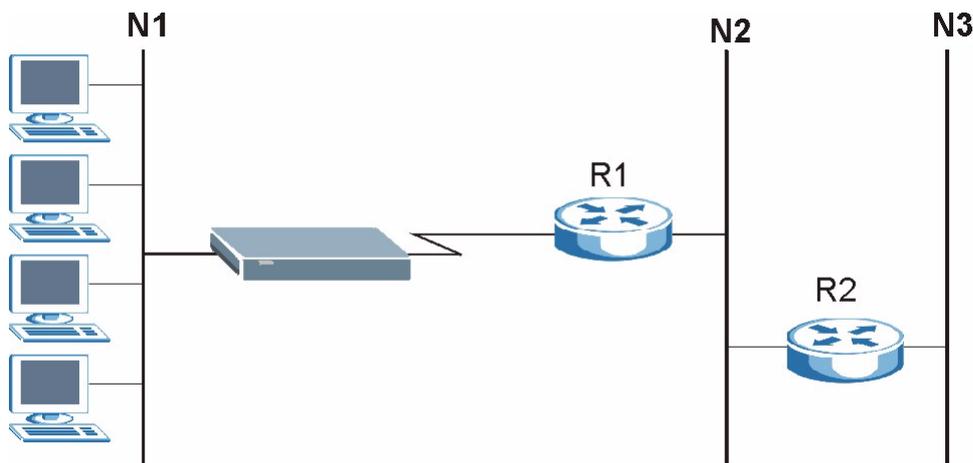
В этой главе описывается создание статических маршрутов IP.

19.1 Описание статических маршрутов IP

Статические маршруты дают модему информацию о маршрутизации, которую устройство не может получить автоматически другими средствами. Такая ситуация может возникать, если в локальной сети отключен RIP, или если удаленная сеть находится за другой сетью, напрямую подключенной к удаленному узлу.

Каждый удаленный узел определяет только ту сеть, к которой непосредственно подключен шлюз, при этом модем не имеет информации о других сетях. Например, модем имеет информацию о сети N2 (на следующем рисунке) через маршрутизатор удаленного узла 1. Однако модем не может послать пакет в сеть N3, так как он "не знает", что существует маршрут через маршрутизатор удаленного узла 1 (и далее через маршрутизатор 2). Статические маршруты дают модему информацию о сетях, находящихся за удаленными узлами.

Рис. 87 Пример топологии статической маршрутизации



19.2 Настройка

- 1 Для создания статического маршрута IP используется **Меню 12 - Настройка статического маршрута** (показано ниже).

Рис. 88 Меню 12 - Настройка статического маршрута

```
Menu 12 - Static Route Setup

1. IP Static Route
3. Bridge Static Route

Please enter selection:
```

2 В Меню 12, выберите 1 для перехода в **Меню 12.1 — Настройка статического маршрута IP** (показано ниже).

Рис. 89 Меню 12.1 - Настройка статического маршрута IP

```
Menu 12.1 - IP Static Route Setup

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

Enter selection number:
```

3 Введите номер статического маршрута, который требуется создать.

Рис. 90 Меню 12.1.1 - Редактирование статического маршрута IP

```
Menu 12.1.1 - Edit IP Static Route

Route #: 1
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

Press ENTER to Confirm or ESC to Cancel:
```

В следующей таблице описываются поля **Меню 12.1.1 – Редактирование статического маршрута IP**.

Табл. 46 Меню 12.1.1 - Редактирование статического маршрута IP

ПОЛЕ	ОПИСАНИЕ
Route # (Номер маршрута)	Это порядковый номер статического маршрута, выбранный в Меню 12.1.
Route Name (Имя маршрута)	Введите описательное имя данного маршрута. Эта информация используется только в целях идентификации.
Active (Включить)	Это поле служит для включения/отключения данного статического маршрута.
Destination IP Address (IP-адрес получателя)	Данный параметр определяет адрес IP-сети конечного получателя. Маршрутизация всегда выполняется на основе сетевого номера. Если нужно определить маршрут к одиночному узлу, в поле маски подсети используйте маску подсети 255.255.255.255, чтобы номер сети и адрес узла были одинаковыми.
IP Subnet Mask (Маска IP подсети)	Введите маску подсети для получателя. См. раздел IP-адрес и маска подсети в данном руководстве.
Gateway IP Address (IP-адрес шлюза)	Введите IP-адрес шлюза. Шлюз - это маршрутизатор или коммутатор, находящийся в том же сегменте сети, что и порт LAN или WAN устройства. Шлюз помогает пересылать пакеты их адресатам.
Metric (Метрика)	Метрика определяет "стоимость" передачи и используется для целей маршрутизации. При маршрутизации IP используется счетчик переходов по сети в качестве единицы "стоимости". Минимальное значение "стоимости" равно 1 и соответствует прямому соединению между сетями. Введите число, которое будет приблизительно выражать "стоимость" трафика для данного канала. Число не обязательно должно быть точным, но должно находиться в диапазоне от 1 до 15. В большинстве случаев хорошо подходит значение 2 или 3.
Private (Частный)	Этот параметр определяет, будет ли модем включать маршрут к этому удаленному узлу в широковещательную рассылку RIP. Если установлено Yes (Да), данный маршрут считается частным и не включается в широковещательную рассылку RIP. Если установлено No (Нет), маршрут к этому удаленному узлу является доступным для других узлов через широковещательную рассылку RIP.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

ГЛАВА 20

Настройка межсетевого моста

В данной главе рассматривается настройка параметров межсетевого моста.

20.1 Общие сведения о межсетевом мосте

При использовании межсетевого моста решение о передаче пакетов принимается на основе MAC-адреса (Media Access Control - Управление доступом к среде) или аппаратного адреса, в то время как при маршрутизации - на основе адреса сетевого уровня (IP). Организация моста позволяет P-660RT передавать пакеты протоколов сетевого уровня, которые P-660RT не маршрутизирует, например, SNA, из одной сети в другую. Недостатком моста является то, что по сравнению с маршрутизацией, передача по мосту генерирует значительно больший объем трафика для того же самого сетевого протокола и потребляет больше памяти и циклов процессора устройства.

В целях повышения производительности *не* следует включать межсетевой мост, пока не возникает необходимость в поддержке в вашей сети протоколов, отличных от IP. Для протокола IP включите маршрутизацию, если необходимо; не используйте межсетевой мост в тех случаях, когда P-660RT может выполнять маршрутизацию.

20.2 Настройка Ethernet для организации моста

В основном, все нелокальные пакеты передаются по мосту в глобальную сеть. Модем не поддерживает протокол IPX (Internetwork Packet eXchange - Межсетевой обмен пакетами).

20.2.1 Настройка межсетевого моста для удаленного узла

Для настройки протоколно-независимых параметров в **Меню 11.1 – Профиль удаленного узла** необходимо выполнить процедуру, описанную в соответствующем разделе. Параметры межсетевого моста настраиваются в **Меню 11.3 – Параметры сетевого уровня удаленного узла**.

- 1 Для настройки **Меню 11.3 – Параметры сетевого уровня удаленного узла**, показанного на следующем рисунке, необходимо выполнить следующие действия:
- 2 В Меню 11.1 убедитесь, что в поле **Bridge** установлено **Yes (Да)**.

Рис. 91 Меню 11.1 - Профиль удаленного узла

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ?
Active= Yes
Encapsulation= ENET ENCAP
Multiplexing= VC-based
Service Name= N/A
Incoming:
  Rem Login= N/A
  Rem Password= N/A
Outgoing:
  My Login= N/A
  My Password= N/A
  Authen= N/A

Route= IP
Bridge= Yes
Edit IP/Bridge= Yes
Edit ATM Options= No
Edit Advance Options= N/A
Telco Option:
  Allocated Budget(min)= N/A
  Period(hr)= N/A
  Schedule Sets= N/A
  Nailed-Up Connection= N/A
Session Options:
  Edit Filter Sets= No
  Idle Timeout(sec)= N/A

Press ENTER to Confirm or ESC to Cancel:
    
```

3 Переместите курсор в поле **Edit IP/Bridge (Редактировать IP/мост)** и нажмите клавишу [ПРОБЕЛ], чтобы установить значение **Yes (Да)**, а затем клавишу [ENTER] для перехода в **Меню 11.3 – Параметры сетевого уровня удаленного узла**.

Рис. 92 Меню 11.3 - Параметры сетевого уровня удаленного узла

```

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= Full Feature
  Address Mapping Set=2
  Metric= 2
  Private= No
  RIP Direction= Both
  Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

Bridge Options:
  Ethernet Addr Timeout (min)= 0

Press ENTER to Confirm or ESC to Cancel:
    
```

Табл. 47 Параметры сетевого уровня удаленного узла: Поля для настройки моста

ПОЛЕ	ОПИСАНИЕ
Bridge (Мост) (Меню 11.1)	Убедитесь, что в данном поле установлено значение Yes (Да) .

Табл. 47 Параметры сетевого уровня удаленного узла: Поля для настройки моста

ПОЛЕ	ОПИСАНИЕ
Edit IP/Bridge (меню 11.1) (Редактировать IP/мост)	Нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да), а затем нажмите клавишу [ENTER] для отображения меню 11.3.
Ethernet Addr Timeout (Время хранения адреса Ethernet)(мин.) (Меню 11.3)	Введите интервал времени (в минутах), в течение которого модем сохраняет информацию об адресе Ethernet в своих внутренних таблицах, пока соединение не работает. Если данная информация сохраняется, то модему не нужно заново компилировать таблицы при восстановлении соединения.

20.2.2 Создание статического маршрута для межсетевого моста

Аналогично статическим маршрутам сетевого уровня, статический маршрут для межсетевого моста дает модему информацию о маршруте до узла, прежде чем устанавливается соединение. Статические маршруты для межсетевого моста настраиваются в Меню 12.3.1, которое показано ниже (перейдите в Меню 12, выберите пункт 3, затем выберите статический маршрут для редактирования).

Рис. 93 Меню 12.3.1 - Редактировать статический маршрут для моста

```

Menu 12.3.1 - Edit Bridge Static Route

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

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описывается Меню **Редактировать статический маршрут для моста**.

Табл. 48 Меню 12.3.1 - Редактировать статический маршрут для моста

ПОЛЕ	ОПИСАНИЕ
Route # (Номер маршрута)	Это порядковый номер маршрута из списка в Меню 12.3 – Создание статического маршрута для межсетевого моста .
Route Name (Имя маршрута)	Введите имя статического маршрута для межсетевого моста в целях идентификации.
Active (Включить)	Это поле показывает включен (Yes (Да)) или отключен (No (Нет)) данный статический маршрут.
Ether Address (Ethernet адрес)	Введите MAC-адрес компьютера получателя, на который должны пересылаться пакеты по мосту.
IP Address (IP-адрес)	Если применяется, введите IP-адрес компьютера получателя, на который должны пересылаться пакеты по мосту.

Табл. 48 Меню 12.3.1 - Редактировать статический маршрут для моста (продолжение)

ПОЛЕ	ОПИСАНИЕ
Gateway Node (Шлюзовой узел)	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER] для выбора номера удаленного узла (от одного до восьми), который является шлюзом для данного статического маршрута.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

ГЛАВА 21

Трансляция сетевых адресов (NAT)

В данной главе описывается настройка функции NAT в модеме.

21.1 Сравнение SUA (Учетная запись одиночного пользователя) и NAT

SUA (Single User Account - Учетная запись одиночного пользователя) - это реализация в операционной системе ZyNOS подмножества NAT, которое поддерживает два типа отображения: **Many-to-One (много-к-одному)** и **Server (сервер)**. См. [раздел Настройка NAT](#) или подробное описание функций NAT для реализации SUA. Модем также поддерживает режим NAT **Full Feature (Полный набор функциональных возможностей)** для отображения нескольких глобальных IP-адресов на несколько частных IP-адресов клиентов или серверов в локальной сети с использованием различных типов отображения.



ПРИМЕЧАНИЕ: 1. Выберите **SUA Only (Только SUA)**, если модем имеет только один общедоступный IP-адрес в глобальной сети.
2. Выберите **Full Feature (Полный набор функциональных возможностей)**, если модем имеет несколько общедоступных IP-адресов в глобальной сети.

21.2 Применение NAT

Для применения NAT используется Меню 4 или Меню 11.3, как показано ниже. На следующем рисунке показано применение NAT в Меню 4 для доступа в Интернет. В Главном меню введите 4 для перехода в **Меню 4 - Настройка доступа в Интернет**.

Рис. 94 Меню 4 - Применение NAT для доступа в Интернет

```

Menu 4 - Internet Access Setup

ISP"s Name= myISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
    Peak Cell Rate (PCR)= 0
    Sustain Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
    IP Address= 0.0.0.0
Network Address Translation= SUA Only
    Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

На следующем рисунке показано применение NAT для удаленного узла в Меню 11.1.

- 1** В Главном меню введите "11".
- 2** В Меню 11 введите номер удаленного узла, параметры которого необходимо настроить, как показано на следующем рисунке.
- 3** Переместите курсор в поле **Edit IP/Bridge (Редактировать IP/мост)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**, а затем нажмите [ENTER] для перехода в **Меню 11.3 - Параметры сетевого уровня удаленного узла**.

Рис. 95 Применение NAT в Меню 4 и Меню 11.3

```

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

Enter here to CONFIRM or ESC to CANCEL:

```

В следующей таблице представлено описание режимов трансляции сетевых адресов.

Табл. 49 Применение NAT в Меню 4 и Меню 11.3

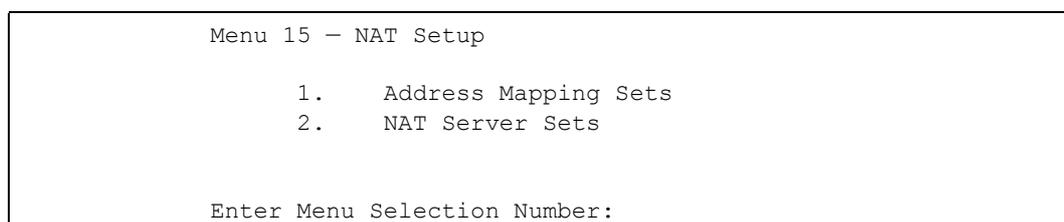
ПОЛЕ	ОПИСАНИЕ
NAT	Нажмите клавишу [ПРОБЕЛ], а затем [ENTER], чтобы выбрать Full Feature (Полный набор функциональных возможностей) , если модем имеет несколько общедоступных IP-адресов в глобальной сети. В SMT используется набор отображения адресов, который вы настроили в поле Address Mapping Set (Набор отображения адресов) (см. раздел Наборы отображения адресов).
	Выберите None (Нет) для отключения функции NAT.
	Если выбрано значение SUA Only (Только SUA) , в SMT используется набор отображения адресов 255 (см. раздел Наборы отображения адресов). Выберите SUA Only (Только SUA) , если модем имеет только один общедоступный IP-адрес в глобальной сети.

21.3 Настройка NAT

Меню и подменю наборов отображения адресов предназначены для создания таблицы отображения, которая используется для назначения глобальных адресов компьютерам в локальной сети. **Set 255 (Набор 255)** используется для SUA. Если в Меню 4 или Меню 11.3 выбрано **Full Feature (Полный набор функциональных возможностей)**, в SMT используется **Set 1 (Набор 1)**. Если выбрано **SUA Only (Только SUA)**, в SMT используется стандартный **Набор 255** (только для чтения).

Server Set (Набор серверов) - это список серверов в локальной сети, которые отображаются на внешние порты. Для использования этого набора, необходимо установить правила отображения серверов в наборе отображения адресов NAT. Для получения более подробной информации по этим меню см. раздел о переадресации портов в главе, посвященной окнам NAT в Web-конфигураторе. Для настройки NAT, в Главном меню введите 15 для перехода к следующему экрану.

Рис. 96 Меню 15 - Настройка NAT



21.3.1 Наборы отображения адресов

Введите 1 для вывода **Меню 15.1 — Наборы отображения адресов**.

Рис. 97 Меню 15.1 - Наборы отображения адресов

```

Menu 15.1 - Address Mapping Sets

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

Enter Menu Selection Number:

```

21.3.1.1 Набор отображения адресов SUA

Введите 255 для отображения следующего меню (см. также [раздел Сравнение SUA \(Учетная запись одиночного пользователя\) и NAT](#)). Поля данного меню не доступны для изменения.

Рис. 98 Меню 15.1.255 - Правила отображения адресов SUA

```

Menu 15.1.255 - Address Mapping Rules
Set Name= SUA
Idx  Local Start IP   Local End IP   Global Start IP  Global End IP   Type
----  -
1.   0.0.0.0           255.255.255.255  0.0.0.0          Server+
2.
3.
4.
5.
6.
7.
8.
9.
10.

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описываются поля данного меню.



ПРИМЕЧАНИЕ: Меню 15.1.255 отображается в режиме только для чтения.

Табл. 50 Правила отображения адресов SUA

ПОЛЕ	ОПИСАНИЕ
Set Name (Имя набора)	Здесь отображается имя набора, выбранного в Меню 15.1, или можно ввести имя нового набора, который вы хотите создать.
Idx (Индекс)	Порядковый номер правила.

Табл. 50 Правила отображения адресов SUA (продолжение)

ПОЛЕ	ОПИСАНИЕ
Local Start IP (Начальный локальный IP-адрес)	Local Start IP - это начальный локальный IP-адрес (ILA).
Local End IP (Конечный локальный IP-адрес)	Local End IP - это конечный локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, то начальный адрес равен 0.0.0.0, а конечный адрес равен 255.255.255.255.
Global Start IP (Начальный глобальный IP-адрес)	Это начальный глобальный IP-адрес (IGA). Если вы используете динамический IP-адрес, введите 0.0.0.0 в качестве начального глобального IP-адреса .
Global End IP (Конечный глобальный IP-адрес)	Это конечный глобальный IP-адрес (IGA).
Тип (Тип отображения)	Здесь показывается тип отображения адресов. Тип Server (Сервер) позволяет определить несколько серверов для различных служб, расположенных за NAT по отношению к модему. См. далее несколько примеров.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

21.3.1.2 Наборы отображения адресов, определяемые пользователем

В Меню 15.1 введите 1 для отображения представленного ниже меню. Рассмотрим только отличие этого меню от предыдущего. Здесь присутствуют дополнительные поля **Action (Действие)** и **Select Rule (Выбор правила)**, что означает, что в данном меню можно настраивать правила. Знак [?] в поле **Set Name (Имя набора)** означает, что это обязательное поле и необходимо ввести имя для данного набора.

Рис. 99 Меню 15.1.1 - Первый набор

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.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Action= Edit Select Rule=
Press ENTER to Confirm or ESC to Cancel:



ПРИМЕЧАНИЕ: Если поле **Set Name (Имя набора)** оставлено пустым, весь набор будет удален.



ПРИМЕЧАНИЕ: Тип отображения, а также локальный или глобальный начальный/конечный IP- адреса устанавливается в Меню 15.1.1.1 (описывается далее), здесь только отображаются значения соответствующих полей.

21.3.1.3 Порядок применения правил

Порядок следования правил имеет большое значение, поскольку модем применяет правила в указанном порядке. Когда текущий пакет соответствует какому-либо правилу, Модем выполняет соответствующее действие и игнорирует остальные правила. Если в таблице существуют пустые правила перед новым создаваемым правилом, это правило перемещается вверх на количество позиций, равное числу пустых правил. Например, если в текущем наборе уже созданы правила с 1-го по 6-е и затем создается правило номер 9, в сводном окне набора новое правило будет иметь номер 7, а не 9.

Теперь, если удалить правило 4, правила с 5-го по 7-е переместятся вверх на одну позицию, т.о. старое правило 5 станет правилом 4, старое правило 6 станет правилом 5 и старое правило 7 станет правилом 6.

Табл. 51 Меню 15.1.1 - Первый набор

ПОЛЕ	ОПИСАНИЕ
Set Name (Имя набора)	Введите имя для данного набора правил. Это обязательное поле. Если это поле оставлено пустым, весь набор будет удален.
Action (Действие)	По умолчанию установлено Edit (Редактировать) . Edit (Редактировать) означает, что вы хотите редактировать выбранное правило (см. следующее поле). Insert Before (Вставить перед) означает вставку нового правила перед выбранным правилом. Правила после выбранного переместятся вниз на одну позицию. Delete (Удалить) означает удаление выбранного правила, после чего все остальные правила после удаленного переместятся вверх на одну позицию. Значение None (Нет) отключает поле Select Rule (Выбор правила) .
Select Rule (Выбор правила)	При выборе значения Edit (Редактировать) , Insert Before (Вставить перед) или Delete (Удалить) в предыдущем поле курсор автоматически перемещается в данное поле для выбора правила, к которому применяется действие.



ПРИМЕЧАНИЕ: Для сохранения всего набора нажмите клавишу [ENTER] в нижней части экрана. Необходимо повторить это действие, если после сохранения в данный набор правил вносятся изменения – включая удаление правила. Изменения не вступят в силу, пока не выполнено сохранение набора.

После установки значения **Edit (Редактировать)** в поле **Action (Действие)** и выбора правила открывается **Меню 15.1.1.1 - Правило отображения адресов**, в котором можно редактировать конкретное правило и настраивать поля **Type (Тип)** и **Local** и **Global Start/End IPs (Локальный и глобальный начальный/конечный IP-адреса)**.



ПРИМЕЧАНИЕ: Конечный IP-адрес должен быть численно больше соответствующего начального IP-адреса.

Рис. 100 Меню 15.1.1.1 - Редактирование/Создание конкретного правила в наборе

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One
Local IP:
  Start=
  End = N/A
Global IP:
  Start=
  End = N/A
Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описываются поля данного меню.

Табл. 52 Меню 15.1.1.1 - Редактирование/Создание конкретного правила в наборе

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора типа отображения из пяти вариантов. Типы отображения обсуждались в главе, посвященной окнам NAT в Web-конфигураторе. Тип Server (Сервер) позволяет определить несколько серверов для различных служб, находящихся за NAT по отношению к модему. См. раздел Пример 3: Несколько общедоступных IP-адресов для внутренних серверов .
Local IP (Локальные IP-адреса)	Для типа отображения "сервер" только поля локальных IP-адресов являются недоступными (N/A); Поля глобальных IP-адресов должны быть обязательно заполнены.
Start (Начальный)	Это начальный локальный IP-адрес (ILA).
End (Конечный)	Это конечный локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, введите начальный адрес 0.0.0.0, а конечный - 255.255.255.255. Это поле является недоступным (N/A) для типов отображения один-к-одному и сервер .
Global IP (Глобальные IP-адреса):	
Start (Начальный)	Это начальный внутренний глобальный IP-адрес (IGA). Если вы используете динамический IP-адрес, введите 0.0.0.0 в качестве начального глобального IP-адреса . ПРИМЕЧАНИЕ: Следует отметить, что поле Начальный глобальный IP-адрес может иметь значение 0.0.0.0, только если используется тип отображения много-к-одному или сервер .
End (Конечный)	Это конечный внутренний глобальный IP-адрес (IGA). Это поле является недоступным (N/A) для типов отображения один-к-одному , много-к-одному и сервер .

ПОЛЕ	ОПИСАНИЕ
Server Mapping Set (Набор отображения серверов)	Это поле доступно, только если в поле Типе (Тип) установлено значение Server (Сервер) . Введите число от 1 до 10, чтобы выбрать набор серверов, установленный в Меню 15.2.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

21.4 Настройка сервера, расположенного за NAT

Для настройки сервера, расположенного за NAT выполните следующие действия:

- 1** В Главном меню введите 15 для перехода в **Меню 15 - Настройка NAT**.
- 2** Введите 2 для перехода в **Меню 15.2 - Наборы серверов за NAT**, которое показано ниже.

Рис. 101 Меню 15.2 - Наборы серверов за NAT

```

Menu 15.2 - NAT Server Sets

      1. Server Set 1 (Used for SUA Only)
      2. Server Set 2
      3. Server Set 3
      4. Server Set 4
      5. Server Set 5
      6. Server Set 6
      7. Server Set 7
      8. Server Set 8
      9. Server Set 9
     10. Server Set 10

Enter Set Number to Edit:

```

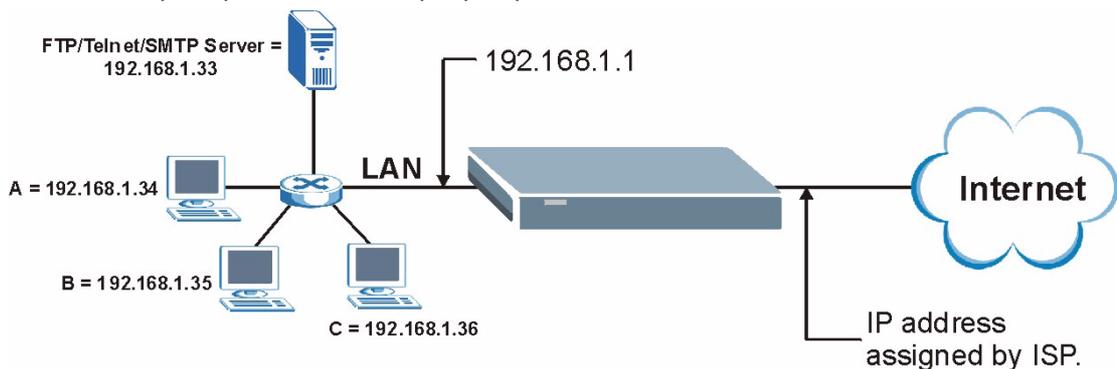
- 3** Введите 1 для перехода в **Меню 15.2.1 - Настройка серверов за NAT**, которое показано ниже.

Рис. 102 Меню 15.2.1 - Настройка серверов за NAT

Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	21	21	192.168.1.33
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

- 4** Введите номер порта в свободное поле **Start Port No (Начальный номер порта)**. Для переадресации только одного порта, введите его номер еще раз в поле **End Port No (Конечный номер порта)**. Чтобы установить диапазон портов, введите номер последнего порта для переадресации в поле **End Port No (Конечный номер порта)**.
- 5** Введите внутренний IP-адрес сервера в поле **IP Address (IP-адрес)**. На следующем рисунке показан компьютер, функционирующий как сервер FTP, Telnet и SMTP (порты 21, 23 и 25) с адресом 192.168.1.33.
- 6** После определения всех серверов нажмите [ENTER] в строке “Press ENTER to confirm ...” для сохранения конфигурации или нажмите [ESC] для отмены внесенных изменений в любое время.

Рис. 103 Пример: Несколько серверов расположены за NAT

21.5 Примеры применения NAT

Далее приводятся несколько примеров конфигурации NAT.

21.5.1 Пример 1: Только доступ в Интернет

В следующем примере для доступа в Интернет требуется только одно правило, по которому все внутренние локальные адреса (ILA) отображаются на один динамический внутренний глобальный адрес (IGA), назначаемый Интернет-провайдером.

Рис. 104 Пример применения NAT 1

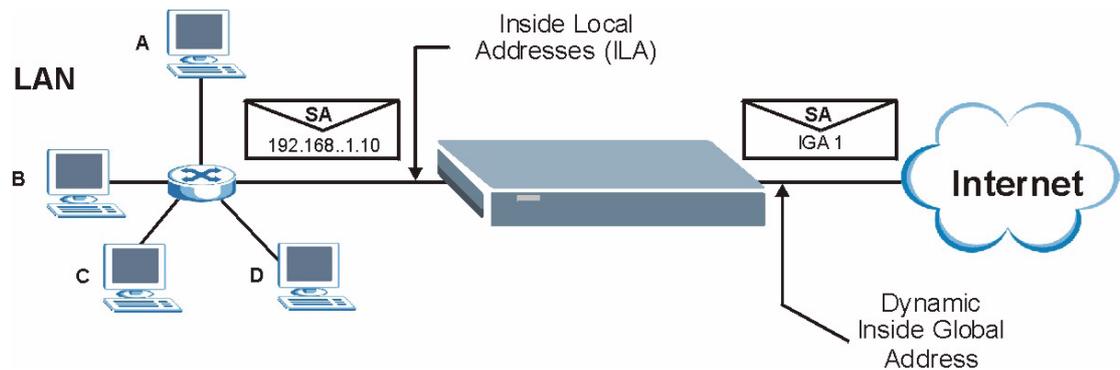


Рис. 105 Меню 4 - Пример доступа в Интернет при использовании NAT

```

Menu 4 - Internet Access Setup
ISP's Name= myISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

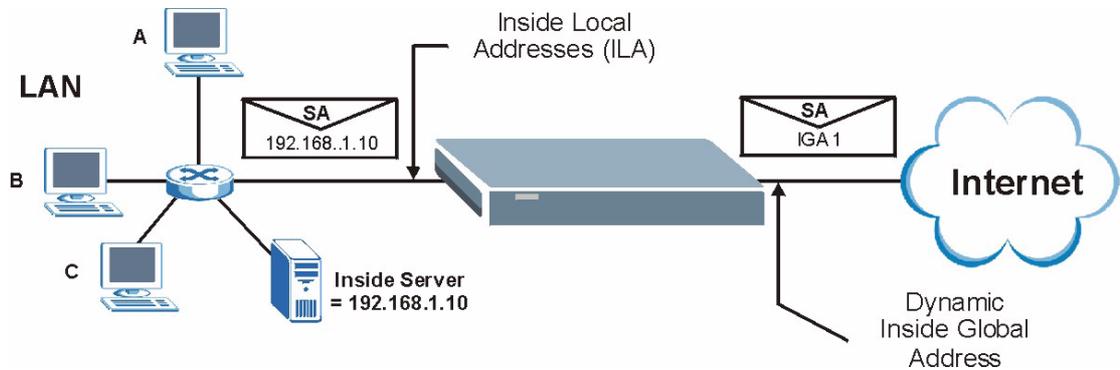
Press ENTER to Confirm or ESC to Cancel:

```

В Меню 4 в поле **Network Address Translation (Трансляция сетевых адресов)** выберите режим **SUA Only (Только SUA)**. Это тип отображения **Много-к-одному**, рассматриваемый в разделе [раздел Примеры применения NAT](#). Доступная только для чтения опция **SUA Only (Только SUA)** в поле **Network Address Translation (Трансляция сетевых адресов)** в Меню 4 и 11.3 специально предустановлена для работы в таком режиме.

21.5.2 Пример 2: Доступ в Интернет с внутренним сервером

Рис. 106 Пример применения NAT 2



В этом случае настройка выполняется аналогично описанной выше (используется предустановленная функция **SUA Only (Только SUA)**), далее необходимо перейти в Меню 15.2, чтобы определить внутренний сервер, расположенный за NAT, как показано на следующем рисунке.

Рис. 107 Меню 15.2.1 - Определение внутреннего сервера

Menu 15.2.1 - NAT Server Setup (Used for SUA Only)			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	192.168.1.10
2.	0	0	0.0.0.0
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

21.5.3 Пример 3: Несколько общедоступных IP-адресов для внутренних серверов

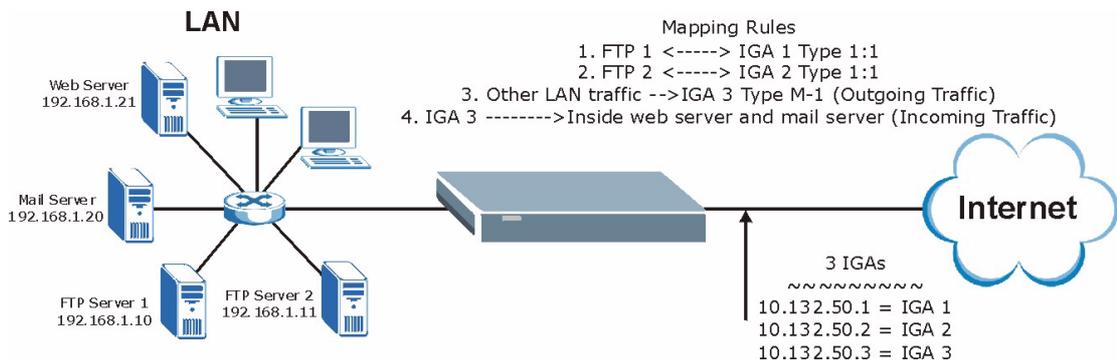
В данном примере существует три адреса IGA, предоставленных Интернет-провайдером. Имеется несколько отделов, и два из них имеют собственные серверы FTP. Все отделы используют один маршрутизатор. В примере каждому отделу с сервером FTP предоставляется по одному IGA и все отделы используют оставшийся IGA. Адреса

серверов FTP отображаются на два первых IGA, а остальной трафик локальной сети отображается на третий IGA. Третий IGA назначается внутреннему web-серверу и почтовому серверу. Для реализации такой конфигурации необходимо создать 4 правила: два для трафика в двух направлениях и два для однонаправленного трафика.

- 1 Первый IGA отображается на первый внутренний сервер FTP для трафика FTP в обоих направлениях (отображение **1: 1**, назначается локальный и глобальный IP-адрес).
- 2 Второй IGA отображается на второй внутренний сервер FTP для трафика FTP в обоих направлениях (отображение **1: 1**, назначается локальный и глобальный IP-адрес).
- 3 Третий IGA отображается на другой исходящий трафик локальной сети (отображение **Много: 1**).
- 4 Также третий IGA отображается на web-сервер и почтовый сервер локальной сети. Тип отображения **Server (Сервер)** позволяет определить несколько серверов для различных служб для других компьютеров, расположенных за NAT в локальной сети.

Приведенный пример представлен на следующем рисунке:

Рис. 108 Пример применения NAT 3



В данном случае необходимо создать **Набор отображения адресов 1** с помощью **Меню 15.1 - Наборы отображения адресов**. Следовательно, необходимо в поле **Network Address Translation (Трансляция сетевых адресов)** (в Меню 4 или 11.3) выбрать значение **Full Feature (Полный набор функциональных возможностей)** [Рис.109](#).

- 1 В Главном меню введите 15 .
- 2 Введите 1 для настройки наборов отображения адресов.
- 3 Введите 1 для настройки нового набора. Введите имя набора, выберите **Edit (Редактировать)** в поле **Action (Действие)** и затем введите 1 в поле **Select Rule (Выбор правила)**. Нажмите клавишу [ENTER] для подтверждения.
- 4 Выберите в поле **Type (Тип)** режим **One-to-One (Один-к-одному)** (прямое отображение для пакетов, передаваемых в обоих направлениях), и введите

локальный **начальный IP-адрес** как 192.168.1.10 (IP-адрес сервера FTP 1),
глобальный **начальный IP-адрес** как 10.132.50.1 (первый IGA). (См. [Рис.110](#)).

- 5** Повторите предыдущие действия для создания правил со 2-го по 4-е, как описано выше.

После завершения настройки Меню 15.1.1 должно выглядеть, как на [Рис.111](#).

Рис. 109 Пример 3: Меню 11.3

```
Menu 11.3 - Remote Node Network Layer Options
IP Options:                               Bridge Options:
  IP Address Assignment= Static           Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
NAT= Full Feature
  Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
  Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

Press ENTER to Confirm or ESC to Cancel:
```

На следующем рисунке показано, как настроить первое правило.

Рис. 110 Пример 3: Меню 15.1.1.1

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One
Local IP:
  Start= 192.168.1.10
  End = N/A
Global IP:
  Start= 10.132.50.1
  End = N/A
Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Рис. 111 Пример 3: Окончательный вид Меню 15.1.1

```

Menu 15.1.1 - Address Mapping Rules

Set Name= Example3
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.  192.168.1.10      10.132.50.1   1-1
2.  192.168.1.11      10.132.50.2   1-1
3.  0.0.0.0           255.255.255.255  10.132.50.3   M-1
4.                                     10.132.50.3   Server
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=
Press ENTER to Confirm or ESC to Cancel:

```

Теперь необходимо настроить отображение третьего IGA на web-сервер и почтовый сервер в локальной сети.

- 1** В Главном меню введите 15 .
- 2** Введите 2 в Меню 15 - Настройка NAT.
- 3** Введите 1 в Меню 15.2 - Наборы серверов за NAT для входа в следующее подменю. Настройте его, как показано ниже.

Рис. 112 Пример 3: Меню 15.2.1

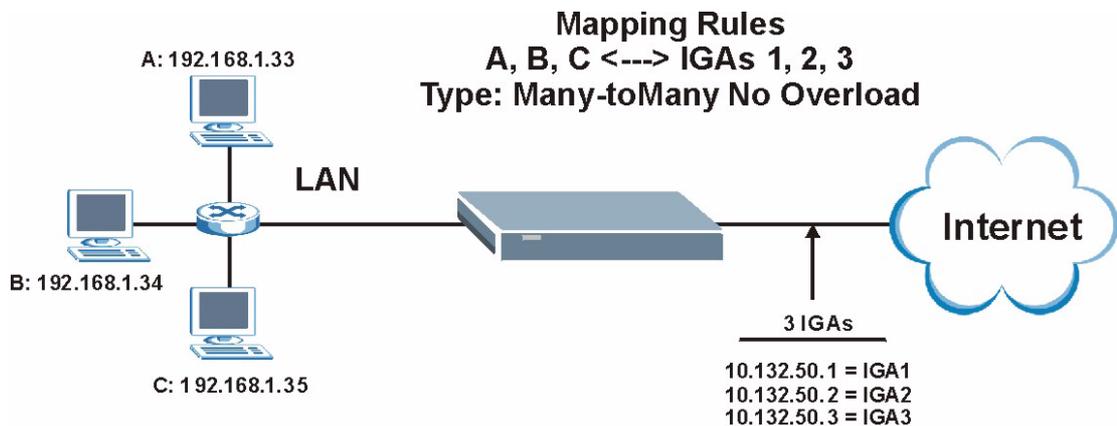
Menu 15.2.1 - NAT Server Setup				
Rule	Start Port No.	End Port No.	IP Address	
1.	Default	Default	0.0.0.0	
2.	80	80	192.168.1.21	
3.	25	25	192.168.1.20	
4.	0	0	0.0.0.0	
5.	0	0	0.0.0.0	
6.	0	0	0.0.0.0	
7.	0	0	0.0.0.0	
8.	0	0	0.0.0.0	
9.	0	0	0.0.0.0	
10.	0	0	0.0.0.0	
11.	0	0	0.0.0.0	
12.	0	0	0.0.0.0	

Press ENTER to Confirm or ESC to Cancel:

21.5.4 Пример 4: Прикладные программы, не поддерживающие NAT

Некоторые приложения не поддерживают отображение NAT с использованием преобразования адресов портов TCP или UDP. В таком случае необходимо использовать отображение **Много-ко-многим без перегрузки**, так как при типе отображения NAT **Много-ко-многим без перегрузки** (а также **Один-к-одному**) номера портов *не* изменяются. Пример показан на следующем рисунке.

Рис. 113 Пример применения NAT 4



Другие приложения, такие как некоторые игры, не поддерживают NAT, поскольку они вставляют информацию об адресации в поток данных. Такие приложения не будут работать через NAT, даже при использовании типов отображения **один-к-одному** и **много-ко-многим без перегрузки**.

Выполните действия, приведенные в примере 3, для настройки тех же двух меню, как показано ниже.

Рис. 114 Пример 4: Меню 15.1.1.1 - Правило отображения адресов

```

Menu 15.1.1.1 Address Mapping Rule

Type= Many-to-Many No Overload
Local IP:
    Start= 192.168.1.10
    End = 192.168.1.12
Global IP:
    Start= 10.132.50.1
    End = 10.132.50.3
Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

После того, как правило настроено, можно проверить настройки в меню 15.1.1, как показано ниже.

Рис. 115 Пример 4: Меню 15.1.1 - Правила отображения адресов

```

Menu 15.1.1 - Address Mapping Rules

Set Name= Example4
Idx  Local Start IP   Local End IP   Global Start IP  Global End IP   Type
---  -
  1.  192.168.1.10      192.168.1.12   10.132.50.1     10.132.50.3    M:M
NO OV
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

Action= Edit      Select Rule=
Press ENTER to Confirm or ESC to Cancel:

```

ГЛАВА 22

Настройка фильтров

В этой главе описывается создание и применение фильтров.

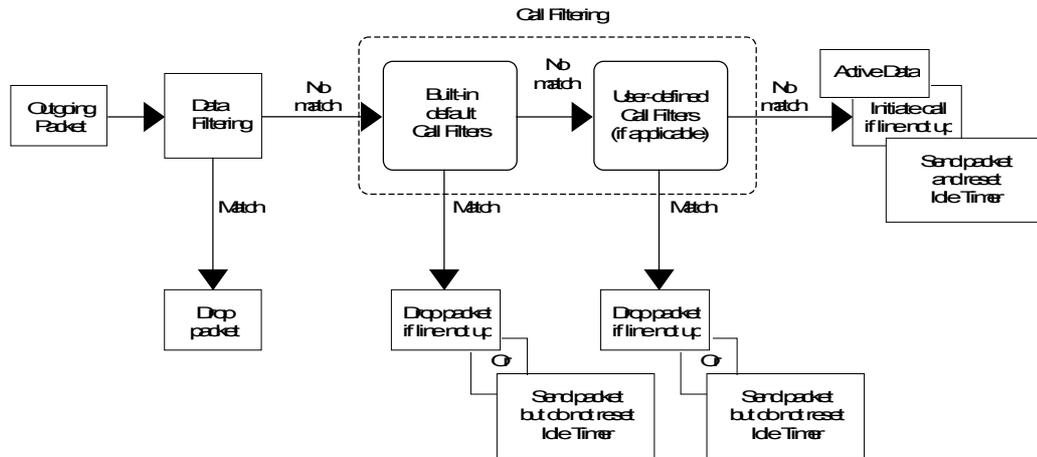
22.1 О фильтрации

Фильтры в модеме используются для принятия решения о разрешении или запрещении пересылки пакета данных и/или выполнения вызова. Фильтры имеют два вида применения: фильтрация данных и фильтрация вызовов. Фильтры подразделяются на фильтры устройств и фильтры протоколов. Далее рассматриваются оба типа фильтров.

Фильтры данных проверяют данные с целью определить разрешение на пересылку пакета. Фильтры данных подразделяются на входящие фильтры и исходящие фильтры в зависимости от направления пакета по отношению к порту. Фильтрация данных может применяться как на интерфейсе глобальной сети, так и на интерфейсе Ethernet. Фильтрация вызовов используется для определения, разрешить ли пакету инициировать вызов.

Исходящие пакеты сначала подвергаются проверке фильтрами данных, а затем поступают на фильтры вызовов. Фильтры вызовов разделяются на две группы: встроенные фильтры вызовов и фильтры вызовов, определяемые пользователем. Модем имеет встроенные фильтры вызовов, которые предотвращают инициирование вызовов управляющими пакетами, например, пакетами RIP. Эти фильтры всегда включены и недоступны для пользователя. Модем сначала применяет встроенные фильтры, а затем - пользовательские фильтры вызовов (если есть), как показано на следующем рисунке.

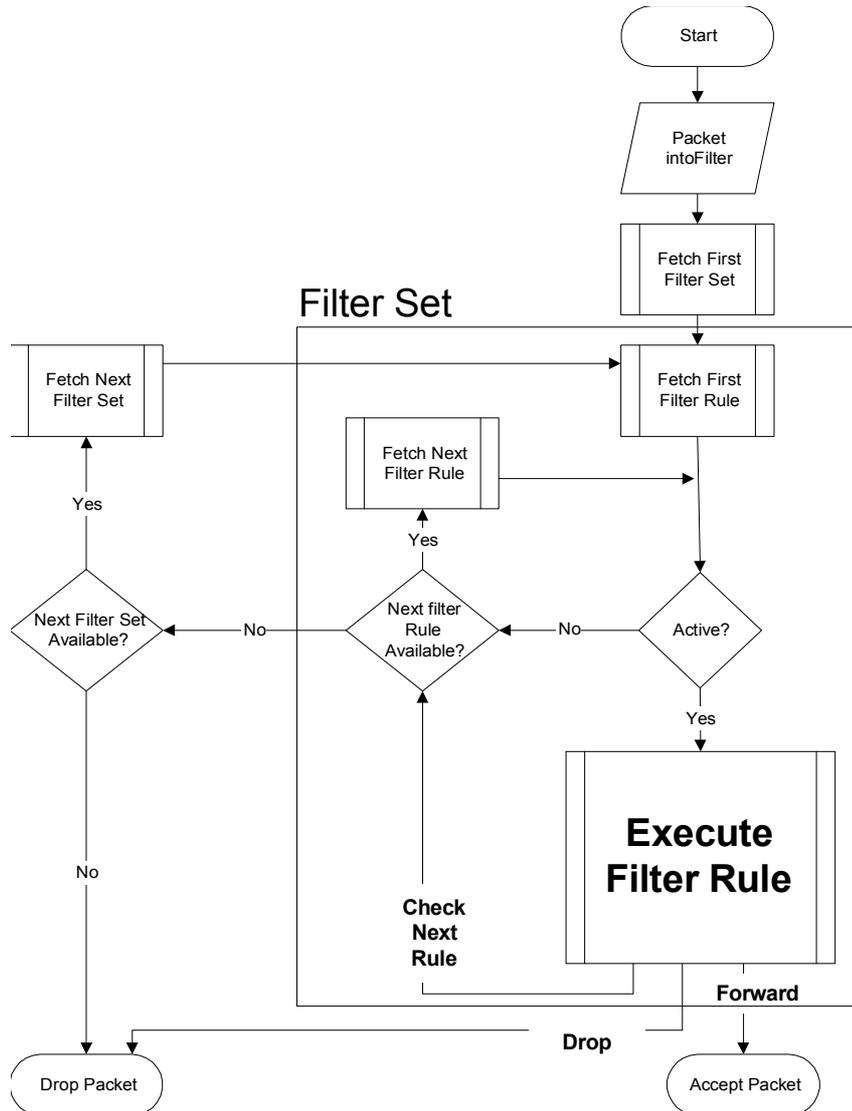
Рис. 116 Процесс фильтрации исходящего пакета



В Меню 21 изготовителем по умолчанию установлено два набора правил фильтров для предотвращения инициирования вызовов трафиком NetBIOS. Сводка правил фильтров показана на рисунках далее.

Следующий рисунок иллюстрирует логическую схему реализации правила фильтра.

Рис. 117 Процесс реализации правил фильтра



К конкретному порту можно применить до четырех наборов фильтров для блокировки пакетов различных типов. Так как в одном наборе может содержаться до шести правил, всего можно установить 24 правила для фильтрации данных каждого конкретного порта.

Для входящих пакетов модем применяет только фильтры данных. Пакеты обрабатываются в зависимости от соответствия правилам фильтра. В следующих разделах описывается настройка наборов фильтров.

22.1.1 Структура фильтра модема

Фильтр состоит из одного или нескольких правил, образующих набор фильтра. Обычно связанные правила группируются, например, все правила для NetBIOS создаются в одном наборе, которому присваивается описательное имя. Можно настроить до двенадцати наборов фильтров с шестью правилами в каждом наборе, итого в системе может быть 72 правила фильтрации.

22.2 Настройка набора фильтров для модема

Для настройки набора фильтров выполните следующие действия.

- 1 В Главном меню введите 21 для перехода в **Меню 21 – Настройка наборов фильтров**, как показано далее.

Рис. 118 Меню 21 - Настройка наборов фильтров

Menu 21 - Filter Set Configuration			
Filter Set #	Comments	Filter Set #	Comments
1	_____	7	_____
2	NetBIOS_WAN	8	_____
3	NetBIOS_LAN	9	_____
4	_____	10	_____
5	_____	11	WebSet1
6	_____	12	WebSet2

Enter Filter Set Number to Configure= 0
 Edit Comments= N/A
 Press ENTER to Confirm or ESC to Cancel:

- 2 В поле "Enter filter set number to configure" введите номер набора фильтров, который необходимо настроить (от 1 до 12), и нажмите клавишу [ENTER].
- 3 Введите описательное имя или комментарий в поле **Edit Comments (Редактировать комментарий)** и нажмите клавишу [ENTER].
- 4 В поле "Press [ENTER] to confirm..." нажмите клавишу [ENTER] для перехода в **Меню 21.1 - Сводка правил фильтра** (т.е., если выбран набор фильтров 1 в Меню 21).

Рис. 119 Сводка правил фильтра NetBIOS_WAN

```

Menu 21.2 - Filter Rules Summary

# A Type                Filter Rules                M m n
-----
1 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137      N D N
2 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138      N D N
3 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139      N D N
4 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137     N D N
5 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138     N D N
6 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139     N D F

Enter Filter Rule Number (1-6) to Configure:

```

Рис. 120 Сводка правил фильтра NetBIOS_LAN

```

Menu 21.1.3 - Filter Rules Summary

# A Type                Filter Rules                M m n
-----
1 Y IP  Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53  N D F
2 N
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure:

```

22.3 Сводное меню правил фильтра

В следующей таблице приводится краткое описание сокращений, используемых в Меню 21.1.1 и 21.1.2.

Табл. 53 Сокращения, используемые в меню Filter Rules Summary (Сводка правил фильтра)

ПОЛЕ	ОПИСАНИЕ
#	Номер правила фильтра: от 1 до 6.
A	Active (Включить): "Y" означает, что данное правило фильтра включено. "N" означает, что данное правило фильтра выключено.
Type (Тип)	Тип правила фильтра. Вариантами являются:"GEN" (общий) или "IP" (TCP/IP).
Filter Rules (Правила фильтра)	В этих полях отображаются параметры правила фильтра.

Табл. 53 Сокращения, используемые в меню Filter Rules Summary (Сводка правил фильтра) (продолжение)

ПОЛЕ	ОПИСАНИЕ
M	More (Дополнительно) "Y" означает, что есть еще правила, которые образуют цепочку правил с текущим правилом. Действие выполняется только после того, как проверена вся цепочка правил. "N" означает, что правил для проверки больше нет. Можно назначить действие, которое должно быть выполнено в результате проверки, например, переслать пакет, сбросить пакет или проверить по следующему правилу. Следующее правило не зависит от только что проверенного правила.
m	(Action Matched) Действие при соответствии. "F" означает немедленную пересылку пакета и пропуск проверки по оставшимся правилам. "D" означает сброс пакета. "N" означает проверку по следующему правилу.
n	Action Not Matched (Действие при несоответствии) "F" означает немедленную пересылку пакета и пропуск проверки по оставшимся правилам. "D" означает сброс пакета. "N" означает проверку по следующему правилу.

Сокращения для правил протоколно-зависимых фильтров представлены в следующей таблице:

Табл. 54 Сокращения, используемые в правилах

ТИП ФИЛЬТРА	ОПИСАНИЕ
IP	
Pr	Protocol (Протокол)
SA	Source Address (Адрес источника)
SP	Source Port Number (Номер порта источника)
DA	Destination Address (Адрес получателя)
DP	Destination Port Number (Номер порта получателя)
GEN	
Off	Offset (Смещение)
Len	Length (Длина)

22.4 Настройка правила фильтра

Для настройки правила фильтра введите его номер в **Меню 21.x – Сводка правил фильтра** и нажмите клавишу [ENTER] для перехода в Меню 21.x.1 для данного правила.

Существует два типа правил фильтров: **TCP/IP** и **Generic (Общий)**. В зависимости от типа, параметры правил могут различаться. Нажмите клавишу [ПРОБЕЛ] для выбора типа правила, которое вы хотите создать, в поле **Filter Type (Тип фильтра)**, затем нажмите клавишу [ENTER] для перехода в соответствующее меню.

Для увеличения скорости фильтрации, все правила в наборе фильтра должны быть одного и того же типа, например, или фильтр протоколов, или общий фильтр. Класс набора фильтра определяется по первому созданному правилу. При применении наборов фильтров к порту для наборов фильтров протоколов и наборов фильтров устройств предусмотрены разные поля. Если фильтр протоколов будет включен в набор фильтра устройств или наоборот, модем выдаст предупреждение и не разрешит сохранить конфигурацию.

22.4.1 Правило фильтра TCP/IP

В этом разделе описывается настройка правил фильтра TCP/IP. Фильтр TCP/IP позволяет создавать правила на основе полей в заголовках IP и протоколов верхнего уровня, например, UDP и TCP.

Для настройки правила TCP/IP, выберите в поле **Filter Type (Тип фильтра)** значение TCP/IP Filter Rule (Правило фильтра TCP/IP) и нажмите [ENTER] для перехода в **Меню 21.x.1 – Правило фильтра TCP/IP**, как показано ниже.

Рис. 121 Меню 21.x.1 - Правило фильтра 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

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описывается создание правила фильтра TCP/IP.

Табл. 55 Меню 21.x.1 - Правило фильтра TCP/IP

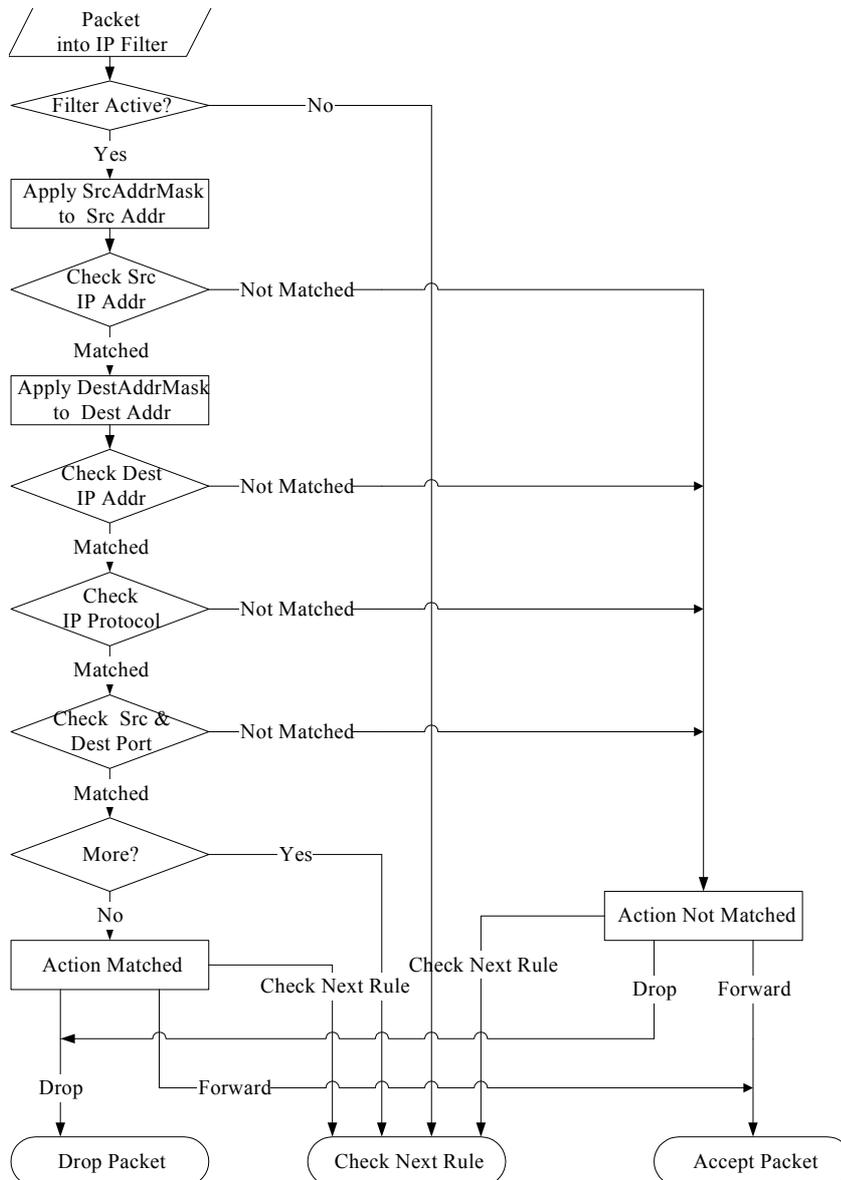
ПОЛЕ	ОПИСАНИЕ
Filter # (Номер фильтра)	Набор фильтра и номер правила фильтра, введенные через запятую, например, 2, 3 означает второй набор фильтров и третье правило фильтра в этом наборе.
Filter Type (Тип фильтра)	Нажмите клавишу [ПРОБЕЛ] и затем клавишу [ENTER] для выбора типа правила. Параметры, отображаемые для каждого типа фильтра, могут различаться. Вариантами являются: TCP/IP Filter Rule (Правило фильтра TCP/IP) или Generic Filter Rule (Правило общего фильтра) .
Active (Включить)	Выберите Yes (Да) для включения или No (Нет) для выключения данного правила фильтра.
IP Protocol (Протокол IP)	Это протокол верхнего уровня, например, TCP - 6, UDP - 17 и ICMP - 1. Значение должно быть в диапазоне от 0 до 255. Значение 0 соответствует ЛЮБОМУ протоколу.
IP Source Route (Маршрут источника IP)	Маршрут источника IP является дополнительным заголовком, определяющим маршрут, по которому IP-пакет направляется от источника к получателю. Если установлено Yes , правило применяется к любому пакету, имеющему маршрут источника IP. Большинство IP-пакетов не имеют маршрута источника.
Destination: (Получатель:)	
IP Addr (IP-адрес)	Введите IP-адрес получателя для пакетов, которые вы хотите фильтровать. Данное поле игнорируется, если его значение равно 0.0.0.0.
IP Mask (IP-маска)	Введите IP-маску для применения к полю Destination: IP Addr. (IP-адрес получателя)
Port # (Номер порта)	Введите номер порта получателя для фильтруемых пакетов. Значение поля должно находиться в диапазоне от 0 до 65535. Поле со значением 0 игнорируется.

Табл. 55 Меню 21.x.1 - Правило фильтра TCP/IP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Port # Comp (Сравнение номера порта)	Выберите критерий сравнения порта получателя в пакете со значением, установленным в поле Destination: Port # (Получатель: Номер порта) . Вариантами являются: None (Нет) , Less (Меньше) , Greater (Больше) , Equal (Равно) или Not Equal (Не равно) .
Source (Источник):	
IP Addr (IP-адрес)	Введите IP-адрес источника для фильтруемых пакетов. Если значение поля равно 0.0.0.0, данное поле игнорируется.
IP Mask (IP-маска)	Введите IP-маску для применения к полю Source: IP Addr. (IP-адрес источника)
Port # (Номер порта)	Введите номер порта источника для фильтруемых пакетов. Значение поля должно находиться в диапазоне от 0 до 65535. Поле со значением 0 игнорируется.
Port # Comp (Сравнение номера порта)	Выберите критерий сравнения порта источника в пакете со значением, установленным в поле Source: Port #. (Номер порта источника). Вариантами являются: None (Нет) , Less (Меньше) , Greater (Больше) , Equal (Равно) или Not Equal (Не равно) .
TCP Estab (Установить соединение TCP)	Применяется только тогда, когда значение поля IP Protocol (Протокол IP) равно 6, т.е. TCP. Если установлено Yes (Да) , правило соответствует пакетам, которые предназначены для установления соединения TCP (SYN=1 и ACK=0); в противном случае правило игнорируется.
More (Дополнительно)	Если установлено значение Yes (Да) , соответствующий правилу пакет проверяется по следующему правилу фильтра, перед тем как будет выполнено заданное действие; в противном случае пакет обрабатывается в соответствии с полями, где назначены действия. Если в поле More (Дополнительно) установлено Yes (Да) , то поля Action Matched (Действие при соответствии) и Action Not Matched (Действие при несоответствии) являются недоступными (N/A).
Log (Регистрационный журнал)	Выберите режим регистрации пакетов из следующих вариантов: None (Нет) – Пакеты не регистрируются в журнальном файле. Action Matched (Действие при соответствии) - Регистрируются только пакеты, соответствующие параметрам правила. Action Not Matched (Действие при несоответствии) - Регистрируются только пакеты, не соответствующие параметрам правила. Both (Все) – Все пакеты регистрируются в журнальном файле.
Action Matched (Действие при соответствии)	Выберите действие для применения к пакету, для которого обнаружено соответствие правилу. Вариантами являются: Check Next Rule (Проверить по следующему правилу) , Forward (Переслать) или Drop (Сбросить) .
Action Not Matched (Действие при несоответствии)	Выберите действие для применения к пакету, для которого соответствие правилу не обнаружено. Вариантами являются: Check Next Rule (Проверить по следующему правилу) , Forward (Переслать) или Drop (Сбросить) .
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

На следующем рисунке представлена логическая схема фильтра IP.

Рис. 122 Применение фильтра IP



22.4.2 Правило общего фильтра

В этом разделе описывается настройка правила общего фильтра. Общие фильтры служат для фильтрации не IP-пакетов. Для пакетов IP проще использовать правила IP.

При применении общих правил модем обрабатывает пакеты, как поток байтов, в противоположность пакетам IP. Вы определяете размер пакета для проверки с помощью полей **Offset (смещение)** (от 0) и **Length (Длина)**, оба измеряются в байтах. Модем применяет маску (побитовое осуществление операции "И") к блоку данных перед сравнением результата со значением поля Value, по которому определяется

соответствие. Поля **Mask (Маска)** и **Value (Значение)** вводятся в шестнадцатиричном формате. Следует отметить, что для записи одного байта требуется две шестнадцатиричные цифры, поэтому если длина равна 4, значение каждого поля будет занимать восемь разрядов, например, FFFFFFFF.

Для настройки общего правила выберите свободный набор фильтров в Меню 21, например, 5. Выберите **Generic Filter Rule (Правило общего фильтра)** в поле **Filter Type (Тип фильтра)** и нажмите клавишу [ENTER] для перехода в Меню **21.5.1 – Правило общего фильтра**, как показано на следующем рисунке.

Рис. 123 Меню 21.5.1 - Правило общего фильтра

```

Menu 21.5.1 - Generic Filter Rule

Filter #: 5,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице приводятся описания полей Меню - **Правило общего фильтра**.

Табл. 56 Меню 21.1.5.1 - Правило общего фильтра

ПОЛЕ	ОПИСАНИЕ
Filter # (Номер фильтра)	Набор фильтра и номер правила фильтра, введенные через запятую, например, 2, 3 означает второй набор фильтров и третье правило фильтра в этом наборе.
Filter Type (Тип фильтра)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора типа правила. Параметры, отображаемые для каждого типа фильтра, будут различаться. Вариантами являются: TCP/IP Filter Rule (Правило фильтра TCP/IP) или Generic Filter Rule (Правило общего фильтра) .
Active (Включить)	Выберите Yes (Да) для включения или No (Нет) для выключения правила фильтра.
Offset (Смещение)	Введите начальный байт блока данных в пакете, для которого будет производиться сравнение. Диапазон значений данного поля от 0 до 255.
Length (Длина)	Введите количество байтов для блока данных в пакете, для которого будет производиться сравнение. Диапазон значений данного поля от 0 до 8.
Mask (Маска)	Введите маску (в шестнадцатеричном формате) для применения к блоку данных перед сравнением.
Value (Значение)	Введите значение (в шестнадцатеричном формате) для сравнения с блоком данных.

Табл. 56 Меню 21.1.5.1 - Правило общего фильтра (продолжение)

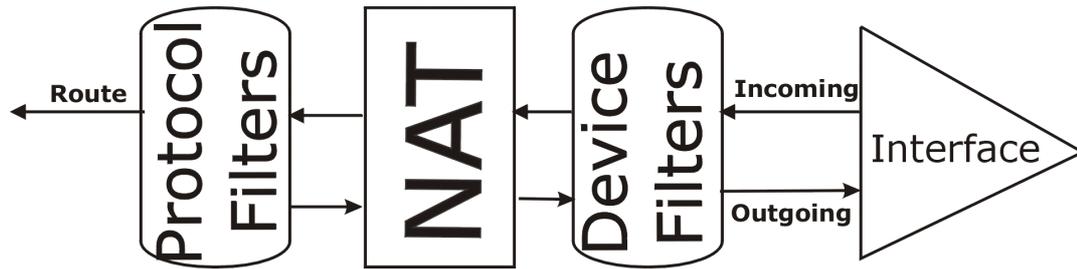
ПОЛЕ	ОПИСАНИЕ
More (Дополнительно)	Если установлено значение Yes (Да) , соответствующий правилу пакет проверяется по следующему правилу фильтра, перед тем как будет выполнено заданное действие; в противном случае пакет обрабатывается в соответствии с полями, где назначены действия. Если в поле More (Дополнительно) установлено Yes (Да) , то поля Action Matched (Действие при соответствии) и Action Not Matched (Действие при несоответствии) являются недоступными (N/A).
Log (Регистрационный журнал)	Выберите режим регистрации пакетов из следующих вариантов: None (Нет) – Пакеты не регистрируются в журнальном файле. Action Matched (Действие при соответствии) – Регистрируются только пакеты, соответствующие параметрам правила. Action Not Matched (Действие при несоответствии) - Регистрируются только пакеты, не соответствующие параметрам правила. Both (Все) – Все пакеты регистрируются в журнальном файле.
Action Matched (Действие при соответствии)	Выберите действие для применения к пакету, для которого обнаружено соответствие правилу. Вариантами являются: Check Next Rule (Проверить по следующему правилу) , Forward (Переслать) или Drop (Сбросить) .
Action Not Matched (Действие при несоответствии)	Выберите действие для применения к пакету, для которого соответствие правилу не обнаружено. Вариантами являются: Check Next Rule (Проверить по следующему правилу) , Forward (Переслать) или Drop (Сбросить) .
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

22.5 Типы фильтров и NAT

Существуют два класса правил фильтра: правила **общего фильтра для устройств** и правила фильтра протоколов (**TCP/IP**). Правила общих фильтров применяются к необработанным данным, передаваемым из/в LAN и WAN. Правила фильтра протоколов применяются к пакетам IP.

Если включена функция NAT (Network Address Translation - Трансляция сетевых адресов), внутренний IP-адрес и номер порта меняются от соединения к соединению, в результате чего становится невозможным выявить точные значения адреса и номера порта. Поэтому, модем применяет фильтры протоколов к исходному IP-адресу и номеру порта до NAT для исходящих пакетов и после NAT - для входящих пакетов. С другой стороны, общие фильтры (или фильтры устройств), применяются к необработанным пакетам, которые поступают из линии передачи. Такие фильтры применяются в точке, где модем осуществляет прием или передачу пакетов, например, на интерфейсе. Интерфейсом может быть порт Ethernet или любой другой аппаратный порт. Применение фильтров показано на следующем рисунке.

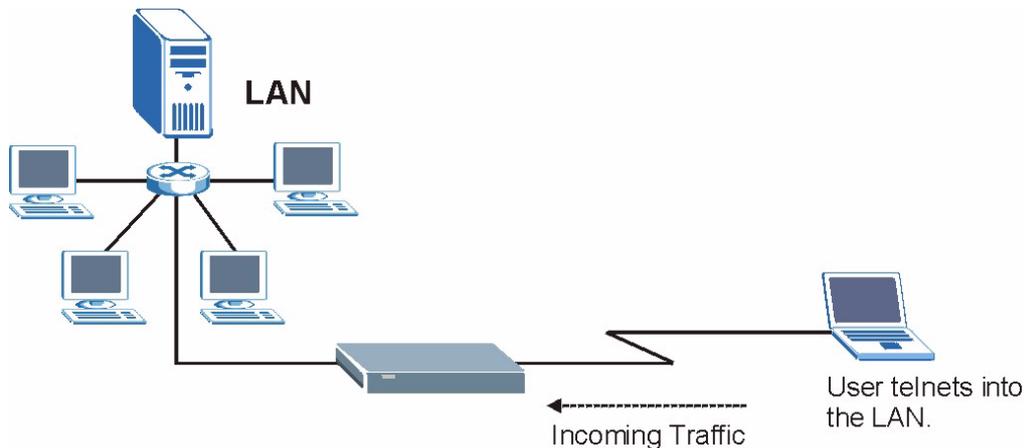
Рис. 124 Наборы фильтров протоколов и фильтров устройств



22.6 Пример фильтра

Рассмотрим пример блокировки подключения к модему внешних пользователей через Telnet.

Рис. 125 Пример фильтра Telnet



- 1 В Главном меню введите 21 для перехода в **Меню 21 — Настройка набора фильтров**.
- 2 Введите номер набора фильтров, который необходимо настроить (в данном случае 6).
- 3 Введите описательное имя или комментарий в поле **Edit Comments (Редактировать комментарий)** (например, TELNET_WAN) и нажмите клавишу [ENTER].
- 4 Нажмите [ENTER] в строке “Press [ENTER] to confirm or [ESC] to cancel ...” для перехода в **Меню 21.6 — Сводка правил фильтра**.
- 5 Введите 1 для создания первого правила фильтра. Настройте параметры в меню, как показано далее.

После нажатия клавиши [ENTER] для подтверждения настроек, появляется следующий экран. Обратите внимание, что в этом наборе только одно правило фильтра.

Рис. 126 Меню 21.6.1 - Пример фильтра

```

Menu 21.6.1 - TCP/IP Filter Rule

Filter #: 6,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port # = 23
              Port # Comp= Equal
Source:       IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port # =
              Port # Comp= Equal

TCP Estab= No
More= No           Log= None
Action Matched= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:

```

Рис. 127 Меню 21.6.1 - Сводка правил фильтра, созданного в примере

```

Menu 21.1.6 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
-----
1 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23           N D F
2 N
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure: 1

```

Данное меню показывает, что вы создали и включили (**A = Y**) правило фильтра TCP/IP (**Type = IP, Pr = 6**) для портов Telnet (**DP = 23**) получателя.

M = N означает, что действие фильтра будет выполнено немедленно. Действием является сброс пакета (**m = D**), если пакет соответствует правилу, или немедленная пересылка пакета (**n = F**), если пакет не соответствует правилу, независимо от того, есть ли еще правила для проверки (в данном примере правил больше нет).

После создания набора фильтров его необходимо применить.

- 1 В Главном меню введите 11 для перехода в Меню 11 и введите номер удаленного узла для редактирования.

- 2 Переместите курсор в поле **Edit Filter Sets (Редактировать наборы фильтров)** и нажмите клавишу [ПРОБЕЛ] для выбора **Yes**, а затем нажмите клавишу [ENTER].
- 3 Появляется Меню 11.5. Примените набор фильтров (например, набор фильтров 3) в этом Меню, как показано в следующем разделе.

22.7 Применение фильтров и заводских настроек по умолчанию

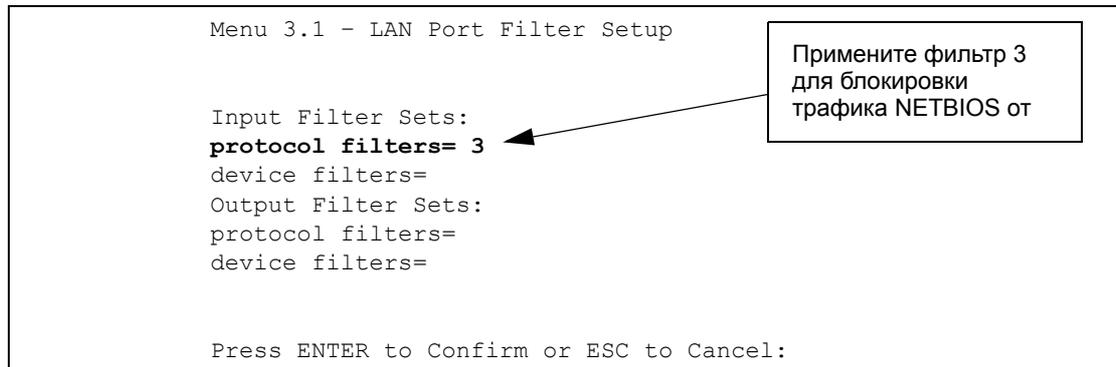
В данном разделе рассматривается, где следует применять фильтр(ы) после его (их) создания. В Меню 21 изготовителем настроены (но не применены) наборы правил фильтров по умолчанию.

Табл. 57 Таблица наборов фильтров

НАБОРЫ ФИЛЬТРОВ	ОПИСАНИЕ
Наборы входных фильтров:	Фильтры применяются для входящего трафика. Можно применять правила фильтров протоколов или фильтров устройств. Более подробно о типах фильтров см. выше в данной главе.
Наборы выходных фильтров:	Фильтры применяются для исходящего трафика модема. Можно применять правила фильтров протоколов или фильтров устройств. Более подробно о типах фильтров см. выше в данной главе.
Наборы фильтров вызовов:	Фильтры применяются для определения, следует ли разрешить конкретному пакету инициировать вызов.

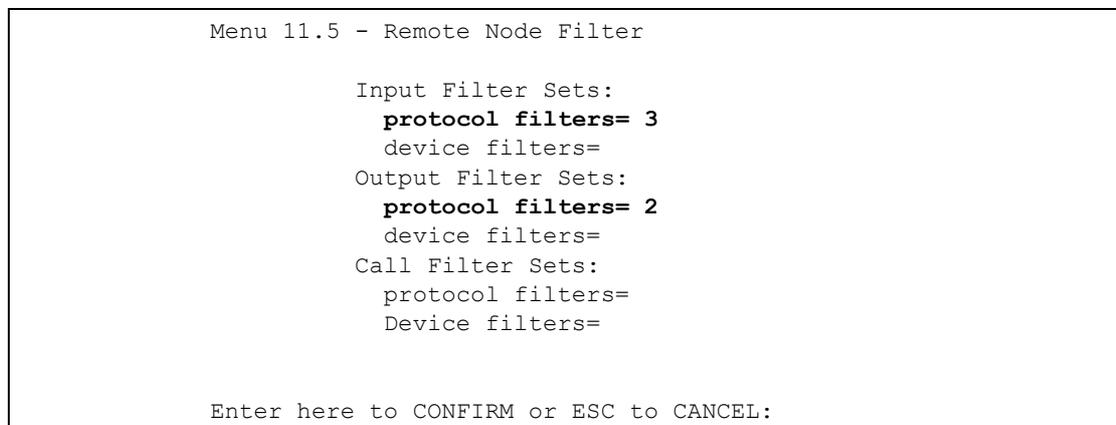
22.7.1 Трафик Ethernet

Необходимость в фильтрации трафика Ethernet возникает редко; тем не менее, наборы фильтров могут быть полезными для блокировки определенных пакетов, снижения объема трафика и предотвращения несанкционированного доступа. Перейдите в Меню 3.1 (показано ниже) и введите номер(а) набора(ов) фильтров, которые вы считаете целесообразным применить. Можно применять до четырех наборов фильтров (из двенадцати) посредством ввода их номеров через запятую, например, 3, 4, 6, 11. Набор фильтров, настроенный изготовителем, NetBIOS_ LAN, установлен в поле **protocol filters (фильтры протоколов)** в разделе **Input Filter Sets (Наборы входных фильтров)** Меню 3.1 с целью предотвращения генерирования вызовов на сервер DNS локальными сообщениями NetBIOS.

Рис. 128 Фильтрация трафика Ethernet

22.7.2 Фильтры для удаленного узла

Перейдите в Меню 11.5 (показано ниже) и введите номер(а) набора(ов) фильтров для конкретной конфигурации. Можно применить последовательно до четырех наборов фильтров посредством ввода их номеров через запятую. Набор фильтров, настроенный изготовителем, NetBIOS _ WAN, установлен в поле **protocol filters (фильтры протоколов)** в разделе **Call Filter Sets (Наборы фильтров вызовов)** Меню 11.5 и служит для блокировки вызовов Интернет-провайдера локальным трафиком NetBIOS.

Рис. 129 Фильтрация трафика удаленного узла

Следует учитывать, что наборы фильтров вызовов доступны, только если выбрана инкапсуляция PPPoA или PPPoE.

ГЛАВА 23

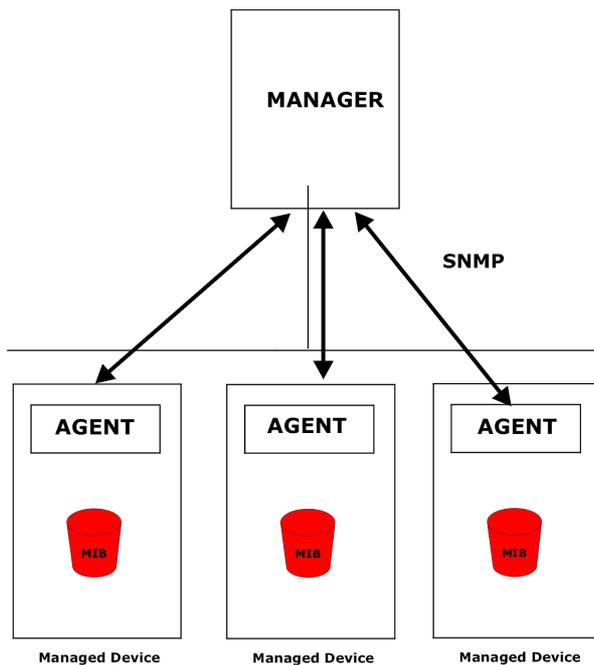
Настройка SNMP

В этой главе описывается Меню 22 - Настройка SNMP.

23.1 О протоколе SNMP

Простой протокол управления сетью (SNMP - Simple Network Management Protocol) используется для осуществления обмена управляющей информацией между сетевыми устройствами. SNMP является одним из элементов стека протоколов TCP/IP. Модем поддерживает функциональные возможности агента SNMP, что позволяет выполнять мониторинг и управление модемом по сети с управляющей станции. Модем поддерживает SNMP версии 1 (SNMPv1) и версии 2 (SNMPv2c). На следующем рисунке показана модель управления по протоколу SNMP. Протокол SNMP является доступным, только если настроен TCP/IP.

Рис. 130 Модель управления SNMP



Сеть, управляемая по протоколу SNMP, состоит из двух основных компонентов: агентов и управляющей программы.

Агент представляет собой модуль программы управления, установленный в управляемом устройстве (в модеме). Агент производит преобразование информации локального управления от управляемого устройства в форму, совместимую с SNMP. Управляющая программа - это консоль управления, с помощью которой сетевые администраторы осуществляют функции управления сетью. С помощью консоли запускаются приложения для контроля и мониторинга управляемых устройств.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют каждую порцию информации, собираемой об этих устройствах. Примерами переменных являются: число принятых пакетов, состояние порта узла и т.д. MIB (Management Information Base - База управляющей информации) - это совокупность данных об управляемых объектах. Протокол SNMP позволяет управляющей программе и агентам взаимодействовать друг с другом с целью доступа к этим объектам.

Протокол SNMP является простым протоколом типа "запрос-ответ" на основе модели "управляющая программа/агент". Управляющая станция посылает запрос, а агент возвращает ответы с помощью следующих протокольных операций:

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

23.2 Поддерживаемые базы управляющей информации

Модем поддерживает RFC-1215 и MIB II, описываемую в RFC-1213, а также собственные MIB корпорации ZyXEL. Базы управляющей информации позволяют сетевым администраторам накапливать статистические данные и выполнять мониторинг состояния и производительности сети.

23.3 Настройка SNMP

Для настройки SNMP в Главном меню введите **22** для перехода в **Меню 22 - Настройка SNMP**, как показано ниже. "Community" для полей "Get", "Set" и "Trap" является просто термином SNMP, обозначающим пароль.

Рис. 131 Меню 22 - Настройка SNMP

```

Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
Trap:
  Community= public
  Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описываются параметры конфигурации SNMP.

Табл. 58 Меню 22 - Настройка SNMP

ПОЛЕ	ОПИСАНИЕ
SNMP:	
Get Community (Пароль 'Get')	Введите параметр Get Community (Пароль Get) , который является паролем для входящих запросов Get- и GetNext- от управляющей станции.
Set Community (Пароль 'Set')	Введите параметр Set Community (Пароль Set) , который является паролем для входящих запросов Set от управляющей станции.
Trusted Host (Доверенный узел)	Если введен адрес доверенного узла, модем будет отвечать только на сообщения SNMP, принятые с этого адреса. Если это поле оставлено пустым (по умолчанию), модем будет отвечать на все принятые сообщения SNMP, независимо от их источника.
Trap: (Прерывание:)	
Community (Пароль)	Введите пароль Trap, передаваемый с каждым прерыванием на управляющую станцию SNMP.
Destination: (Адресат:)	Введите IP-адрес станции, на которую будут посылаться прерывания SNMP.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

23.4 Прерывания SNMP

Модем посылает прерывания на управляющую станцию SNMP, если произошло какое-либо из следующих событий:

Табл. 59 Прерывания SNMP

НОМЕР ПРЕРЫВАНИЯ #	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
1	coldStart (описывается в RFC-1215)	Прерывание посылается после начальной загрузки (включения питания).
2	warmStart (описывается в RFC-1215)	Прерывание посылается после загрузки (программная перезагрузка).
3	linkDown (описывается в RFC-1215)	Прерывание посылается с указанием номера порта, когда какой-либо из каналов связи не работает. См. следующую таблицу.
4	linkUp (описывается в RFC-1215)	Прерывание об установлении соединения посылается с указанием номера порта.
5	authenticationFailure (описывается в RFC-1215)	Прерывание посылается на управляющую станцию при приеме запросов get или set SNMP с неверным паролем.
6	whyReboot (описывается в MIB ZYXEL)	Прерывание посылается с указанием кода причины перезапуска перед перезапуском, если система собирается выполнить перезапуск ("горячий" запуск).
6a	Для преднамеренной перезагрузки:	Прерывание посылается с сообщением "System reboot by user!" (перезагрузка системы пользователем), когда перезагрузка производится намеренно (например, загрузка новых файлов, команда "sys reboot" и т.д.).

Номером порта является индекс его интерфейса в группе интерфейсов.

Табл. 60 Порты и постоянные виртуальные каналы

ПОРТ	PVC
1	LAN Ethernet
2	1
3	2
...	...
13	12
14	xDSL

ГЛАВА 24

Информация о системе и диагностика

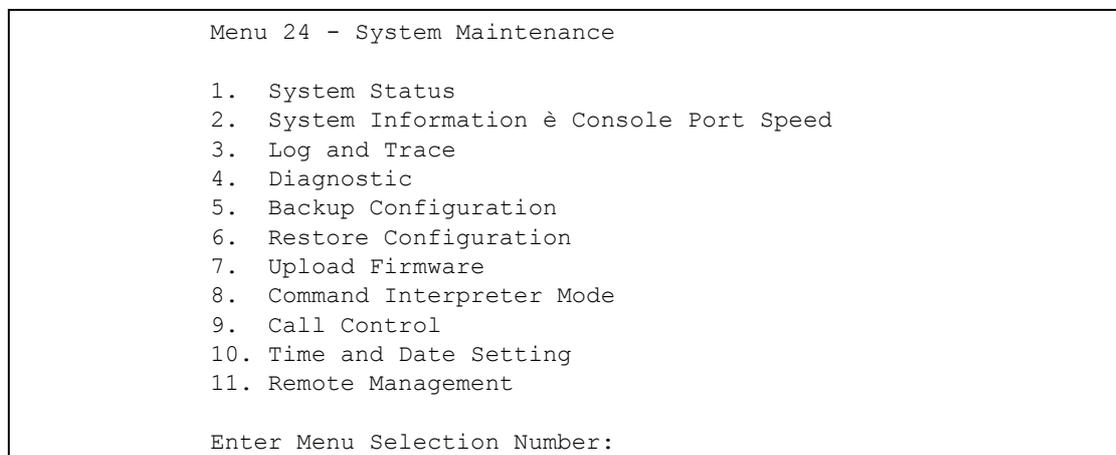
В этой главе описывается информация о системе и средства диагностики, которые содержатся в Меню SMT с 24.1 по 24.4.

24.1 Обзор

Средства диагностики включают обновление состояния системы и состояния портов, системные журналы регистрации событий и трассировки, а также обновление микропрограммы системы. Далее в настоящей главе эти средства описываются более подробно.

В Главном меню введите 24 для перехода в **Меню 24 – Сопровождение системы**, как показано на следующем рисунке.

Рис. 132 Меню 24 - Сопровождение системы



24.2 Состояние системы

При выборе первого пункта - System Status (Состояние системы) - выводится информация о состоянии и статистике портов, как показано ниже. Состояние системы является средством, которое используется для контроля функционирования модема. В частности, отображается информация о состоянии ADSL линии и количестве переданных и принятых пакетов.

Для получения информации о состоянии системы введите 24 для перехода в **Меню 24 – Сопровождение системы**. В Меню 24 введите 1 для перехода в меню **System Status (Состояние системы)**. **Меню 24.1 – Сопровождение системы – Состояние** включает две команды. При вводе 1 сбрасываются счетчики; при нажатии клавиши [ESC] производится возврат к предыдущему экрану.

В следующей таблице описываются поля **Меню 24.1 – Сопровождение системы – Состояние**, которые выводятся в режиме ТОЛЬКО ДЛЯ ЧТЕНИЯ и используются для диагностики.

Рис. 133 Меню 24.1 - Сопровождение системы: Состояние

```

Menu 24.1 - System Maintenance - Status                                03:05:59
                                                                    Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s      Up
Time
1-PPPoE Idle         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: 23216   Line Status: Down
  Collisions: 0           Rx Pkts: 23740   Upstream Speed: 0 Kbps
CPU Load = 1.65%           Downstream Speed: 0 Kbps

Press Command:
COMMANDS: 1-Reset Counters  Esc-Exit

```

В следующей таблице описываются поля **Меню 24.1 - Сопровождение системы - Состояние**.

Табл. 61 Меню 24.1 - Сопровождение системы: Состояние

ПОЛЕ	ОПИСАНИЕ
Node-Link (Номер - Вид соединения)	Номер удаленного узла и тип соединения. Вариантами соединения являются: PPP, ENET, 1483.
Status (Состояние)	Здесь отображается состояние удаленного узла.
TxPkts (Передано пакетов)	Количество пакетов, переданных на данный удаленный узел.
RxPkts (Принято пакетов)	Количество пакетов, принятых от данного удаленного узла.

Табл. 61 Меню 24.1 - Сопровождение системы: Состояние (продолжение)

ПОЛЕ	ОПИСАНИЕ
Errors (Ошибки)	Количество пакетов, принятых с ошибками по данному соединению.
Tx B/s (Скорость передачи, байт/с)	Здесь отображается скорость передачи в байтах в секунду.
Rx B/s (Скорость приема, байт/с)	Здесь отображается скорость приема в байтах в секунду.
Up Time (Время соединения)	Время соединения с текущим удаленным узлом.
My WAN IP (from ISP) (IP адрес глобальной сети (от Интернет-провайдера))	IP-адрес удаленного узла Интернет-провайдера.
Ethernet	Здесь отображается статистика порта LAN.
Status (Состояние)	Здесь отображается текущее состояние порта LAN.
Tx Pkts (Передано пакетов)	Количество пакетов, переданных в локальную сеть.
Rx Pkts (Принято пакетов)	Количество пакетов, принятых из локальной сети.
Collision (Конфликты)	Количество конфликтов.
WAN	Здесь отображается статистика порта WAN.
Line Status (Состояние линии)	Здесь отображается текущее состояние линии xDSL: Up (Работает) или Down (Не работает) .
Upstream Speed (Скорость исходящего трафика)	Здесь отображается скорость передачи исходящего трафика в кбит/с.
Downstream Speed (Скорость входящего трафика)	Здесь отображается скорость передачи входящего трафика в кбит/с.
CPU Load (Загрузка ЦП)	Здесь отображается процент загрузки процессора модема.

24.3 Информация о системе

Для получения информации о системе:

- 1 Введите 24 для перехода в **Меню 24 - Сопровождение системы**.

2 Введите 2 для перехода в **Меню 24.2 - Информация о системе и скорость консольного порта.**

В этом меню имеется два варианта выбора информации для отображения, как показано на следующем рисунке.

Рис. 134 Меню 24.2 - Информация о системе и скорость консольного порта

```
Menu 24.2 - System Information and Console Port Speed

1. System Information
2. Console Port Speed

Please enter selection:
```



ПРИМЕЧАНИЕ: Модем имеет внутренний консольный порт только для обслуживающего персонала. Не вскрывайте модем, так как это может привести к потере гарантийного обслуживания устройства.

24.3.1 Информация о системе

В Меню 24.2 введите 1 для отображения следующего экрана.

Рис. 135 Меню 24.2.1 - Сопровождение системы: Информация

```

Menu 24.2.1 - System Maintenance -
Information

Name:
Routing: IP
ZyNOS F/W Version: V3.40(ST.0) | 12/16/2004
ADSL Chipset Vendor: DMT FwVer: 3.0.10.3_A_TC, HwVer: T14F7_0.+
Standard: Multi-Mode

LAN
Ethernet Address: 00:a0:c5:01:23:45
IP Address 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:

```

В следующей таблице описываются поля данного меню.

Табл. 62 Меню 24.2.1 - Сопровождение системы: Информация

ПОЛЕ	ОПИСАНИЕ
Name (Имя)	Здесь отображается системное имя модема. Данный параметр можно изменить в Меню 1 - Настройка общих параметров .
Routing (Маршрутизация)	Здесь отображается протокол, который используется для маршрутизации.
ZyNOS F/W Version (Версия ПО ZyNOS)	Здесь отображается версия системной микропрограммы ZyNOS (ZyXEL Network Operating System - Сетевая операционная система ZyXEL). ZyNOS является зарегистрированной торговой маркой ZyXEL Communications Corporation.
ADSL Chipset Vendor (Производитель микросхемы ADSL)	Здесь отображается производитель микросхемы ADSL и версия DSL.
Standard (Стандарт)	Здесь отображается рабочий протокол, используемый модемом и DSL-коммутатором.
LAN	
Ethernet Address (Ethernet адрес)	Здесь отображается MAC-адрес модема (Media Access Control - Управление доступом к среде) или иначе Ethernet адрес.
IP Address (IP-адрес)	Здесь отображается IP-адрес модема в десятичном формате с разделительными точками.
IP Mask (IP-маска)	Здесь отображается маска подсети модема.
DHCP	Здесь отображается режим DHCP модема: None (Отключить), Relay (Ретранслятор) или Server (Сервер).

24.3.2 Скорость консольного порта

В Меню 24.2.2 – Сопровождение системы – Скорость консольного порта можно установить различную скорость для консольного порта. Модем поддерживает скорости: 9600 (по умолчанию), 19200, 38400, 57600 и 115200 бит/с. Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора требуемой скорости в Меню 24.2.2, как показано на следующем рисунке.

Рис. 136 Меню 24.2.2 - Сопровождение системы: Изменение скорости консольного порта

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

Console Port Speed: 9600

Press ENTER to Confirm or ESC to Cancel:
```

24.4 Журнал регистрации и трассировка

Модем имеет две функции журнальной регистрации. Первая - ведение журналов регистрации ошибок и результатов трассировок, которые хранятся локально. Вторая - ведение системного журнала для регистрации сообщений.

24.4.1 Просмотр журнала регистрации ошибок

При появлении отказов сначала необходимо просмотреть журнал регистрации ошибок для установления причин их возникновения. Для просмотра локального журнала регистрации ошибок/трассировки выполните следующие действия:

- 1 В Главном меню введите 24 для перехода в **Меню 24 - Сопровождение системы**.
- 2 В Меню 24 введите 3 для перехода в **Меню 24.3 – Сопровождение системы – Журнал регистрации и трассировка**.

Рис. 137 Меню 24.3 - Сопровождение системы: Журнал регистрации и трассировка

```
Menu 24.3 - System Maintenance - Log and Trace

1. View Error Log
2. UNIX Syslog

Please enter selection
```

- 3 Выберите первую опцию в **Меню 24.3 - Сопровождение системы - Журнал регистрации и трассировка** для просмотра журнала регистрации ошибок в системе.

После того как модем выполнит отображение журнала регистрации ошибок, можно очистить журнал, удалив все записи. Примеры типичных сообщений об ошибках и уведомлениях приведены на следующем рисунке.

Рис. 138 Пример сообщений об ошибках и уведомлениях

```
52 Sat Jan 01 00:00:00 2000 PP12 INFO LAN promiscuous mode <1>
53 Sat Jan 01 00:00:00 2000 PP00 INFO Last errorlog repeat 1 Times
54 Sat Jan 01 00:00:00 2000 PP00 -WARN SNMP TRAP 0: cold start
55 Sat Jan 01 00:00:00 2000 PP00 INFO main: init completed
56 Sat Jan 01 00:00:00 2000 PP00 INFO Starting Connectivity Monitor
57 Sat Jan 01 00:00:00 2000 PP1c INFO monitoring WAN connectivity
58 Sat Jan 01 00:00:00 2000 PP0a WARN MPOA Link Down
59 Sat Jan 01 00:00:02 2000 PP09 -WARN SNMP TRAP 3: link up
60 Sat Jan 01 00:00:05 2000 PP1b INFO adjtime task pause 1 day
61 Sat Jan 01 00:01:36 2000 PP14 INFO SMT Password pass
62 Sat Jan 01 00:01:36 2000 PP00 INFO SMT Session Begin
63 Sat Jan 01 00:03:59 2000 PP00 WARN M1Save:Iface not found for DDNS
Clear Error Log (y/n) :
```

24.4.2 Системный журнал и учет ресурсов

Модем использует функцию системного журнала для записи CDR (Call Detail Record - Запись о деталях установления вызова) и системных сообщений на сервере системного журнала (syslog сервере). Параметры системного журнала и учета ресурсов можно настраивать в **Меню 24.3.2 – Сопровождение системы – Системный журнал UNIX**, как показано ниже.

Рис. 139 Меню 24.3.2 - Сопровождение системы: Системный журнал и учет ресурсов

```

Menu 24.3.2 - System Maintenance - UNIX Syslog

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

Types:
  CDR= No
  Packet Triggered= No
  Filter Log= No
  PPP Log= No

Press ENTER to Confirm or ESC to Cancel:

```

Необходимо настроить параметры системного журнала UNIX syslog, как описывается в следующей таблице, чтобы активизировать системный журнал, а затем выбрать, события для регистрации.

Табл. 63 Меню 24.3.2 - Сопровождение системы: Системный журнал и учет ресурсов

ПАРАМЕТР	ОПИСАНИЕ
UNIX Syslog (Системный журнал UNIX):	
Active (Включить)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для включения или отключения системного журнала.
Syslog IP Address (IP-адрес системного журнала)	Введите IP-адрес сервера системного журнала.
Log Facility (Функция журнала)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора одного из семи локальных режимов. Функция журнальной регистрации позволяет регистрировать сообщения в разных файлах на сервере. См. руководство по UNIX.
Types: (Типы:)	
CDR (Запись о деталях установления вызова)	Если установлено значение Yes (Да), в CDR регистрируется любая активность установления вызовов.
Packet triggered (Иницирующий пакет)	Если установлено значение Yes (Да), первые 48 байт, а также тип протокола пакета, инициировавшего вызов, посылаются на сервер системного журнала UNIX.
Filter Log (Журнал фильтров)	Если установлено значение No , фильтры не регистрируются. Если установлено значение Yes , регистрируются фильтры, у которых поле Log (Журнал) имеет значение Yes .

Табл. 63 Меню 24.3.2 - Сопровождение системы: Системный журнал и учет ресурсов

ПАРАМЕТР	ОПИСАНИЕ
PPP Log (Журнал PPP)	Если установлено значение Yes , регистрируются события PPP.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

На следующем рисунке представлены примеры для четырех типов сообщений системного журнала, отправленных модемом:

Рис. 140 Пример системного журнала

```

1 - CDR
SdcmdSyslogSend ( SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new
call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxxx (L2TP, xxxxxx = Remote Call ID)
C01 Incoming Call xxxxx (= connected speed) xxxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxxx (= connected speed) xxxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing
Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated
2 - Packet Triggered
SdcmdSyslogSend (SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxxxx...x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server

```

Рис. 140 Пример системного журнала (продолжение)

```

Jul 19 11:28:39 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 - Filter Log

SdcmSyslogSend (SYSLOG_FILLOG, SYSLOG_NOTICE, String);

String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match
(m), drop (D).

Src: Source Address
Dst: Destination Address

prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port

Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP
spo=0208 dpo=0208]} S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF

4 - PPP Log

SdcmSyslogSend (SYSLOG_PPLOG, SYSLOG_NOTICE, String);

String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown

Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP

Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing

```

24.5 Диагностика

Средства диагностики позволяют проводить тестирование различных функций модема, чтобы установить, нормально ли работает устройство. Меню 24.4 позволяет выбрать различные типы диагностических тестов для оценки работоспособности системы, как показано на следующем рисунке.

Для перехода в меню **Диагностика** выполните следующие действия.

- 1** В Главном меню введите 24 для перехода в **Меню 24 – Сопровождение системы**.
- 2** В Меню 24 введите 4 для отображения **Меню 24.4 - Сопровождение системы - Диагностика**, как показано далее.

Рис. 141 Меню 24.4 - Сопровождение 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

```

В следующей таблице приведено описание диагностических тестов устройства и соединений, доступ к которым осуществляется через Меню 24.4.

Табл. 64 Меню 24.4 - Сопровождение системы: Диагностика

ПОЛЕ	ОПИСАНИЕ
Reset xDSL (Сброс соединения xDSL)	Повторно инициализирует соединение xDSL с оборудованием телефонной компании.
Ping Host (Эхо- тестирование соединения с узлом)	Выполняет эхо-тестирование узла для определения работоспособности соединений и протокола TCP/IP в обеих системах.
Reboot System (Перезагрузка системы)	Перезагружает модем.
Command Mode (Режим интерпретатора команд)	Обеспечивает проведение диагностики и тестирования модема с помощью определенных команд.
Host IP Address (IP-адрес узла)	Если выбрана опция 12 для эхо-тестирования узла, введите адрес компьютера для тестирования.

ГЛАВА 25

Сопровождение файлов конфигурации и микропрограммы

В этой главе рассматриваются вопросы резервного копирования и восстановления текущего файла конфигурации, а также обновления файлов конфигурации и микропрограммы.

25.1 Структура имен файлов

Файл конфигурации (часто называемый "romfile" или "rom-0") содержит заводские настройки по умолчанию в некоторых меню, таких как, Пароль, Настройка DHCP, Настройка TCP/IP и т. д. Файл конфигурации при поставке имеет расширение "rom". После выполнения пользовательских настроек модема, файл конфигурации можно сохранить на компьютере в файле с любым именем.

Файл ZyNOS (ZyXEL Network Operating System - Сетевая операционная система ZyXEL), иногда называемый также файлом "gas", является системной микропрограммой и имеет расширение "bin". При использовании большинства клиентов FTP and TFTP, имена файлов имеют вид, показанный далее.



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

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

Это пример сеанса FTP для передачи файла "firmware.bin" с компьютера на модем.

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

Это пример сеанса FTP для сохранения на компьютере текущей конфигурации модема в файле "config.cfg".

Если ваш клиент (T)FTP не позволяет использовать разные имена для исходного и целевого файлов, то необходимо их переименовать, так как модем распознает только файлы "rom-0" и "gas". Сохраните исходные копии обоих файлов для дальнейшего использования.

В следующей таблице представлена краткая информация. Обратите внимание, что внутреннее имя файла относится к имени файла в модеме, а внешнее имя файла относится к имени файла вне модема, то есть на компьютере, в локальной сети или на ftp-сайте, таким образом, имена файлов (но не расширение) могут различаться. После загрузки новой микропрограммы убедитесь, что в поле **ZyNOS F/W Version (Версия микропрограммы ZyNOS)** в **Меню 24.2.1 - Сопровождение системы - Информация** отображается правильная версия микропрограммы. В ответ на приглашение перейти в режим отладки в меню SMT, нажмите "Y", а затем введите команду AT.

Табл. 65 Структура имен файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл конфигурации	rom-0	Это имя файла конфигурации модема. При загрузке файла rom-0 производится замена всей файловой системы ПЗУ, включая конфигурацию модема, параметры системы (включая пароль по умолчанию), журнала ошибок и журнала трассировки.	*.rom
Firmware (Микропрограмма)	gas	Это базовое имя микропрограммы ZyNOS для модема.	*.bin

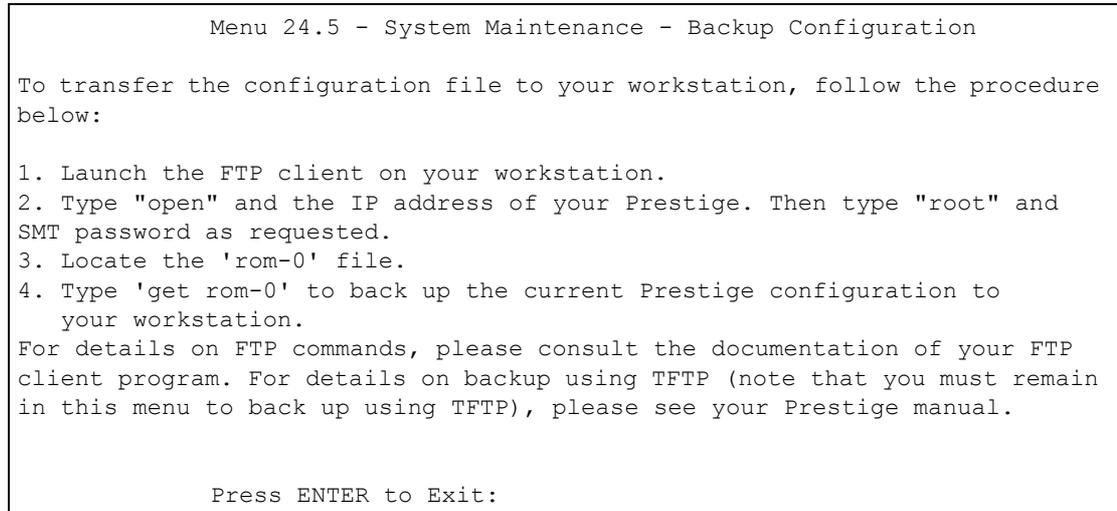
25.2 Резервное копирование конфигурации

Опция 5 в **Меню 24 - Сопровождение системы** позволяет сохранять текущую конфигурацию модема на компьютере. После того, как получена работающая конфигурация модема, настоятельно рекомендуется выполнить ее резервное копирование. Наиболее предпочтительным способом для копирования текущей конфигурации на компьютере является сеанс FTP вследствие его высокой скорости. Также может быть использована любая коммуникационная программа, однако для загрузки/выгрузки микропрограммы необходимо использовать протокол Xmodem, в этом случае переименовывать файлы не нужно.

Следует отметить, что термины "загрузка" и "выгрузка" относятся к компьютеру. "Загрузка" означает передачу файла с модема на компьютер, а "выгрузка" - с компьютера на модем.

25.2.1 Резервное копирование конфигурации

Выполните действия, как показано в следующем меню.

Рис. 142 Сеанс Telnet в Меню 24.5

25.2.2 Использование команд FTP в командной строке

- 1 Запустите клиент FTP на компьютере.
- 2 Введите "open", а затем через пробел - IP-адрес модема.
- 3 При появлении запроса на ввод имени пользователя нажмите клавишу [ENTER].
- 4 Введите пароль (по умолчанию "1234").
- 5 Введите "bin" для установки двоичного режима передачи.
- 6 Введите команду "get" для передачи файлов с модема на компьютер, например, команда "get rom-0 config.rom" передает файл конфигурации с модема на компьютер и переименовывает его в "config.rom". Более подробно о структуре имен файлов см. выше в этой главе.
- 7 Введите "quit" для выхода из режима FTP.

25.2.3 Пример использования команд FTP в командной строке

Рис. 143 Пример сеанса FTP

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

25.2.4 Клиенты FTP на основе GUI

В следующей таблице описываются некоторые команды, которые могут встретиться в программах клиента FTP на основе GUI (Graphical User Interface - Графический интерфейс пользователя).

Табл. 66 Основные команды для клиентов FTP на основе GUI

ПОЛЕ	ОПИСАНИЕ
Host Address (Адрес узла)	Введите адрес узла.
Login Type (Тип регистрации)	Анонимная. В этом случае серверу автоматически предоставляется идентификатор пользователя и пароль для анонимного доступа. Анонимная регистрация возможна только, если эта функция включена Интернет-провайдером или администратором услуг. Обычная. Для регистрации требуется ввести уникальный идентификатор пользователя и пароль.
Transfer Type (Тип передачи)	Передача файлов либо в формате ASCII (формат открытого текста), либо в режиме binary (двоичный).
Initial Remote Directory (Исходный удаленный каталог)	Укажите удаленный каталог по умолчанию (путь).
Initial Local Directory (Исходный локальный каталог)	Укажите локальный каталог по умолчанию (путь).

25.2.5 Ограничения на управление с помощью TFTP и FTP по глобальной сети

TFTP, FTP и Telnet через глобальную сеть не будут работать, если:

- Служба Telnet отключена в Меню 24.11.
- В Меню 3.1 (локальная сеть) или Меню 11.5 (глобальная сеть) применен фильтр для блокировки службы Telnet.

- IP-адрес в поле **Secured Client IP (IP-адрес доверенного клиента)** Меню 24.11 не совпадает с IP-адресом клиента. Если адреса не совпадают, модем немедленно разрывает сеанс Telnet.
- Уже выполняется сеанс управления с помощью SMT.

25.2.6 Резервное копирование конфигурации с помощью TFTP

Модем поддерживает загрузку/выгрузку микропрограммы и файла конфигурации с помощью протокола TFTP (Trivial File Transfer Protocol - Простейший протокол передачи данных) по локальной сети. Хотя TFTP также работает и по глобальной сети, этого делать не рекомендуется.

Для использования TFTP на компьютере должны быть установлены клиенты Telnet и TFTP. Для копирования файла конфигурации выполните следующие действия:

- 1** Подключитесь к модему с помощью Telnet и войдите в систему. Так как в TFTP не предусмотрена проверка на безопасность, модем регистрирует IP-адрес клиента Telnet и принимает запросы TFTP только с этого адреса.
- 2** Переведите SMT в режим интерпретатор команда посредством ввода 8 в **Меню 24 – Сопровождение системы**.
- 3** Введите команду "sys stdio 0" для отключения времени неактивности SMT, чтобы сеанс TFTP не прерывался. После завершения передачи файла введите команду "sys stdio 5", чтобы заново установить время неактивности SMT 5 минут (по умолчанию).
- 4** Запустите на компьютере клиент TFTP и подключитесь к модему. Перед началом передачи данных установите двоичный (binary) режим передачи.
- 5** Используйте клиент TFTP для передачи файлов между модемом и компьютером (см. пример далее). Для файла конфигурации используется имя "rom-0" (rom-ноль, а не заглавная буква O).

Следует помнить, что перед началом и в процессе передачи данных по TFTP, должно быть установлено соединение Telnet, а SMT должен находиться в режиме интерпретатора команд. Для получения подробной информации о командах TFTP (см. следующий пример) следует обратиться к документации по используемой программе клиента TFTP. В операционной системе UNIX используется команда "get" для передачи файлов с модема на компьютер и команда "binary" - для установки двоичного режима передачи.

25.2.7 Пример команды TFTP

Далее приводится пример команды TFTP:

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

где "i" обозначает двоичный режим передачи (этот режим используется при передаче файлов в двоичном коде), "host" - IP-адрес модема, "get" выполняет передачу файла источника, находящегося в модеме, (rom-0 - имя файла конфигурации модема) на компьютер и переименовывает его в config.rom.

25.2.8 Клиенты TFTP на основе GUI

В следующей таблице описываются некоторые команды, которые могут встретиться в программах клиента TFTP на основе GUI.

Табл. 67 Основные команды клиентов TFTP на основе GUI

КОМАНДА	ОПИСАНИЕ
Host (Узел)	Введите IP-адрес модема. IP-адрес модема по умолчанию при поставке - 192.168.1.1.
Send/Fetch (Отправить/Получить)	"Send" используется для загрузки файла в модем, а "Fetch" - для резервного копирования файла на компьютер.
Local File (Локальный файл)	Введите путь и имя файла микропрограммы (*.bin) или файла конфигурации (*.rom) на компьютере.
Remote File (Файл на удаленном узле)	Имя файла в модеме. Для файла микропрограммы используется имя "ras", а для файла конфигурации - "rom-0".
Binary (Двоичный)	Используется для передачи файла в двоичном режиме.
Abort (Отказ)	Прекращение передачи файла.

См. в разделе [Ограничения на управление с помощью TFTP и FTP по глобальной сети](#) информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети.

25.3 Восстановление конфигурации

В данном разделе описывается восстановление предварительно сохраненной конфигурации. Следует помнить, что при восстановлении конфигурации стирается текущая конфигурация; поэтому перед началом восстановления предыдущей конфигурации следует сохранить текущий файл конфигурации на компьютере.

Более предпочтительным способом восстановления конфигурации с компьютера на модем является сеанс FTP вследствие его высокой скорости. После завершения передачи файла следует подождать, пока система автоматически перезапустится.



ПРИМЕЧАНИЕ: Не прерывайте процесс передачи файла, так как это может привести к НЕУСТРАНИМОМУ ПОВРЕЖДЕНИЮ МОДЕМА.

25.3.1 Восстановление конфигурации с помощью FTP

Более подробно о резервном копировании с помощью (T)FTP см. в предыдущих разделах этой главы, где описывается загрузка файлов с помощью FTP и TFTP.

Рис. 144 Установка соединения Telnet в Меню 24.6

```

Menu 24.6 -- System Maintenance - Restore Configuration
To transfer the firmware and configuration file to your workstation, follow
the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and
SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
your backup configuration file on your workstation and rom-0 is the
remote file name on the Prestige. This restores the configuration to
your Prestige.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.

Press ENTER to Exit:

```

- 1** Запустите на компьютере клиент FTP.
- 2** Введите "open", а затем через пробел IP-адрес модема.
- 3** При появлении запроса на ввод имени пользователя нажмите клавишу [ENTER].
- 4** Введите пароль (по умолчанию "1234").
- 5** Введите "bin" для установки двоичного режима передачи.
- 6** Найдите файл "rom" (на компьютере), который вы хотите восстановить в модем.
- 7** Введите команду "put" для передачи файлов с компьютера в модем, например, "put config.rom rom-0" передает файл конфигурации "config.rom" с компьютера в модем. Более подробно о структуре имен файлов см. выше в этой главе.
- 8** Введите "quit" для выхода из режима FTP. После успешного завершения процесса восстановления конфигурации модем автоматически перезапускается.

25.3.2 Пример восстановления конфигурации с помощью сеанса FTP

Рис. 145 Пример восстановления конфигурации с помощью сеанса FTP

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp> quit
```

См. в разделе [Ограничения на управление с помощью TFTP и FTP по глобальной сети](#) информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети.

25.4 Загрузка файлов конфигурации и микропрограммы

В этом разделе рассматривается загрузка файлов конфигурации и микропрограммы. Для загрузки файла конфигурации можно использовать процедуру, описываемую в разделе [Резервное копирование конфигурации](#), или выполнить следующие действия в Меню 24.7.2 – Сопровождение системы – Загрузка файла конфигурации системы.

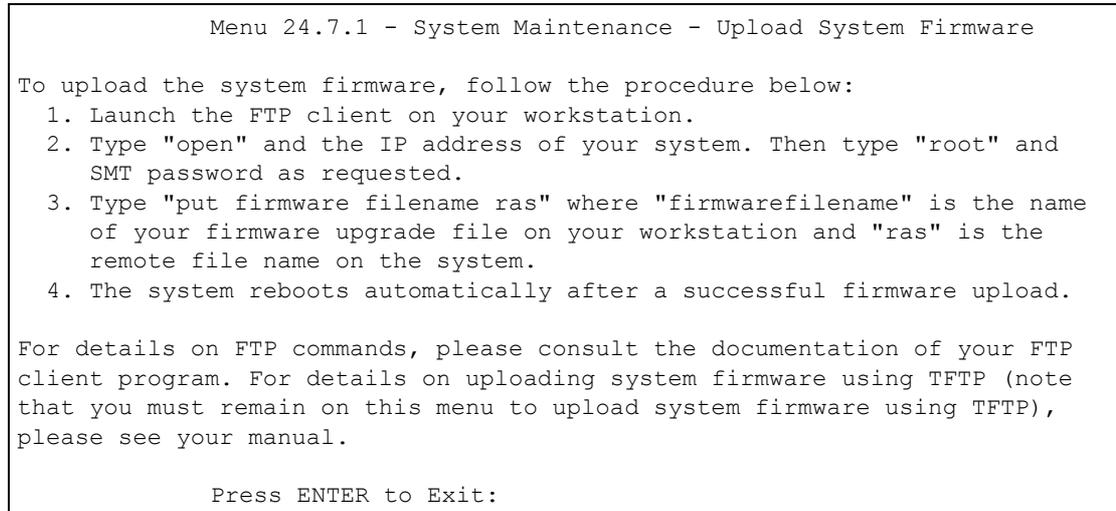


ПРИМЕЧАНИЕ: Не прерывайте процесс передачи файла, так как это может привести к неустранимому повреждению устройства.

25.4.1 Загрузка микропрограммы

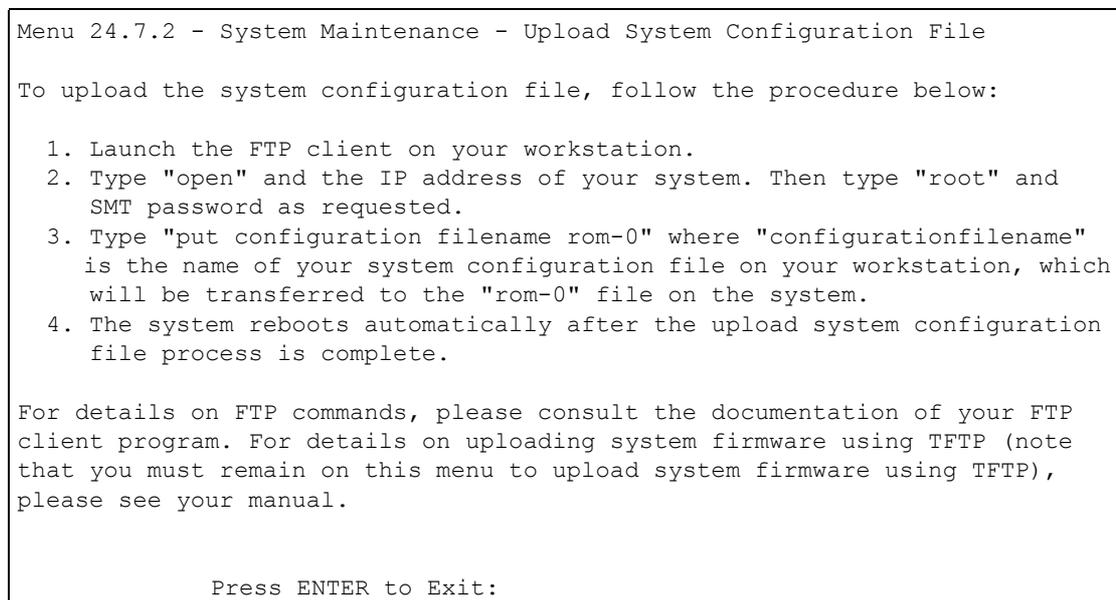
FTP является наиболее предпочтительным методом для загрузки файлов конфигурации и микропрограммы. Чтобы использовать эту функцию, на компьютере должен быть установлен клиент FTP.

При подключении к модему через Telnet используются следующие меню для загрузки файла конфигурации и микропрограммы при помощи сеанса FTP.

Рис. 146 Подключение Telnet в Меню 24.7.1 - Загрузка системной микропрограммы

25.4.2 Загрузка файла конфигурации

При подключении через Telnet с помощью Меню 24.7.2 появляется следующий экран.

Рис. 147 Подключение с помощью Telnet в Меню 24.7.2 - Сопровождение системы

Для загрузки файлов конфигурации и микропрограммы выполните действия, показанные в приведенных ниже примерах.

25.4.3 Пример загрузки файлов с помощью сеанса FTP из командной строки DOS

- 1 Запустите на компьютере клиент FTP.
- 2 Введите "open", а затем через пробел IP-адрес модема.
- 3 При появлении запроса на ввод имени пользователя нажмите клавишу [ENTER].
- 4 Введите пароль (по умолчанию "1234").
- 5 Введите "bin" для установки двоичного режима передачи.
- 6 Введите команду "put" для передачи файлов с компьютера на модем, например, "put firmware.bin ras" передает файл микропрограммы (firmware.bin) с компьютера на модем и переименовывает его в "ras". Аналогично команда "put config.rom rom-0" передает файл конфигурации (config.rom) с компьютера на модем и переименовывает его в "rom-0". Подобным образом, команда "get rom-0 config.rom" передает файл конфигурации с модема на компьютер и переименовывает его в "config.rom". Более подробно о структуре имен файлов см. выше в этой главе.
- 7 Введите "quit" для выхода из режима FTP.



ПРИМЕЧАНИЕ: После успешной загрузки файла, модем автоматически перезапускается.

25.4.4 Пример загрузки микропрограммы с помощью сеанса FTP

Рис. 148 Пример загрузки микропрограммы с помощью сеанса FTP

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

Другие команды (для клиентов FTP на основе GUI) перечислены в этой главе ранее.

См. в разделе [Ограничения на управление с помощью TFTP и FTP по глобальной сети](#) информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети.

25.4.5 Загрузка файлов с помощью TFTP

Модем поддерживает загрузку файлов микропрограммы с помощью протокола TFTP (Trivial File Transfer Protocol - Простейший протокол передачи данных) по локальной сети. Хотя TFTP также работает и по глобальной сети, этого делать не рекомендуется.

Для использования TFTP на компьютере должны быть установлены клиенты Telnet и TFTP. Для передачи микропрограммы и файла конфигурации выполните следующие действия.

- 1 Подключитесь к модему с помощью Telnet и войдите в систему. Так как в TFTP не предусмотрена проверка на безопасность, модем регистрирует IP-адрес клиента Telnet и принимает запросы TFTP только с этого адреса.
- 2 Переведите SMT в режим интерпретатора команд посредством ввода 8 в **Меню 24 – Сопровождение системы**.
- 3 Введите команду "sys stdio 0" для отключения времени неактивности SMT, чтобы сеанс TFTP не прерывался. После завершения передачи файла введите команду "sys stdio 5", чтобы заново установить время неактивности SMT 5 минут (по умолчанию).
- 4 Запустите на компьютере клиент TFTP и подключитесь к модему. Перед началом передачи данных установите двоичный режим передачи.
- 5 Используйте клиент TFTP для передачи файлов между модемом и компьютером (см. пример далее). Имя файла микропрограммы - "ras".

Следует помнить, что перед началом и в процессе передачи данных по TFTP, должно быть установлено соединение Telnet, а SMT должен находиться в режиме интерпретатора команд. Для получения подробной информации о командах TFTP (см. следующий пример) следует обратиться к документации по используемой программе клиента TFTP. В операционной системе UNIX используется команда "get" для передачи файлов с модема на компьютер, "put" - для передачи в обратном направлении и "binary" - для установки двоичного режима передачи.

25.4.6 Пример команды для загрузки файла с помощью сеанса TFTP

Далее приводится пример команды TFTP:

```
tftp [-i] host put firmware.bin ras
```

где "i" обозначает двоичный режим передачи (этот режим используется при передаче двоичных файлов), "host" - IP-адрес модема, "put" выполняет передачу файла с компьютера (firmware.bin - имя файла микропрограммы на компьютере) в целевой файл на удаленном узле (ras - имя файла микропрограммы в модеме).

Команды для клиентов TFTP на основе GUI перечислены ранее в этой главе.

ГЛАВА 26

Сопровождение системы

В данной главе описываются меню SMT с 24.8 до 24.10.

26.1 Режим интерпретатора команд

Интерпретатор команд CI (Command Interpreter) является частью основного встроенного системного программного обеспечения. CI обеспечивает большинство функций SMT, а также некоторые возможности настройки и диагностики более низкого уровня. Для входа в режим CI используется Меню SMT 24.8. Более подробную информацию о командах CI можно найти на компакт-диске, входящем в комплект поставки или на Web-сайте www.zyxel.ru. Введите 8 в **Меню 24 - Сопровождение системы**. Список доступных команд отображается с помощью введения в командной строке команды `help` или `?`. Для возвращения в Главное меню SMT после завершения работы используется команда `"exit"`.

Рис. 149 Командный режим в Меню 24

```
Menu 24 - System Maintenance

1. System Status
2. System Information & Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management

Enter Menu Selection Number:
```

Рис. 150 Доступные команды

```

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit             device         ether
wan            poe             ip             ppp
bridge         hdap           lan
ras>

```

26.2 Контроль вызовов

Функция контроля вызовов является доступной, только если в поле **Encapsulation (Инкапсуляция)** Меню 4 или Меню 11.1 установлено значение **PPPoE**.

Функция управления бюджетом позволяет установить ограничение на общую продолжительность исходящих соединений модема за определенный период времени. Если общая продолжительность исходящих вызовов превысит установленный предел, текущий вызов будет сброшен, а все последующие исходящие вызовы заблокированы.

Для доступа к меню контроля вызовов в Меню 24 введите "9" для перехода в **Меню 24.9 - Сопровождение системы - Контроль вызовов**, как показано в следующей таблице.

Рис. 151 Меню 24.9 - Сопровождение системы: Контроль вызовов

```

Menu 24.9 - System Maintenance - Call Control

1. Budget Management

Enter Menu Selection Number:

```

26.2.1 Управление бюджетом

В Меню 24.9.1 отображается статистика управления бюджетом для исходящих вызовов. Введите 1 в **Меню 24.9 — Сопровождение системы — Контроль вызовов** для перехода в следующее меню.

Рис. 152 Меню 24.9.1 - Сопровождение системы: Управление бюджетом

Menu 24.9.1 - System Maintenance - Budget Management		
Remote Node	Connection Time/Total Budget	Elapsed Time/Total Period
1.MyIsp	No Budget	No Budget
2.-----	---	---
3.-----	---	---
4.-----	---	---
5.-----	---	---
6.-----	---	---
7.-----	---	---
8.-----	---	---
Reset Node (0 to update screen):		

Общий бюджет представляет собой ограничение на суммарное время исходящих вызовов на удаленный узел. Достижение данного лимита времени приводит к сбрасыванию текущего вызова, а последующие исходящие вызовы на этот удаленный узел блокируются. По истечении каждого периода действия общий бюджет сбрасывается. По умолчанию для общего бюджета установлено 0 минут, а для периода - 0 часов, т.е. функция управления бюджетом отключена. Пользователь может сбросить суммарное время соединения, посредством ввода номера удаленного узла. Введите 0 для обновления экрана. Бюджет и период сброса бюджета для удаленного узла устанавливаются в Меню 11.1, если выбрана инкапсуляция PPPoE.

Табл. 68 Меню 24.9.1 - Сопровождение системы: Управление бюджетом

ПОЛЕ	ОПИСАНИЕ
Remote Node (Удаленный узел)	Введите порядковый номер удаленного узла, для которого требуется сбросить время соединения (только один в данном случае).
Connection Time/Total Budget (Время соединения/Общий бюджет)	Общее время соединения, прошедшее в рамках выделенного бюджета, установленного в Меню 11.1.
Elapsed Time/Total Period (Истекшее время/Общий период)	Период - это цикл времени в часах, через который сбрасывается выделенный бюджет (см. меню 11.1.). Истекшее время - это общее время соединения за этот период.
Введите "0" для обновления экрана или нажмите клавишу [ESC] для возврата к предыдущему экрану.	

26.3 Установка времени и даты

Модем ведет счет времени и даты. Устройство оснащено программным механизмом для установки времени вручную, а также для получения текущего времени и даты от внешнего сервера при включении модема. Меню 24.10 позволяет обновить параметры времени и даты модема. При этом реальное время отображается в журналах регистрации ошибок модема.

В Главном меню выберите Меню 24 для перехода в **Меню 24 - Сопровождение системы**, как показано ниже.

Рис. 153 Меню 24 - Сопровождение системы

```
Menu 24 - System Maintenance

1. System Status
2. System Information & Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management

Enter Menu Selection Number:
```

Введите 10 для перехода в **Меню 24.10 - Сопровождение системы - Установка времени и даты** для обновления параметров времени и даты модема, как показано на следующем рисунке.

Рис. 154 Меню 24.10 - Сопровождение системы: Установка времени и даты

```

Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= None
Time Server Address= N/A

Current Time:                03: 10 : 50
New Time (hh:mm:ss):        03: 10 : 43

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2000 - 01 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):          01 - 00
End Date (mm-dd):           01 - 00

Press ENTER to Confirm or ESC to Cancel:

```

Табл. 69 Меню 24.10 - Сопровождение системы: Установка времени и даты

ПОЛЕ	ОПИСАНИЕ
Use Time Server when Bootup (Использовать сервер времени при загрузке)	Введите протокол сервиса времени по которому ваш сервер времени передает информацию при включении модема. Не все серверы времени поддерживают все протоколы, поэтому следует проконсультироваться с Интернет-провайдером/сетевым администратором, или попытаться определить работающий протокол методом проб и ошибок. Основные отличия между протоколами заключаются в формате представления времени. Формат Daytime (RFC 867) содержит день/месяц/год/часовой пояс сервера. Формат Time (RFC-868) представляет собой 4-байтовое целое число, которое определяет общее количество секунд, прошедших с даты 1.01.1970 на 0:0:0 часов. Формат NTP (RFC-1305) аналогичен формату Time (RFC-868) . None (Нет) . Это значение установлено по умолчанию, введите время вручную.
Time Server Address (Адрес сервера времени)	Введите IP-адрес или доменное имя сервера времени. Если вы не обладаете этой информацией, следует обратиться к Интернет-провайдеру/сетевому администратору.
Current Time (Текущее время) New Time (Новое время)	В данном поле после повторного входа в это меню отображается обновленное время. Введите новое время в формате часы, минуты и секунды.
Current Date (Текущая дата) New Date (Новая дата)	В данном поле после повторного входа в это меню отображается обновленная дата. Введите новую дату в формате год, месяц и день.
Time Zone (Часовой пояс)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для установки разницы во времени между вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time - GMT).

Табл. 69 Меню 24.10 - Сопровождение системы: Установка времени и даты

ПОЛЕ	ОПИСАНИЕ
Daylight Saving (Переход на летнее время)	Если используется переход на летнее время, выберите Yes (Да).
Start Date (Дата начала)	Если используется переход на летнее время, введите месяц и день начала летнего времени.
End Date (Дата окончания)	Если используется переход на летнее время, введите месяц и день окончания летнего времени.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

26.3.1 Обновление времени

Модем обновляет время в следующих трех случаях:

- При выходе из Меню 24.10 после внесения изменений.
- При загрузке модема, если в Меню 24.10 настроен сервер времени.
- Каждые 24 часа после запуска.

ГЛАВА 27

Удаленное управление

В этой главе описывается удаленное управление модемом (Меню SMT 24.11).

27.1 Описание удаленного управления

Функция удаленного управления позволяет определить компьютеры и службы/протоколы, которым разрешен доступ к интерфейсу управления модемом.

27.2 Удаленное управление

Чтобы отключить использование конкретной службы для удаленного управления, выберите **Disable (Отключить)** в соответствующем поле **Server Access (Доступ к серверу)**.

Введите 11 в Меню 24 для перехода в **Меню 24.11 — Контроль удаленного управления**.

27.2.1 Настройка удаленного управления

Вы можете удаленно управлять модемом через:

глобальную сеть (**WAN only**), локальную сеть (**LAN only**), локальную и глобальную сеть (**ALL**) или удаленное управление может быть запрещено (**Disable**).

- через Интернет (только через глобальную сеть)
- отовсюду (через локальную и глобальную сеть)
- только через локальную сеть
- никак (функция отключена).



ПРИМЕЧАНИЕ: Если функция удаленного управления для конкретной службы включена, но при этом применен фильтр блокировки этой службы, то выполнять удаленное управление модемом с помощью этой службы будет нельзя.

Введите 11 в Меню 24 для перехода в **Меню 24.11 — Контроль удаленного управления** (показано далее).

Рис. 155 Меню 24.11 - Контроль удаленного управления

```

Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                Server Access = LAN only
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                Server Access = LAN only
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                Server Access = LAN only
  Secured Client IP = 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описываются поля данного меню.

Табл. 70 Меню 24.11 - Контроль удаленного управления

ПОЛЕ	ОПИСАНИЕ
Telnet Server (Telnet-сервер) FTP Server (FTP-сервер) Web Server (Web-сервер)	Каждое из этих полей только для чтения обозначает службу или протокол.
Port (Порт)	В данном поле отображается номер порта для службы или протокола. Если требуется, вы можете здесь изменить номер порта, но для доступа к модему будет необходимо использовать этот же номер порта.
Access (Доступ)	При необходимости выберите, откуда разрешено управления, нажав клавишу [ПРОБЕЛ]. Вариантами являются: LAN only (Только через локальную сеть) , WAN only (Только через глобальную сеть) , All (Через локальную и глобальную сеть) или Disable (Отключить) . По умолчанию установлено LAN only (только через локальную сеть).
Secured Client IP (IP-адрес доверенного клиента)	По умолчанию используется адрес 0.0.0.0, что позволяет любому клиенту использовать данную службу или протокол для удаленного управления модемом. Введите IP-адрес, чтобы предоставить доступ только клиентам с совпадающим IP-адресом.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

27.2.2 Ограничения на удаленное управление

Удаленное управление не будет работать по локальной или глобальной сети, если:

- Применен фильтр для блокировки службы Telnet, FTP или Web в Меню 3.1 (локальная сеть) или Меню 11.5 (глобальная сеть) .
- Эта служба отключена в Меню 24.11.

- IP-адрес, установленный в поле **Secured Client IP (IP-адрес доверенного клиента)** Меню 24.11 не совпадает с IP-адресом клиента. В случае несовпадения адресов модем немедленно разрывает сеанс управления.
- Уже выполняется другой сеанс удаленного управления, имеющий равный или более высокий приоритет. Одновременно допускается проведение только одного сеанса удаленного управления.

27.3 Удаленное управление и NAT

При включении функции NAT:

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

27.4 Время бездействия системы

Интервал бездействия системы во время сеанса управления по умолчанию установлен 5 минут (300 секунд). Модем автоматически завершает сеанс управления при бездействии более этого периода. Сеанс управления не разрывается, если выполняется непрерывное обновление состояния системы в Меню 24.1, или если время бездействия было изменено с помощью команды `sys studio` в командной строке.

ГЛАВА 28

Маршрутизация на базе стратегии IP

В этой главе рассматривается настройка и применение стратегий, используемых для маршрутизации IP.

28.1 Описание маршрутизации на базе стратегии IP (IP Policy Routing)

Как правило, маршрутизация производится только на основе адреса получателя, поэтому маршрутизатор выбирает самый короткий путь для пересылки пакета. Маршрутизация на базе стратегии IP (IPPR) обеспечивает механизм замены схемы маршрутизации по умолчанию, и позволяет изменить правила для пересылки пакета на основе стратегии, определяемой сетевым администратором. Маршрутизация на основе стратегии, применяемая к входящим пакетам каждого интерфейса, имеет приоритет перед стандартной маршрутизацией.

28.2 Преимущества маршрутизации на базе стратегии IP

Маршрутизация на базе источника (Source-Based Routing) - Сетевые администраторы могут использовать такую стратегию для направления трафика от разных пользователей по различным соединениям.

Качество обслуживания предоставляемых услуг передачи данных (QoS) – Организации могут дифференцировать трафик с помощью установки приоритета и значения TOS (Type of Service - Тип услуги) в IP-заголовке на периферии сети для включения функции распределения трафика в магистральной сети в соответствии с приоритетом.

Сокращение расходов (Cost Savings) - IPPR позволяет организациям использовать дорогостоящие каналы с высокой пропускной способностью для интерактивного трафика, а дешевые каналы - для пакетного трафика.

Распределение нагрузки (Load Sharing) - Сетевые администраторы могут использовать IPPR для распределения трафика по нескольким каналам.

28.3 Стратегия маршрутизации

Конкретные стратегии маршрутизации используются как часть общего процесса IPPR. Стратегия определяет критерии соответствия и действие, которое должно быть выполнено, если пакет отвечает этим критериям. Действие выполняется только в случае, если достигнуто соответствие всем критериям. Критериями служат адрес и порт источника, протокол IP (ICMP, UDP, TCP и т.д.), адрес и порт получателя, TOS и приоритет (поля в IP-заголовке), а также длина пакета. Критерий длины используется для разделения интерактивного трафика и трафика массивов данных. Интерактивные приложения, например, Telnet, обычно используют короткие пакеты, тогда как трафик массивов данных, например, передача файлов, - длинные.

Действия, выполняемые при соответствии критериям:

- маршрутизация пакета на другой шлюз (и, следовательно, выходной интерфейс)
- установка полей TOS и приоритета в IP-заголовке.

По характеру и реализации IPPR аналогична существующей функции фильтрации пакетов RAS (Remote access service - Служба удаленного доступа). Стратегии группируются в наборы, каждый из которых состоит из родственных стратегий. Прежде чем применять стратегии к интерфейсу или удаленному узлу, их необходимо создать, аналогично созданию фильтров. Существует возможность создания 12 наборов стратегий по шесть стратегий в каждом.

28.4 Настройка стратегий маршрутизации IP

В Меню 25 отображаются все установленные стратегии.

Рис. 156 Меню 25 - Настройка стратегий маршрутизации IP

```

Menu 25 - IP Routing Policy Setup

Policy                               Policy
Set #                               Set #                               Name
-----                               -----                               -----
1      test
2      _____
3      _____
4      _____
5      _____
6      _____
7      _____
8      _____
9      _____
10     _____
11     _____
12     _____

Enter Policy Set Number to Configure= 0

Edit Name= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Для создания стратегии маршрутизации выполните следующие действия:

1 В Главном меню ведите 25 для перехода в **Меню 25 – Настройка стратегий маршрутизации IP.**

2 Введите номер набора стратегий, который необходимо настроить, для перехода в **Меню 25.1 – Настройка стратегии маршрутизации IP.**

Меню 25.1 содержит сводную информацию о наборе стратегий, включая критерии и действие для каждой конкретной стратегии, а также ее состояние: включена или нет. Каждая стратегия состоит из двух строк. В первой части определяются критерии для входящего пакета, а во второй - применяемое действие. Разделитель "|", стоящий между двумя частями, означает, что действие применяется при соответствии пакета критериям, а разделитель "=" - при несоответствии.

Рис. 157 Меню 25.1 - Настройка стратегий маршрутизации IP

```

Menu 25.1 - IP Routing Policy Setup

# A                      Criteria/Action
- - -----
1 Y SA=1.1.1.1-1.1.1.1 DA=2.2.2.2-2.2.2.5
   SP=20-20 DP=20-20 P=6 T=NM PR=0           |GW=192.168.1.1 T=MT PR=0
2 N _____
3 N _____
4 N _____
5 N _____
6 N _____

Enter Policy Rule Number (1-6) to Configure:

```

Табл. 71 Меню 25.1 - Настройка стратегии маршрутизации IP

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
Критерий SA	IP-адрес источника
SP	Порт источника
DA	IP-адрес получателя
DP	Порт получателя
P	Номер протокола IP уровня 4 (TCP=6, UDP=17...)
T	Тип услуги для входящего пакета
Pr	Приоритет входящего пакета
Действие GW	IP-адрес шлюза
T	Тип услуги для исходящего пакета
P	Приоритет исходящего пакета

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
Услуга NM	Стандартный режим
MD	Минимальная задержка
MT	Максимальная пропускная способность
MR	Максимальная надежность
MC	Минимальная стоимость

Введите число от 1 до 6 для перехода в **Меню 25.1.1 – Стратегия маршрутизации IP** (см. следующий рисунок). Это меню позволяет настраивать правила стратегии.

Рис. 158 Меню 25.1.1 - Стратегия маршрутизации IP

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= test
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Normal      Packet length= 40
  Precedence      = 0          Len Comp= Not Equal
Source:
  addr start= 1.1.1.1          end= 1.1.1.1
  port start= 20              end= 20
Destination:
  addr start= 2.2.2.2          end= 2.2.2.2
  port start= 20              end= 20
Action= Matched
Gateway addr      = 192.168.1.1  Log= No
Type of Service= Max Thruput
Precedence      = 0

Press ENTER to Confirm or ESC to Cancel:

```

В следующей таблице описываются поля данного меню.

Табл. 72 Меню 25.1.1 - Стратегия маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
Policy Set Name (Имя набора стратегий)	Имя набора стратегий, присвоенное в Меню 25 – Настройка стратегий маршрутизации IP .
Active (Включить)	Нажмите клавишу [ПРОБЕЛ] и затем клавишу [ENTER] для выбора Yes , чтобы включить данную стратегию, или No , чтобы отключить. Неактивные стратегии отображаются в Меню 25 SMT со знаком минуса ("-").
Criteria (Критерии)	
IP Protocol (Протокол IP)	Протокол IP уровня 4, например, UDP, TCP, ICMP и т. д.

Табл. 72 Меню 25.1.1 - Стратегия маршрутизации IP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Type of service (Тип услуги)	Определите тип услуги для входящего сетевого трафика. Вариантами являются: Don't Care (Не определен) , Normal (Стандартное) , Min Delay (Минимальная задержка) , Max Thruput (Максимальная пропускная способность) , Min Cost (Минимальная стоимость) или Max Reliable (Максимальная надежность) .
Precedence (Приоритет)	Значение приоритета входящего пакета. Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора значения от 0 до 7 или Don't Care (Не определен) .
Packet Length (Размер пакета)	Введите размер входящих пакетов (в байтах). Операторы в поле Len Comp (Сравнение размера) (следующее поле) применяются к пакетам для сравнения по этому размеру.
Len Comp (Сравнение размера)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора оператора сравнения. Вариантами являются: Equal (Равно) , Not Equal (Не равно) , Less (Меньше) , Greater (Больше) , Less or Equal (Меньше или равно) или Greater or Equal (Больше или равно) .
Source (Источник):	
addr start / end (начальный/конечный адрес)	Диапазон IP-адресов источника от начального до конечного.
port start / end (начальный/конечный порт)	Диапазон номеров портов источника от начального до конечного; применяется только для TCP/UDP.
Destination: (Получатель:)	
addr start / end (начальный/конечный адрес)	Диапазон IP-адресов получателя от начального до конечного.
port start / end (начальный/конечный порт)	Диапазон номеров портов получателя от начального до конечного; применяется только для TCP/UDP.
Action (Действие)	Определяет, условие выполнения действия: при соответствии пакета критериям (Matched) или несоответствии (Not Matched).
Gateway addr (Адрес шлюза)	Определяет адрес исходящего шлюза. Если шлюз находится в локальной сети, он должен принадлежать к той же подсети, что и модем, в противном случае шлюзу должен быть назначен IP-адрес удаленного узла. Для шлюза по умолчанию установлено значение 0.0.0.0.
Type of service (Тип услуги)	Установите новое значение типа услуги для исходящего пакета. Вариантами являются: No Change (Не изменять) , Normal (Стандартный) , Min Delay (С минимальной задержкой) , Max Thruput (Максимальная пропускная способность) или Max Reliable (Максимальная надежность) или Min Cost (Минимальная стоимость) .
Precedence (Приоритет)	Установите новое значение приоритета для исходящего пакета. Значение приоритета может быть от 0 до 7 или No Change (Без изменения) .
Log (Регистрационный журнал)	Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора Yes , чтобы после создания стратегии в системном журнале была сделана запись.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

28.5 Применение стратегии IP

В этом разделе описывается применение стратегий IP после их создания.

28.5.1 Стратегии IP для Ethernet

В Меню 3 – Настройка Ethernet введите 2 для перехода в Меню 3.2 – Настройка TCP/IP и DHCP для Ethernet.

Можно применить до четырех наборов стратегий IP (из 12), посредством ввода их номеров через запятую, например, 2, 4, 7, 9.

Рис. 159 Меню 3.2 - Настройка TCP/IP и DHCP для Ethernet

```
Menu 3.2 - TCP/IP and DHCP Setup

      DHCP Setup
      DHCP= Server
      Client IP Pool Starting Address= 192.168.1.33
      Size of Client IP Pool= 32
      Primary DNS Server= 0.0.0.0
      Secondary DNS Server= 0.0.0.0
      Remote DHCP Server= N/A
      TCP/IP Setup:
      IP-address= 192.168.1.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= Both
      Version= RIP-1
      Multicast= None
      IP Policies= 2,4,7,9
      Edit IP Alias= No

      Press ENTER to Confirm or ESC to Cancel:
```

Перейдите в Меню 11.3 (показано ниже) и введите номер(а) набора(ов) стратегий маршрутизации IP по мере необходимости. Можно последовательно применить до четырех наборов стратегий посредством ввода их номеров через запятую.

Рис. 160 Меню 11.3 - Параметры сетевого уровня удаленного узла

```
Menu 11.3 - Remote Node Network Layer Options

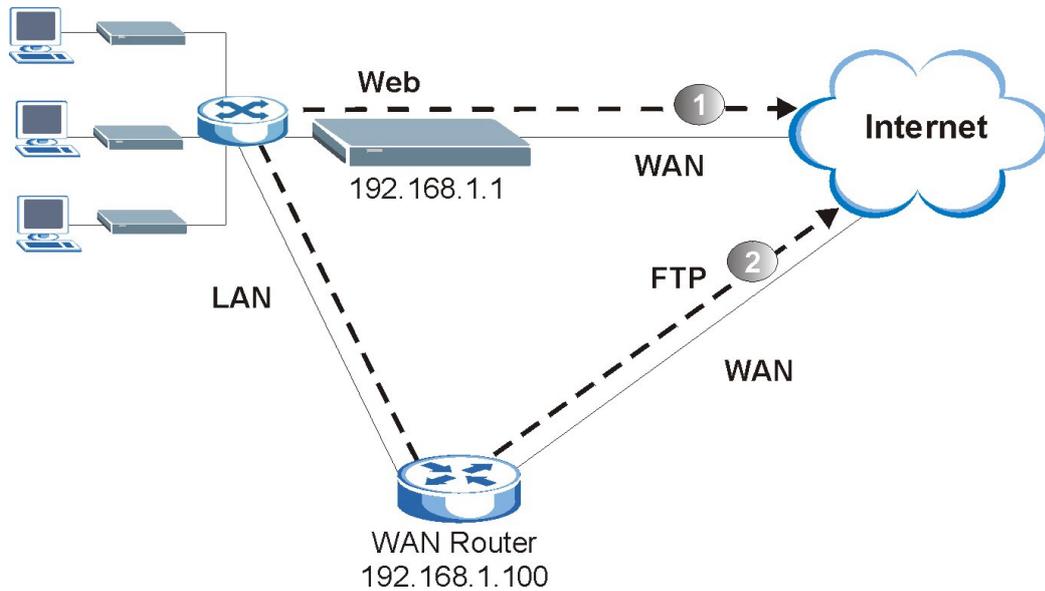
IP Options:                               Bridge Options:
IP Address Assignment= Static             Ethernet Addr Timeout (min)= 0
Rem IP Addr: 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
NAT= Full Feature
      Address Mapping Set= 2
Metric= 2
Private= No
RIP Direction= Both
      Version= RIP-2B
Multicast= IGMP-v2
IP Policies= 2,4,7,9

Press ENTER to Confirm or ESC to Cancel:
```

28.6 Пример маршрутизации на базе стратегии IP

Если сеть одновременно имеет два соединения: с Интернетом и с удаленным узлом, Web-пакеты можно пересылать в Интернет с использованием одной стратегии, а FTP-пакеты в удаленную сеть - с использованием другой стратегии. См. следующий рисунок.

Маршрут 1 является маршрутом IP по умолчанию, а маршрут 2 представляет собой созданный маршрут IP.

Рис. 161 Пример маршрутизации на базе стратегии IP

Для принудительного направления пакетов от клиентов с IP-адресами от 192.168.1.33 до 192.168.1.64 в Интернет через порт WAN модема, выполните следующие действия.

- 1 Создайте набор стратегий маршрутизации в Меню 25.
- 2 Создайте правило в этом наборе в **Меню 25.1.1 - Стратегия маршрутизации IP**, как показано ниже.

Рис. 162 Маршрутизация на базе стратегии IP. Пример 1

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= set1
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service  = Don't Care      Packet length= 10
  Precedence       = Don't Care      Len Comp= N/A
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= No Change
Precedence       = No Change

Press ENTER to Confirm or ESC to Cancel:

```

- 3 Проверьте в **Меню 25.1 - Настройка стратегии маршрутизации IP** правильно ли создано новое правило.
- 4 Создайте еще один набор стратегий маршрутизации в Меню 25.
- 5 Создайте в Меню 25.1 правило в этом наборе, предназначенное для маршрутизации пакетов от любого узла (IP=0.0.0.0 обозначает любой узел) с помощью протокола TCP и для доступа к порту FTP через другой шлюз (192.168.1.100).

Рис. 163 Маршрутизация на базе стратегии IP. Пример 2

```
Menu 25.1.1 - IP Routing Policy

Policy Set Name= set2
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service  = Don't Care      Packet length= 10
  Precedence       = Don't Care      Len Comp= N/A
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      = 192.168.1.100      Log= No
Type of Service= No Change
Precedence      = No Change

Press ENTER to Confirm or ESC to Cancel:
```

- 6 Проверьте в **Меню 25.1 - Настройка стратегии маршрутизации IP** правильно ли создано новое правило.
- 7 Примените оба набора стратегий в Меню 3.2, как показано ниже.

Рис. 164 Пример применения стратегий IP

```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 64
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP-address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
  Version= RIP-1
  Multicast= None
  IP Policies= 1,2
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:
```

ГЛАВА 29

Расписание вызовов

Функция расписания вызовов (применяется только для инкапсуляции PPPoA или PPPoE) позволяет определять время и продолжительность вызовов на удаленный узел.

29.1 Введение

Функция расписания вызовов позволяет модему управлять удаленным узлом и определять время и продолжительность вызовов на удаленный узел. Эта функция аналогична таймеру записи видеомэгнофона (где можно установить период времени для записи). Можно применять до 4 наборов расписаний с помощью **Меню 11.1 - Профиль удаленного узла**. В Главном меню, введите 26 для перехода в **Меню 26 - Создание расписания**, как показано ниже.

Рис. 165 Меню 26 - Создание расписания

```

Menu 26 - Schedule Setup

Schedule
Set #      Name
-----
  1      _____
  2      _____
  3      _____
  4      _____
  5      _____
  6      _____

Schedule
Set #      Name
-----
  7      _____
  8      _____
  9      _____
 10      _____
 11      _____
 12      _____

Enter Schedule Set Number to Configure= 0

Edit Name= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Расписание с меньшим номером имеет приоритет над расписанием с более высоким номером, благодаря чему исключаются конфликты между расписаниями. Например, если для удаленного узла применены наборы 1, 2, 3 и 4, то набор 1 будет иметь приоритет над наборами 2, 3 и 4, так как модем по умолчанию применяет сначала наборы с более низкими номерами. Набор 2 будет иметь приоритет над наборами 3 и 4 и так далее.

Для одного удаленного узла можно создать до 12 наборов расписаний, но применить можно - не более четырех.



ПРИМЕЧАНИЕ: Для удаления расписания введите номер набора и нажмите клавишу **[ПРОБЕЛ]** и затем **[ENTER]** (или **[delete]**) в поле **Edit Name** (Редактировать имя).

Для создания набора расписания, выберите набор в Меню 26 (1-12) и нажмите клавишу **[ENTER]** для перехода в **Меню 26.1 — Создание набора расписания**, как показано ниже.

Рис. 166 Меню 26.1 - создание набора расписания

```

Menu 26.1 Schedule Set Setup

Active= Yes
Start Date (yyyy-mm-dd)= 2000 - 01 - 01
How Often= Once
Once:
    Date (yyyy-mm-dd)= 2000 - 01 - 01
Weekdays:
    Sunday= N/A
    Monday= N/A
    Tuesday= N/A
    Wednesday= N/A
    Thursday= N/A
    Friday= N/A
    Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On

Press ENTER to Confirm or ESC to Cancel:

```

Если соединение уже установлено, модем не будет его разрывать. После разрыва соединения вручную или вследствие превышения времени неактивности, к удаленному узлу нельзя будет обратиться до истечения периода **Duration (Продолжительность)**.

Табл. 73 Меню 26.1 - Создание расписания

ПОЛЕ	ОПИСАНИЕ
Active (Включить)	Нажмите клавишу [ПРОБЕЛ] для выбора Yes или No . Выберите Yes и нажмите клавишу [ENTER] для включения данного расписания.
Start Date (Дата начала)	Введите дату начала применения данного расписания, в формате "год-месяц-день". Допускаются даты, начиная с текущей и до 31 декабря 2036 года.
How Often (Периодичность)	Применяется ли данное расписание еженедельно или выполниться только один раз. Нажмите клавишу [ПРОБЕЛ] и затем [ENTER] для выбора Once (Однократно) или Weekly (Еженедельно) . Оба эти варианта взаимно исключают друг друга. Если выбрано Once (Однократно) , выбор дня недели недоступен N/A . Если выбрано Once (Однократно) , правило расписания автоматически удаляется после того, как указанное время прошло.

Табл. 73 Меню 26.1 - Создание расписания (продолжение)

ПОЛЕ	ОПИСАНИЕ
Once (Однократно): Date (Дата)	Если в указанном выше поле How Often (Периодичность) выбрано Once (Однократно) , введите дату активирования расписания в формате "год-месяц-день".
Weekday (День недели): Day (День)	Если в указанном выше поле How Often (Периодичность) выбрано Weekly (Еженедельно) , выберите день (дни), когда необходимо активировать набор (или повторить), т.е. перейдите к нужному дню(дням) и нажмите клавишу [ПРОБЕЛ] для выбора Yes (Да) , а затем нажмите клавишу [ENTER].
Start Time (Время начала)	Введите время начала применения расписания в формате "часы-минуты".
Duration (Продолжительность)	Введите максимально допустимую продолжительность соединения в формате "часы-минуты".
Action (Действие)	Значение Forced On (Принудительно поддерживать) означает, что соединение поддерживается независимо от наличия запроса в линии и сохраняется в течение времени, заданного в поле Duration (Продолжительность) . Forced Down (Принудительно разрывать) означает, что соединение блокируется независимо от наличия запроса в линии. Enable Dial-On-Demand (Разрешить вызов по требованию) означает, что данное расписание разрешает соединение по запросу в линии. Disable Dial-On-Demand (Запретить вызов по требованию) означает, что данное расписание не разрешает соединение по запросу в линии.
После завершения настройки данного меню, нажмите клавишу [ENTER] в строке приглашения "Press ENTER to Confirm or ESC to Cancel:" (Нажмите [ENTER] для подтверждения или [ESC] для отмены) для сохранения сделанных изменений, или нажмите клавишу [ESC] для отмены в любое время.	

После настройки расписаний их нужно применить к требуемому удаленному узлу(ам). Введите 11 в **Главном меню**, а затем введите индекс удаленного узла. Используя клавишу [ПРОБЕЛ] выберите **PPPoE** или **PPPoA** в поле **Encapsulation (Инкапсуляция)**, а затем нажмите клавишу [ENTER] для того, чтобы сделать доступными поля расписаний, как показано ниже.

Рис. 167 Применение расписания к удаленному узлу (PPPoE)

```
Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                Route= IP
Active= Yes                          Bridge= No
Encapsulation= PPPoA                Edit IP/Bridge= No
Multiplexing= LLC-based              Edit ATM Options= No
Service Name= N/A                   Edit Advance Options= N/A
Incoming:                             Telco Option:
  Rem Login=                          Allocated Budget(min)= 0
  Rem Password= *****               Period(hr)= 0
Outgoing:                               Schedules Sets= 1,2,3,4
  My Login= ChangeMe                  Nailed-Up Connection= No
  My Password= *****               Session Options:
  Authen= CHAP/PAP                    Edit Filter Sets= No
                                       Idle Timeout(sec)= 0

Press ENTER to Confirm or ESC to Cancel:
```

Для одного удаленного узла можно применить до четырех расписаний, посредством ввода их номеров через запятую. Измените номера расписаний в соответствии с требованиями.

ГЛАВА 30

Поиск и устранение неисправностей

В данной главе рассматриваются возможные неисправности и способы их устранения.

30.1 Неисправности при запуске модема

Табл. 74 Поиск и устранение неисправностей при запуске модема

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
При включении электропитания модема ни один из светодиодов не загорается.	Убедитесь, что адаптер питания подключен к модему и к соответствующему источнику питания. Проверьте, что модем и источник питания включены. Выключите и снова включите модем. Если проблема не устранена, возможно, имеет место аппаратная неисправность. В этом случае следует связаться с поставщиком оборудования.

30.2 Неисправность светодиода LAN

Табл. 75 Устранение неисправностей светодиода LAN

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Светодиод LAN не горит.	Проверьте тип кабеля Ethernet и его подключение (более подробно см. <i>Краткое руководство</i>). Проверьте исправность кабеля Ethernet.
	Убедитесь, что карта Ethernet компьютера работает нормально.

30.3 Неисправность светодиода DSL

Табл. 76 Устранение неисправностей светодиода DSL

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Светодиод DSL не горит.	Проверьте телефонный провод и соединение между портом DSL модема и телефонной розеткой.
	Убедитесь, что телефонная компания проверила вашу телефонную линию и установила оборудование для услуг DSL.
	Сбросьте ADSL линию, а затем повторно установите соединение с DSL-коммутатором. Более подробно см. Глава 12 Сопровождение (Web-конфигуратор) или Глава 24 Информация о системе и диагностика (SMT) .

30.4 Неисправность интерфейса LAN

Табл. 77 Устранение неисправности интерфейса LAN

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Отсутствует доступ к модему из локальной сети.	Если оба светодиода 10M/100M на передней панели не горят, см. раздел Неисправность светодиода LAN . Убедитесь, что IP-адрес и маска подсети модема и компьютера(ов) находятся в одной подсети.
На команду "ping" не отвечает ни один компьютер локальной сети.	Если оба светодиода 10M/100M на передней панели не горят, см. раздел Неисправность светодиода LAN . Убедитесь, что IP-адрес и маска подсети модема и компьютера(ов) находятся в одной подсети.

30.5 Неисправность интерфейса WAN

Табл. 78 Устранение неисправности интерфейса WAN

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Невозможно получить IP-адрес в глобальной сети от Интернет-провайдера.	Интернет-провайдер предоставляет IP-адрес в глобальной сети после проведения аутентификации. Аутентификация может проводиться с использованием имени пользователя и пароля, MAC-адреса или имени узла. Имя пользователя и пароль применяются только при инкапсуляции PPPoE и PPPoA. Убедитесь, что вы правильно ввели Service Type (Тип услуги) , User Name (Имя пользователя) и Password (Пароль) (убедитесь в правильном использовании регистра символов). См. Глава 6 Настройка глобальной сети (Web-конфигуратор) или Глава 17 Доступ в Интернет (SMT) .

30.6 Неисправность при доступе в Интернет

Табл. 79 Устранение неисправностей при доступе в Интернет

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Невозможно получить доступ в Интернет.	<p>Убедитесь, что модем включен и подключен к сети.</p> <p>Если светодиод DSL не горит, см. раздел Неисправность светодиода DSL .</p> <p>Проверьте настройки глобальной сети. См. главу по настройке глобальной сети (Web-конфигуратор) или раздел о доступе в Интернет (SMT).</p> <p>Убедитесь, что вы ввели правильное имя пользователя и пароль.</p> <p>Если включено сквозное пропускание PPPoE, убедитесь, что функция моста отключена. Более подробно см. Глава 14 Меню 1 - Настройка общих параметров .</p>
Подключение к Интернету разрывается.	<p>Проверьте правила расписания вызовов. См. Глава 29 Расписание вызовов (SMT).</p> <p>Если используется инкапсуляция PPPoA или PPPoE, проверьте значение времени неактивности. См. Глава 6 Настройка глобальной сети (Web-конфигуратор) или Глава 18 Настройка удаленного узла (SMT).</p> <p>Свяжитесь с вашим Интернет-провайдером.</p>

30.7 Неисправности, связанные с паролем

Табл. 80 Устранение неисправностей, связанных с паролем

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Невозможно получить доступ к модему.	<p>Имя пользователя для доступа - "admin". По умолчанию установлен пароль "1234". Поля Password (Пароль) и Username (Имя пользователя) необходимо заполнять с учетом регистра. Убедитесь, что вы ввели правильный пароль и имя пользователя в соответствующем регистре.</p> <p>Если вы изменили пароль и забыли его, необходимо загрузить файл конфигурации по умолчанию (см. раздел Сброс модема к заводским установкам в Глава 2 Знакомство с Web-конфигуратором). При этом восстанавливаются заводские настройки по умолчанию, включая пароль.</p>

30.8 Неисправности, связанные с Web-конфигуратором

Табл. 81 Устранение неисправностей, связанных Web-конфигуратором

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Нет доступа к Web-конфигуратору.	<p>Проверьте подключение оборудования, см. <i>Краткое руководство</i>.</p> <p>Убедитесь, что не проводится сеанс управления с помощью SMT.</p> <p>Проверьте, что доступ к службе web включен. Если установлен IP-адрес доверенного клиента, IP-адрес вашего компьютера должен совпадать с ним. Для получения более подробной информации см. Глава 27 Удаленное управление.</p> <p>Для доступа через глобальную сеть, необходимо в настройке удаленного управления разрешить управление из глобальной сети или отовсюду: опция WAN only (Только через глобальную сеть) или All (Через локальную и глобальную сеть). Для получения более подробной информации см. Глава 27 Удаленное управление.</p> <p>Для доступа через локальную сеть, IP-адреса вашего компьютера и модема должны находиться в одной подсети.</p> <p>Если вы изменили IP-адрес модема в локальной сети, то в поле URL необходимо ввести новый адрес.</p> <p>Удалите все фильтры в меню SMT 3.1 (LAN) или 11.5 (WAN), которые блокируют службу web.</p> <p>Также см. раздел Неисправности при удаленном управлении.</p>

30.9 Неисправности при удаленном управлении

Табл. 82 Устранение неисправностей при удаленном управлении

НЕИСПРАВНОСТЬ	СПОСОБЫ УСТРАНЕНИЯ
Невозможно удаленно управлять модемом из локальной или глобальной сети.	См. Глава 10 Настройка удаленного управления раздел Ограничения на удаленное управление о сценариях, при которых выполнение удаленного управления невозможно.
	При настройке через глобальную сеть следует использовать IP-адрес модема в глобальной сети.
	При настройке через локальную сеть следует использовать IP-адрес модема в локальной сети.
	См. указания для выполнения проверки подключения к локальной сети.
	См. раздел Неисправность интерфейса LAN для выполнения проверки подключения к глобальной сети.
	Также см. раздел Неисправности, связанные с Web-конфигуратором .

Приложение А

Сплиттеры и микрофильтры

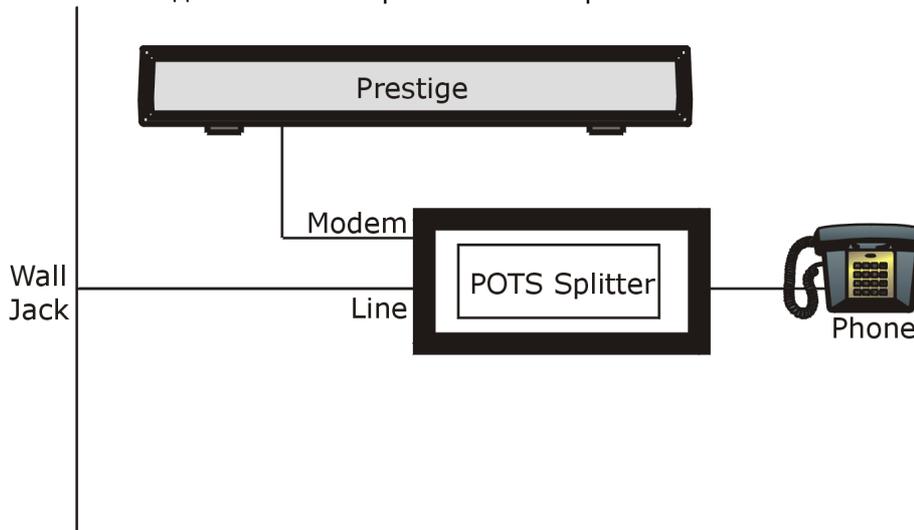
В этом приложении описывается установка сплиттера для подключения телефонного аппарата и телефонного микрофильтра.

Подключение телефонного сплиттера

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

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

Рис. 168 Подключение телефонного сплиттера



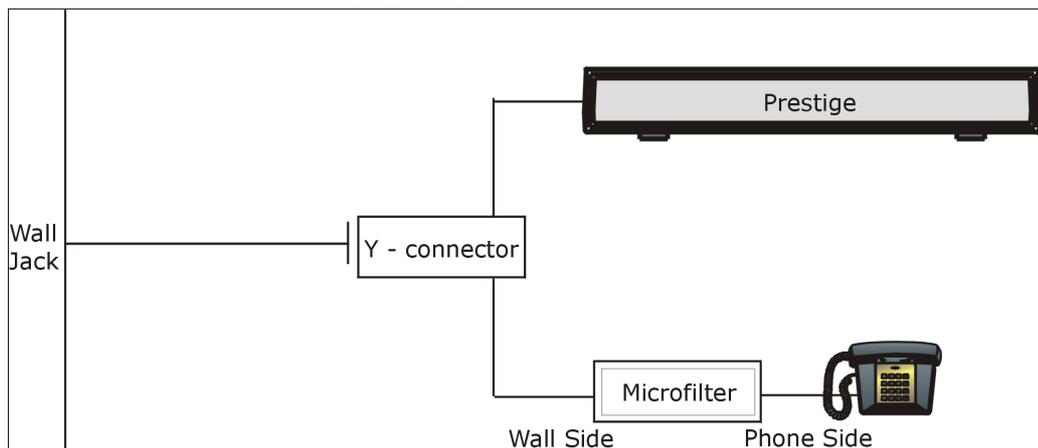
- 1 Подключите разъем с маркировкой "Phone" к телефону.
- 2 Подключите разъем с маркировкой "Modem" к модему.
- 3 Подключите разъем с маркировкой "Line" к настенной телефонной розетке.

Телефонные микрофильтры

Передача речи по телефонной линии осуществляется в нижнем диапазоне частот от 0 до 4 кГц, а сигналы ADSL передаются в более высоком диапазоне частот, выше 4 кГц. Микрофильтр действует как фильтр нижних частот для телефона, что обеспечивает отсутствие влияния сигналов ADSL на передачу телефонных сигналов. Телефонный микрофильтр поставляется отдельно.

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

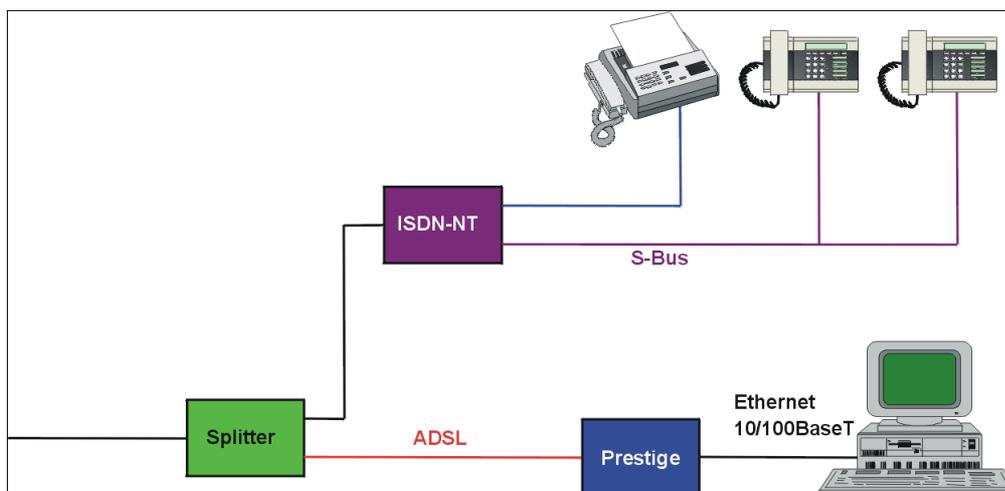
Рис. 169 Подключение микрофильтра



Использование модема с ISDN

Этот раздел предназначен только для тех, кто использует модем с ADSL по сети ISDN (Integrated Services Digital Network - Цифровая сеть с предоставлением комплексных услуг). Далее приводится пример установки модема для использования с ISDN.

Рис. 170 Использование модема с ISDN



Приложение В

Установка IP-адреса компьютера

На все компьютеры должны быть установлены сетевые адаптеры Ethernet 10 Мбит/с или 100 Мбит/с и протоколы TCP/IP.

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

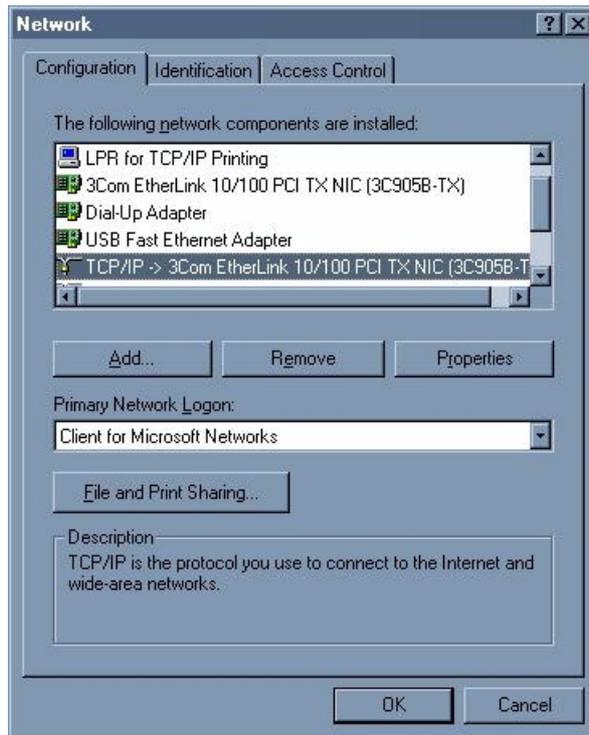
TCP/IP должен быть уже инсталлирован на компьютерах с системами Windows NT/2000/XP, Macintosh OS 7 или более поздними операционными системами.

После соответствующей установки компонентов TCP/IP, настройте параметры TCP/IP для взаимодействия с вашей сетью.

Если параметры IP назначаются вручную вместо динамического назначения, убедитесь, что ваши компьютеры имеют IP-адреса, относящиеся к той же подсети, что и порт LAN модема.

Windows 95/98/Me

Щелкните **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)** и дважды щелкните на иконке **Network (Сеть)** для отображения окна **Network (Сеть)**.

Рис. 171 Windows 95/98/Me: Сеть: Конфигурация

Установка компонент

В окне **Network (Сеть)** на закладке **Configuration (Настройки)** отображается список установленных компонентов. Вам необходим сетевой адаптер, протокол TCP/IP и Client for Microsoft Networks (Клиент для сетей Microsoft).

Если необходимо установить адаптер:

- 1 В окне **Network (Сеть)** щелкните **Add (Добавить)**.
- 2 Выберите **Adapter (Адаптер)** и щелкните **Add (Добавить)**.
- 3 Выберите производителя и модель вашего сетевого адаптера и щелкните **OK**.

Если необходимо установить протокол TCP/IP:

- 1 В окне **Network (Сеть)** щелкните **Add (Добавить)**
- 2 Выберите **Protocol (Протокол)** и щелкните **Add (Добавить)**.
- 3 Выберите **Microsoft** в списке **производителей**.
- 4 Выберите **TCP/IP** из списка сетевых протоколов и щелкните по кнопке **OK**.

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

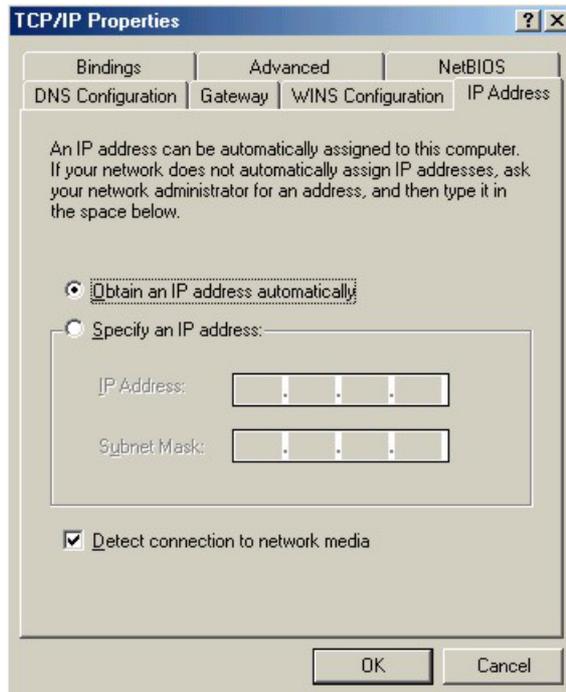
- 1 Щелкните по кнопке **Add (Добавить)**.
- 2 Выберите **Client (Клиент)** и щелкните **Add (Добавить)**.

- 3 Выберите **Microsoft** в списке производителей.
- 4 Выберите **Client for Microsoft Networks (Клиент для сетей Microsoft)** из списка сетевых клиентов и щелкните **ОК**.
- 5 Перезагрузите компьютер, чтобы сделанные изменения вступили в силу.

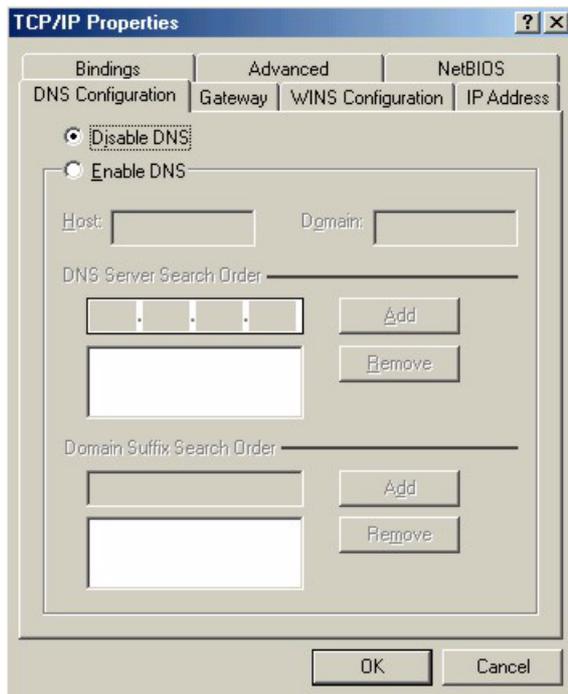
Настройка

- 1 В окне **Network (Сеть)** щелкните на закладке **Configuration (Конфигурация)**, выберите запись TCP/IP для вашего сетевого адаптера и щелкните **Properties (Свойства)**
- 2 Щелкните на закладке **IP Address (IP-адрес)**.
 - Если вы используете динамический IP-адрес, выберите **Obtain an IP address automatically (Получать IP-адрес автоматически)**.
 - Если вы используете статический IP-адрес, выберите **Specify an IP address (Использовать следующий IP-адрес)** и заполните поля **IP Address (IP-адрес)** и **Subnet Mask (Маска подсети)**.

Рис. 172 Windows 95/98/Me: Свойства TCP/IP: IP-адрес



- 3 Щелкните на закладке **DNS**.
 - Если вы не знаете параметры DNS, выберите **Disable DNS (Отключить DNS)**.
 - Если вам известны параметры DNS, выберите **Enable DNS (Включить DNS)** и заполните поля, расположенные ниже (возможно, потребуется заполнять не все поля).

Рис. 173 Windows 95/98/Me: Свойства TCP/IP: Конфигурация DNS**4** Щелкните на закладке **Gateway (Шлюз)**.

- Если вы не знаете IP-адрес шлюза, удалите все установленные ранее шлюзы.
- Если у вас есть IP-адрес шлюза, введите его в поле **New gateway (Новый шлюз)** и щелкните по кнопке **Add (Добавить)**.

5 Щелкните **OK**, чтобы сохранить сделанные изменения и закрыть окно **TCP/IP Properties (Свойства TCP/IP)**.**6** Щелкните по кнопке **OK**, чтобы закрыть окно **Network (Сеть)**. При появлении запроса вставьте компакт-диск Windows.**7** Включите модем и перезагрузите компьютер при появлении запроса.**Проверка конфигурации****1** Щелкните **Start (Пуск)**, а затем **Run (Выполнить)**.**2** В окне **Run (Выполнить)** введите команду "winipcfg", а затем щелкните **OK** для отображения окна **IP Configuration (Настройки IP)**.**3** Выберите свой сетевой адаптер. При этом должен отображаться IP-адрес и маска подсети вашего компьютера, а также шлюз по умолчанию.

Windows 2000/NT/XP

- 1 В Windows XP щелкните **Start (Пуск)**, **Control Panel (Панель управления)**. В Windows 2000/NT щелкните **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)**.

Рис. 174 Windows XP: Меню Start (Пуск)

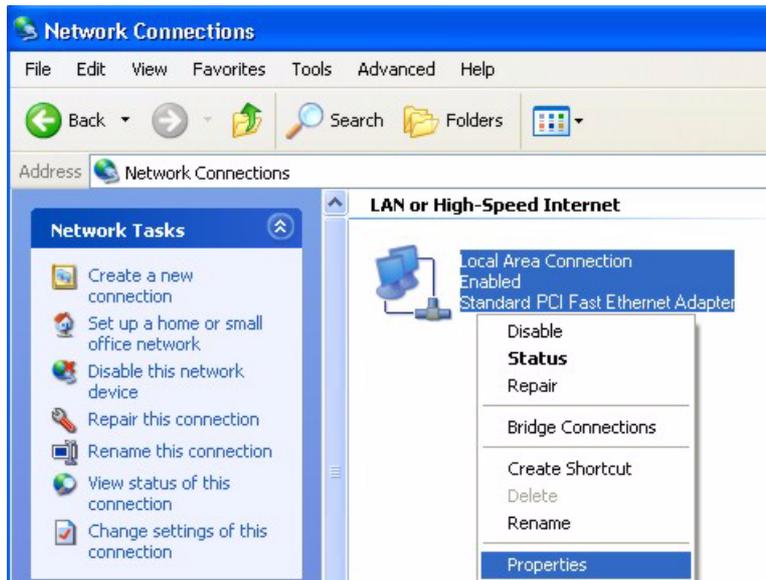


- 2 В Windows XP щелкните **Network Connections (Сетевые подключения)**. В Windows 2000/NT щелкните **Network and Dial-up Connections (Сеть и удаленный доступ к сети)**.

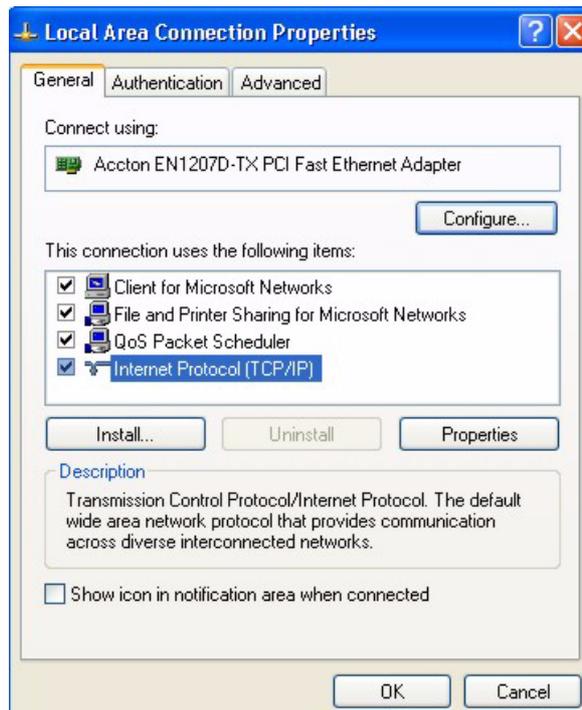
Рис. 175 Windows XP: Панель управления



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

Рис. 176 Windows XP: Панель управления: Сетевые подключения: Свойства

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

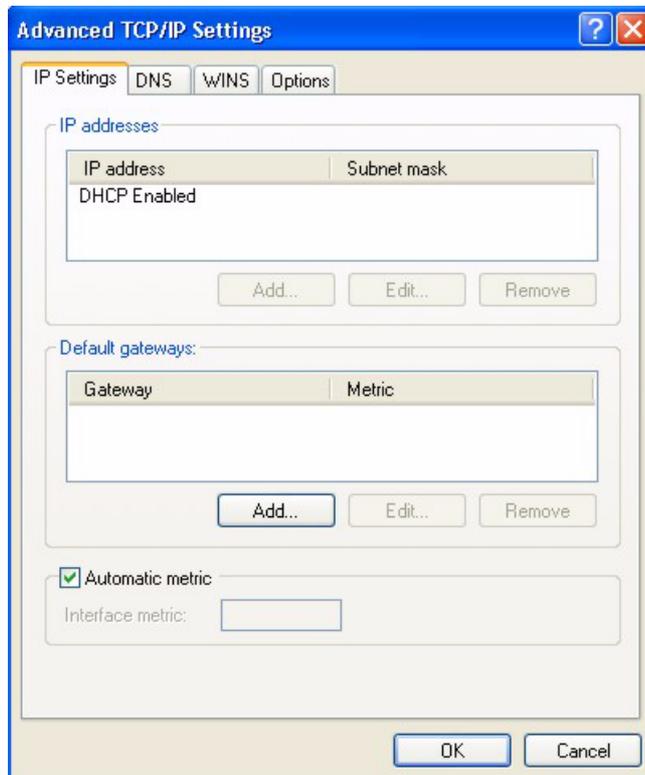
Рис. 177 Windows XP: Свойства подключения по локальной сети

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

- Если вы используете динамический IP-адрес, щелкните **Obtain an IP address automatically (Получать IP-адрес автоматически)**.

- Если вы имеете статический IP-адрес, щелкните **Use the following IP Address (Использовать следующий IP-адрес)** и заполните поля **IP address (IP-адрес)**, **Subnet mask (Маска подсети)** и **Default gateway (Шлюз по умолчанию)**. Щелкните **Advanced (Дополнительно)**.

Рис. 178 Windows XP: Дополнительные параметры TCP/IP



- 6** Если Вы не знаете IP-адрес шлюза, удалите все предварительно установленные шлюзы на закладке **IP Settings (Параметры IP)** и щелкните **OK**.

Для настройки дополнительных IP-адресов выполните следующую процедуру один или более раз:

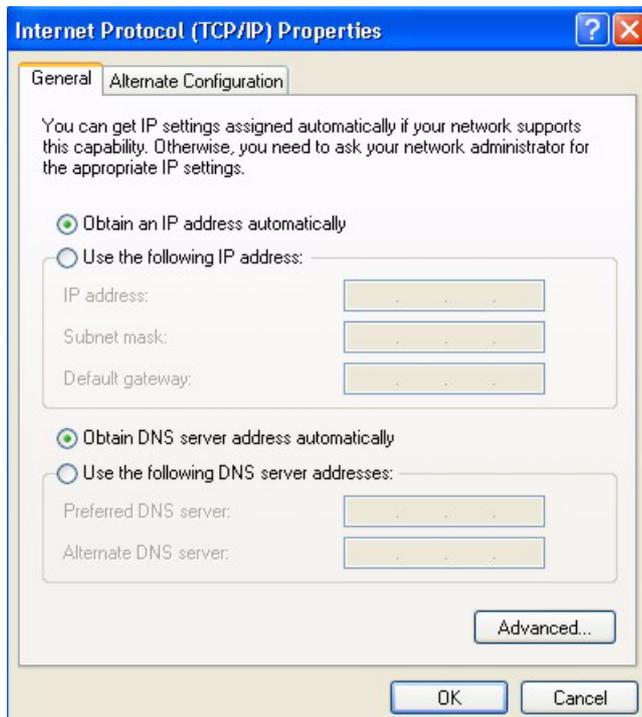
- На закладке **IP Settings (Настройки IP)** в поле для IP-адресов щелкните **Add (Добавить)**.
- В окошке **TCP/IP Address**, введите IP-адрес в поле **IP address (IP-адрес)** и маску подсети в поле **Subnet mask (Маска подсети)**, затем щелкните по кнопке **Add (Добавить)**.
- Повторите два предыдущих действия для каждого IP-адреса, который вы хотите добавить.
- Настройте дополнительные шлюзы по умолчанию на закладке **IP Settings (Параметры IP)**, щелкнув по кнопке **Add (Добавить)** в разделе **Default gateways (Шлюзы по умолчанию)**.

- В окне **TCP/IP Gateway Address (Адрес шлюза TCP/IP)**, введите IP-адрес шлюза по умолчанию в поле **Gateway (Шлюз)**. Для ручной настройки метрики по умолчанию (количества транзитных пунктов при передаче), снимите флажок **Automatic metric (Автоматическая метрика)** и введите значение в поле **Metric (Метрика)**.
- Щелкните по кнопке **Add (Добавить)**.
- Повторите описанные предыдущие три действия для всех шлюзов, которые необходимо добавить.
- Щелкните **ОК** после завершения настройки.

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

- Щелкните **Obtain DNS server automatically (Получить сервер DNS автоматически)**, если вы не знаете IP-адрес(а) сервера(ов) DNS.
- Если вы знаете IP-адрес(а) сервера(ов) DNS, щелкните **Use the following DNS server addresses (Использовать следующие адреса сервера DNS)**, и введите их в поля **Preferred DNS server (Предпочтительный сервер DNS)** и **Alternate DNS server (Альтернативный сервер DNS)**.

Если серверы DNS были настроены ранее, щелкните **Advanced (Дополнительно)** и затем закладку **DNS** для определения порядка их использования.

Рис. 179 Windows XP: Свойства: Протокол Интернета (TCP/IP)

- 8** Щелкните **ОК**, чтобы закрыть окно **Internet Protocol (TCP/IP) Properties** (**Свойства: Протокол Интернета TCP/IP**).
- 9** Щелкните **ОК**, чтобы закрыть окно **Local Area Connection Properties** (**Свойства подключения по локальной сети**).
- 10** Включите модем и перезагрузите компьютер при появлении запроса.

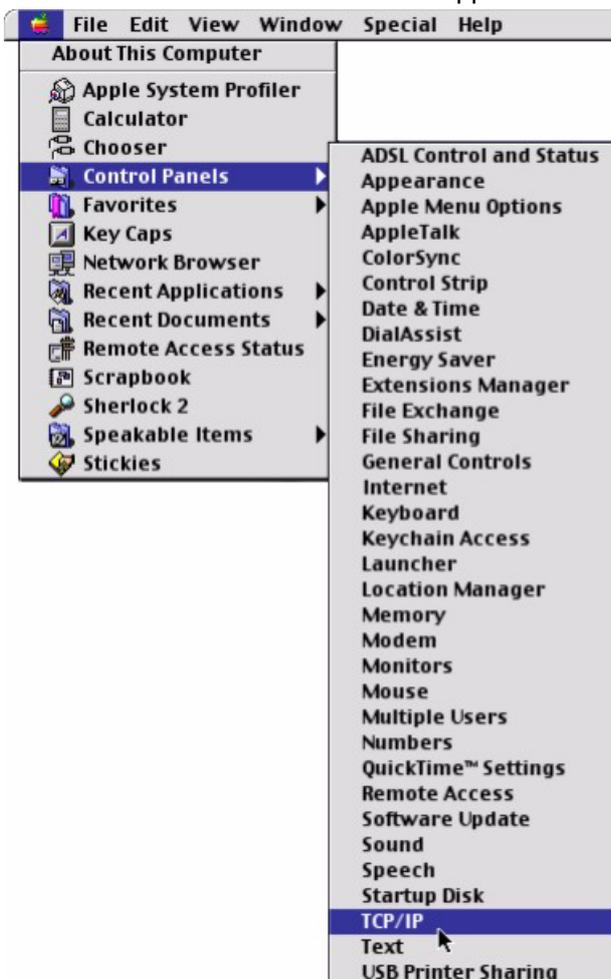
Проверка конфигурации

- 1** Щелкните **Start** (**Пуск**), **All Programs** (**Программы**), **Accessories** (**Стандартные**), **Command Prompt** (**Командная строка**).
- 2** В окне **Command Prompt** (**Командная строка**) введите команду "ipconfig" и нажмите клавишу [ENTER]. Также можно открыть окно **Network Connections** (**Сетевые подключения**), щелкнуть правой кнопкой мыши на сетевом подключении, выбрать **Status** (**Состояние**) и затем щелкнуть закладку **Support** (**Поддержка**).

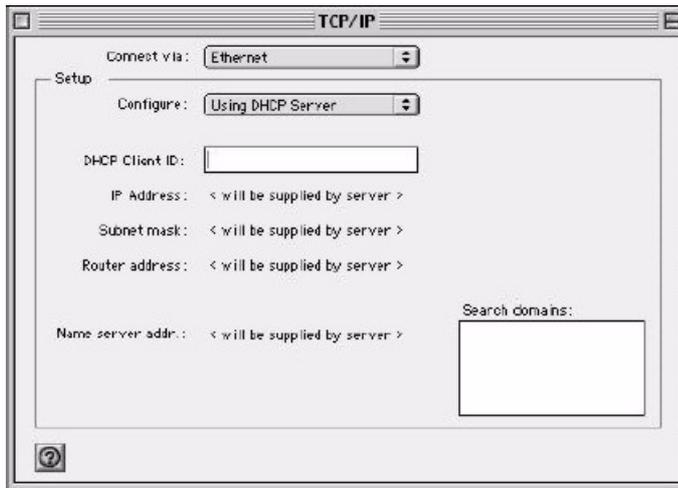
Macintosh OS 8/9

- 1** Щелкните меню **Apple**, **Control Panel** (**Панель управления**), а затем дважды щелкните **TCP/IP**, чтобы открыть **TCP/IP Control Panel** (**Панель управления TCP/IP**).

Рис. 180 Macintosh OS 8/9: Меню Apple



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

Рис. 181 Macintosh OS 8/9: TCP/IP

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

4 Для настройки статических параметров выполните следующие действия:

- В разделе **Configure (Настроить)**, выберите **Manually (Настроить вручную)**.
- Введите IP-адрес в окне **IP Address (IP-адрес)**.
- Введите маску подсети в окне **Subnet mask (Маска подсети)**.
- Введите IP-адрес модема в поле **Router address (Адрес маршрутизатора)**.

5 Закройте окно **TCP/IP Control Panel (Панель управления TCP/IP)**.

6 При появлении запроса щелкните **Save (Сохранить)** для сохранения изменений в конфигурации.

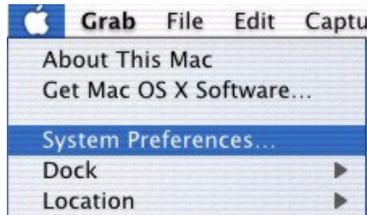
7 Включите модем и перезагрузите компьютер при появлении запроса.

Проверка конфигурации

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

Macintosh OS X

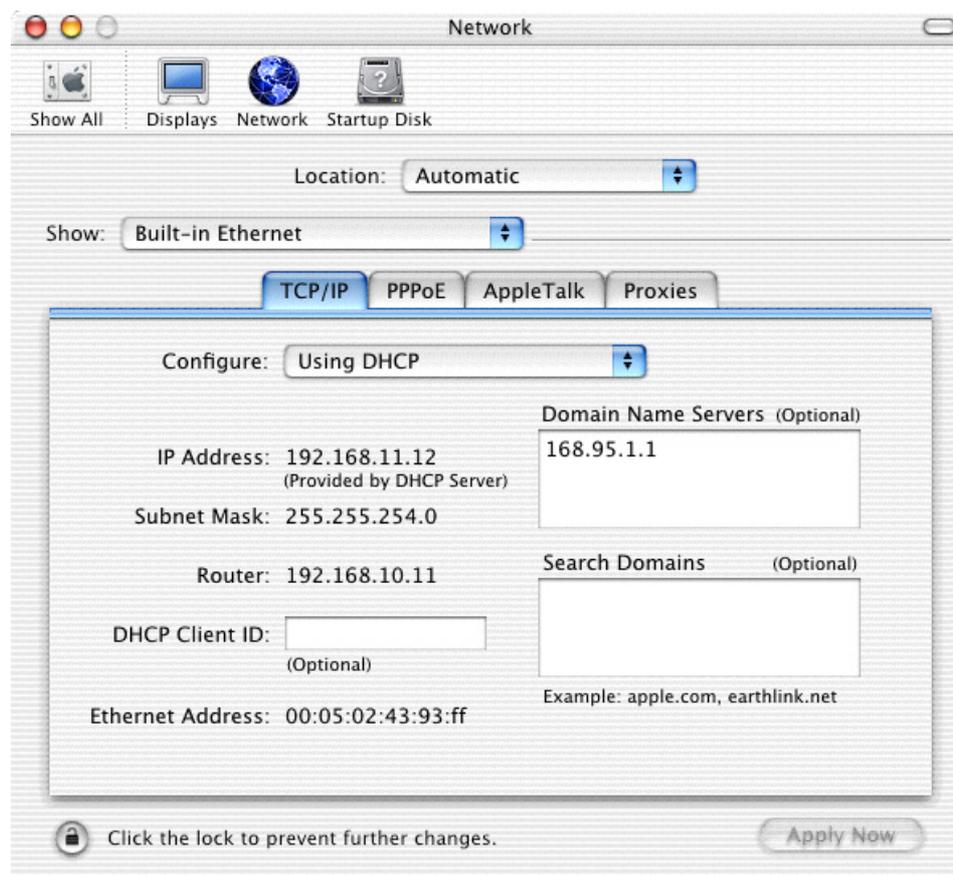
1 Щелкните меню **Apple** и затем **System Preferences (Настройки системы)**, чтобы открыть окно **System Preferences (Настройки системы)**.

Рис. 182 Macintosh OS X: Меню Apple

2 Щелкните **Network (Сеть)** на панели иконок.

- Выберите **Automatic (Автоматически)** в списке **Location (Местонахождение)**.
- Выберите **Built-in Ethernet (Встроенный сетевой контроллер)** из списка **Show (Показать)**.
- Щелкните по закладке **TCP/IP**.

3 Для настройки динамических параметров выберите **Using DHCP (Использовать DHCP)** в списке **Configure (Настроить)**.

Рис. 183 Macintosh OS X: Сеть

4 Для настройки статических параметров выполните следующие действия:

- В разделе **Configure (Настроить)**, выберите **Manually (Настроить вручную)**.
- Введите IP-адрес в окне **IP Address (IP-адрес)**.

- Введите маску подсети в окне **Subnet mask (Маска подсети)**.
- Введите IP-адрес модема в поле **Router address (Адрес маршрутизатора)**.

5 Щелкните **Apply Now (Применить)** и закройте окно.

6 Включите модем и перезагрузите компьютер при появлении запроса.

Проверка конфигурации

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

Приложение С

Организация подсетей IP

Адресация IP

Маршрутизаторы выбирают “маршрут” на основе номера сети. Маршрутизатор при доставке пакета данных соответствующему получателю использует идентификатор узла.

Классы IP

IP-адрес состоит из четырех байтов (8 бит каждый), записанных в десятичном формате с разделительными точками, например, 192.168.1.1. IP-адреса подразделяются на различные классы. Класс адреса зависит от значения первого байта.

- Адреса класса “А” имеют значение 0 в самом левом бите. В адресах класса “А” первый байт является номером сети, а остальные три байта составляют идентификатор узла.
- Адреса класса “В” имеют 1 в самом левом бите и 0 в следующем. В адресах класса “В” первые два байта являются номером сети, а остальные два байта составляют идентификатор узла.
- Адреса класса “С” начинаются (читая слева направо) с последовательности 1 1 0. В адресах класса “С” первые три байта составляют номер сети, а последний байт является идентификатором узла.
- Адреса класса “D” начинаются с 1 1 1 0. Адреса класса “D” используются для многоадресных рассылок. (Еще существуют адреса класса “Е”. Они зарезервированы для будущего использования.)

Табл. 83 Классы IP-адресов

IP-АДРЕС:		БАЙТ 1	БАЙТ 2	БАЙТ 3	БАЙТ 4
Класс А	0	Номер сети	Идентификатор узла	Идентификатор узла	Идентификатор узла
Класс В	10	Номер сети	Номер сети	Идентификатор узла	Идентификатор узла
Класс С	110	Номер сети	Номер сети	Номер сети	Идентификатор узла



ПРИМЕЧАНИЕ: Идентификатор узла не может содержать только нули или только единицы.

Поэтому:

В сети класса “С” (8 бит для узлов) может быть $2^8 - 2$, т. е. 254 узла.

В сети класса “В” (16 бит для узлов) может быть $2^{16} - 2$, т. е. 65534 узла.

В сети класса “А” (24 бита для узлов) может быть $2^{24} - 2$ узлов (примерно 16 миллионов узлов).

Поскольку первый байт IP-адреса класса “А” должен начинаться с “0”, первый байт адреса класса “А” может принимать значения от 0 до 127.

Аналогично, первый байт адреса класса “В” должен начинаться с “10”, поэтому первый байт адреса класса “В” может принимать значения от 128 до 191. Первый байт адреса класса “С” начинается с “110”, и поэтому имеет диапазон значений от 192 до 223.

Табл. 84 Допустимые диапазоны IP-адресов для каждого класса

КЛАСС	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО БАЙТА (В ДВОИЧНОЙ ЗАПИСИ)	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО БАЙТА (В ДЕСЯТИЧНОЙ ЗАПИСИ)
Класс А	от 00000000 до 01111111	от 0 до 127
Класс В	от 10000000 до 10111111	от 128 до 191
Класс С	от 11000000 до 11011111	от 192 до 223
Класс D	от 11100000 до 11101111	от 224 до 239

Маска подсети

Маска подсети используется для определения, сколько битов используется для номера сети и сколько для идентификатора узла (при помощи операции логического "И"). Если бит маски подсети имеет значение “1”, это значит, что соответствующий бит IP-адреса является частью номера сети. Если бит маски подсети имеет значение “0”, это значит, что соответствующий бит IP-адреса является частью идентификатора узла.

Маски подсети записываются в десятичном формате с разделительными точками, так же, как и IP-адреса. “Естественные” маски для классов IP-адресов А, В и С приведены ниже.

Табл. 85 “Естественные” маски

КЛАСС	ЕСТЕСТВЕННАЯ МАСКА
А	255.0.0.0
В	255.255.0.0
С	255.255.255.0

Организация подсетей

При организации подсетей распределение IP-адресов по классам игнорируется. Например, адрес класса C не обязательно должен иметь номер сети из 24 бит и идентификатор узла из 8 бит. При организации подсетей некоторые биты идентификатора узла можно использовать в качестве битов номера сети. По договоренности маска подсети всегда состоит из непрерывной последовательности единиц в начале маски (слева), за которой следует непрерывная последовательность нулей, и имеет общую длину 32 бита.

Поскольку маска всегда состоит из непрерывной последовательности единиц в начале и непрерывной последовательности нулей в оставшихся битах и имеет длину 32 бита, можно просто указывать количество единиц вместо того, чтобы записывать значение каждого бита. Это обычно обозначается посредством записи символа “/” после адреса и количества бит с единицами.

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

В следующей таблице приведены все возможные маски подсети для адресов класса “C”, записанные в двух вариантах.

Табл. 86 Альтернативные варианты записи маски подсети

МАСКА IP ПОДСЕТИ-АДРЕСА	МАСКА ПОДСЕТИ ПРИ ЗАПИСИ КОЛИЧЕСТВА “1”	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

Первая маска - это естественная маска класса “C”. Обычно, если маска подсети не указана, то считается, что используется естественная маска.

Пример: Две подсети

В качестве примера рассмотрим адрес класса “С” 192.168.1.0 с маской подсети 255.255.255.0.

Табл. 87 Пример организации 2-х подсетей

	НОМЕР СЕТИ	ИДЕНТИФИКАТОР УЗЛА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	00000000
Маска подсети	255.255.255.	0
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	00000000

Первые три байта адреса образуют номер сети (класс “С”). Необходимо иметь две отдельные сети.

Разделите сеть 192.168.1.0 на две отдельных подсети, преобразовав один бит идентификатора узла в IP-адресе в бит номера сети. “Заимствованный” бит идентификатора узла может принимать значение “0” или “1”, что позволяет организовать две подсети; 192.168.1.0 с маской подсети 255.255.255.128 и 192.168.1.128 с маской подсети 255.255.255.128.



ПРИМЕЧАНИЕ: В следующих таблицах затененные/выделенные жирным шрифтом значения битов последнего байта обозначают “заимствованные” биты идентификатора узла для образования дополнительных битов номера сети. Количество “заимствованных” битов идентификатора узла определяет число подсетей, которые Вы можете создать. Оставшееся количество битов идентификатора узла (после “заема”) определяет максимально возможное количество узлов в каждой подсети.

Табл. 88 Подсеть 1

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	00000000
Subnet Mask (Маска подсети)	255.255.255.	128
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	10000000
Адрес подсети: 192.168.1.0	Младший идентификатор узла: 192.168.1.1	
Широковещательный адрес: 192.168.1.127	Старший идентификатор узла: 192.168.1.126	

Табл. 89 Подсеть 2

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	128
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	10000000
Subnet Mask (Маска подсети)	255.255.255.	128
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	10000000
Адрес подсети: 192.168.1.128	Младший идентификатор узла: 192.168.1.129	
Широковещательный адрес: 192.168.1.255	Старший идентификатор узла: 192.168.1.254	

Оставшиеся 7 бит определяют максимально возможное количество узлов в каждой подсети. Идентификаторы узлов, состоящие только из нулей, представляют собственно подсеть, а идентификаторы узлов, состоящие только из единиц, являются адресами широковещательной рассылки для каждой подсети, поэтому реальное количество доступных узлов для каждой подсети для данного примера равно $2^7 - 2$, т.е. 126 узлов в каждой подсети.

192.168.1.0 с маской 255.255.255.128 это сама сеть, а 192.168.1.127 с маской 255.255.255.128 является адресом прямой широковещательной рассылки первой подсети. Следовательно, самый младший IP-адрес, который может быть назначен действительному узлу для первой подсети - 192.168.1.1, а старший - 192.168.1.126. Аналогично диапазон адресов для узлов второй подсети - от 192.168.1.129 до 192.168.1.254.

Пример: Четыре подсети

В примере выше демонстрируется использование 25-битной маски подсети для разделения адресного пространства класса "C" на две подсети. Аналогично для разделения адреса класса "C" на четыре подсети, потребуется "позаимствовать" два бита от идентификатора узла для получения четырех возможных комбинаций: 00, 01, 10 и 11. Маска подсети имеет 26 бит (11111111.11111111.11111111.11000000) или 255.255.255.192. Каждая подсеть имеет 6 бит для идентификатора узла, при этом получается $2^6 - 2$ или 62 узла в каждой подсети (все 0 обозначают саму подсеть, все 1 являются широковещательным адресом этой подсети).

Табл. 90 Подсеть 1

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	00000000

Табл. 90 Подсеть 1 (продолжение)

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.0	Младший идентификатор узла: 192.168.1.1	
Широковещательный адрес: 192.168.1.63	Старший идентификатор узла: 192.168.1.62	

Табл. 91 Подсеть 2

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	64
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	01000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.64	Младший идентификатор узла: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Старший идентификатор узла: 192.168.1.126	

Табл. 92 Подсеть 3

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	128
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	10000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	11000000
Адрес подсети: 192.168.1.128	Младший идентификатор узла: 192.168.1.129	
Широковещательный адрес: 192.168.1.191	Старший идентификатор узла: 192.168.1.190	

Табл. 93 Подсеть 4

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	192
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	11000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	11000000

Табл. 93 Подсеть 4 (продолжение)

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
Адрес подсети: 192.168.1.192	Младший идентификатор узла: 192.168.1.193	
Широковещательный адрес: 192.168.1.255	Старший идентификатор узла: 192.168.1.254	

Пример: Восемь подсетей

Аналогично используется 27-битная маска для создания 8-ми подсетей (001, 010, 011, 100, 101, 110).

В следующей таблице приведены значения битов последнего байта адреса класса С для каждой подсети.

Табл. 94 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	223	254	255

В следующей таблице приведены сводные данные по организации подсетей класса “С”.

Табл. 95 Организация подсетей класса С

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

Организация подсетей в сетях класса А и класса В.

Для адресов класса “А” и класса “В” маска подсети также определяет, сколько битов используется для номера сети и сколько для идентификатора узла.

Адреса класса “В” имеют два байта идентификатора узла, доступных для организации подсетей, а адреса класса “А” имеют три доступных байта идентификатора узла (см. Табл. 83) для организации подсетей.

В следующей таблице приведены сводные данные по организации подсетей класса “В”.

Табл. 96 Организация подсетей класса В

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

Приложение D

PPPoE

PPPoE в действии

ADSL-модем образует мост для сеанса PPP поверх Ethernet (PPP over Ethernet, RFC 2516) от вашего компьютера к постоянному виртуальному каналу ATM (Permanent Virtual Circuit - PVC), до DSL-коммутатора, на котором PPP сеанс завершается. (см. Рис. 184). Один постоянный виртуальный канал (PVC) может поддерживать любое количество сеансов PPP из вашей локальной сети. Протокол PPPoE обеспечивает функции управления доступом и учета аналогично услуге доступа по коммутируемой линии с использованием протокола PPP.

Преимущества PPPoE

PPPoE предлагает следующие преимущества:

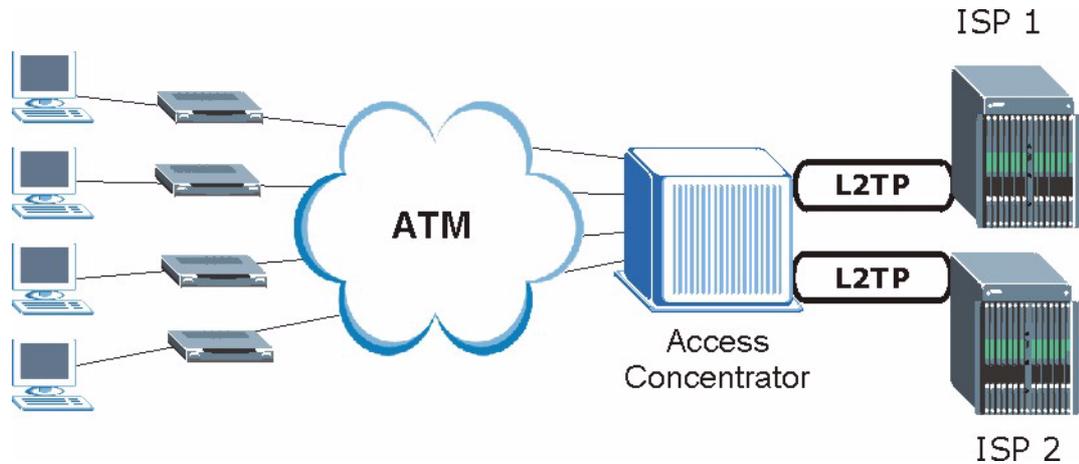
Обеспечивает знакомым по доступу в сеть по коммутируемой линии (Dial-Up Networking - DUN) пользовательским интерфейсом.

Уменьшает затраты операторов связи по обеспечению виртуальных каналов к многочисленным коммутаторам для тысяч пользователей на всем пути до Интернет-провайдера. Для GSTN (PSTN и ISDN) инфраструктура коммутации уже существует.

Позволяет Интернет-провайдеру использовать существующую модель доступа по коммутируемой линии для аутентификации и предоставлять (дополнительно) дифференцированные услуги.

Традиционный сценарий доступа по коммутируемой линии

На следующей схеме представлена типичная конфигурация оборудования, когда компьютеры используют традиционный доступ в сеть по коммутируемой линии.

Рис. 184 Конфигурация оборудования "один маршрутизатор для одного компьютера"

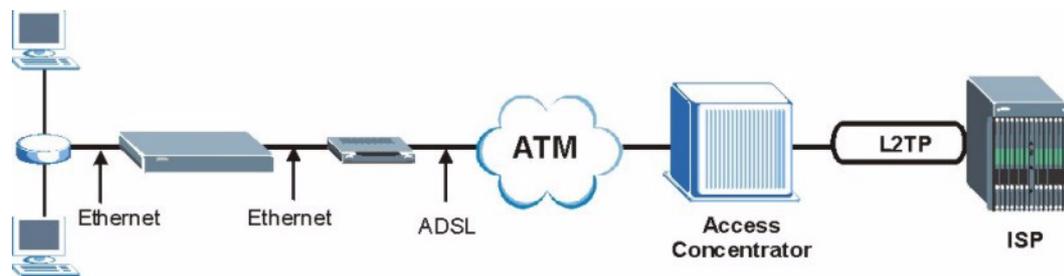
Как работает PPPoE

Драйвер PPPoE представляет Ethernet как последовательный канал связи с компьютером, по которому компьютер использует протокол PPP, в то время как модем передает по образованному мосту кадры Ethernet к DSL-коммутатору, который также называют концентратором доступа (Access Concentrator). При рассмотрении взаимодействия между DSL-коммутатором и Интернет-провайдером, DSL-коммутатор выступает в качестве L2TP (Layer 2 Tunneling Protocol - Протокол туннелирования 2 уровня) LAC (L2TP Access Concentrator - концентратор доступа L2TP) и туннелирует PPP кадры к Интернет-провайдеру. L2TP туннель поддерживает одновременное сквозное пропускание несколько сеансов PPP.

При использовании PPPoE, виртуальный канал (VC - Virtual Circuit) является аналогом коммутируемого соединения и проходит между модемом и DSL-коммутатором на всем пути к Интернет-провайдеру. Однако сеанс PPP устанавливается между компьютером и Интернет-провайдером.

Модем в качестве клиента PPPoE

При использовании модема в качестве клиента PPPoE, компьютеры локальной сети видят только Ethernet и не знают о PPPoE. Это облегчает работу администратора, избавляя его от необходимости настройки клиентов PPPoE на отдельных компьютерах.

Рис. 185 Модем в качестве клиента PPPoE

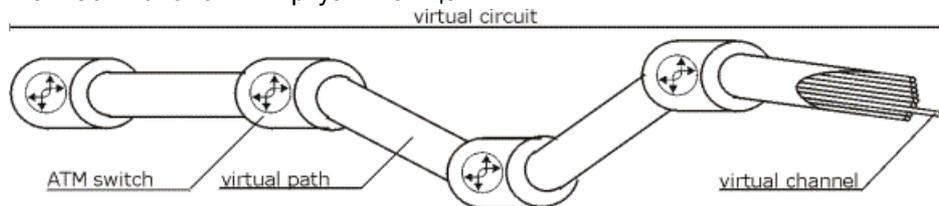
Приложение Е

Топология виртуальной цепи

АТМ представляет собой технологию, ориентированную на соединение, что означает создание виртуальных цепей, по которым осуществляется связь между оконечными системами. Для виртуальных цепей используется следующая терминология:

- Виртуальный канал (VC - Virtual Channel) - логические соединения между коммутаторами АТМ
- Виртуальный путь (VP - Virtual Path) - набор виртуальных каналов
- Виртуальная цепь - ряд виртуальных путей между конечными точками в сети

Рис. 186 Топология виртуальной цепи



Представьте себе, что виртуальный путь - это кабель, состоящий из нескольких проводов. Кабель связывает две точки, при этом провода внутри кабеля обеспечивают отдельные соединения между этими двумя точками. В заголовке ячейки АТМ, VPI (Virtual Path Identifier - Идентификатор виртуального пути) идентифицирует канал связи, образованный виртуальным путем, VCI (Virtual Channel Identifier - Идентификатор виртуального канала) идентифицирует канал внутри виртуального пути.

VPI и VCI идентифицируют виртуальный путь, то есть конечные точки между коммутаторами АТМ. Ряд виртуальных путей образует виртуальную цепь.

Номера VPI/VCI предоставляются Интернет-провайдером.

Приложение F

Интерпретатор команд

Ниже приводятся инструкции по работе с интерпретатором команд. В Главном меню введите "24" для перехода в меню обслуживания системы. Затем введите "8" для перехода в **Меню 24.8 - Режим интерпретатора команд**. Более подробная информация по этим командам находится на компакт-диске, входящем в комплект поставки и на веб-сайте www.zyxel.ru.



ПРИМЕЧАНИЕ: Использование команд, не описанных в документации, или неправильная настройка могут нарушить работу устройства и даже привести к невозможности его использования.

Синтаксис команд

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

Например:

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

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

Использование команд

Список доступных команд отображается с помощью введения команды `help` или `?` в командной строке. Команду необходимо всегда печатать полностью. После завершения работы введите `exit` для возврата в Главное меню SMT.

Приложение G

Описание регистрационных журналов

В этом приложении описывается пример записей в регистрационном журнале.

Табл. 97 Сообщения по обслуживанию системы

СООБЩЕНИЕ	ОПИСАНИЕ
Time calibration is successful	Маршрутизатор синхронизировал свое время на базе информации, полученной от сервера времени.
Time calibration failed	При синхронизации времени маршрутизатора с сервером времени произошел сбой.
WAN interface gets IP: %s	Интерфейсу WAN назначен новый IP-адрес от сервера DHCP, PPPoE, PPTP или удаленного сервера.
DHCP client IP expired	Время аренды IP-адреса клиента DHCP истекло.
DHCP server assigns %s	Сервер DHCP назначил клиенту IP-адрес.
Successful SMT login	Успешный вход в систему через интерфейс SMT.
SMT login failed	Произошел сбой при входе в систему через интерфейс SMT маршрутизатора.
Successful WEB login	Успешный вход в систему через интерфейс Web-конфигуратора.
WEB login failed	Произошел сбой при входе в систему через интерфейс Web-конфигуратора.
Successful TELNET login	Успешный вход в систему по telnet.
TELNET login failed	Произошел сбой при входе в систему по telnet.
Successful FTP login	Успешный вход в систему по ftp.
FTP login failed	Произошел сбой при входе в систему по ftp.
NAT Session Table is Full!	Достигнуто максимальное число записей в таблице NAT и таблица заполнена.
Starting Connectivity Monitor	Запуск Диспетчера соединений.
Time initialized by Daytime Server	Маршрутизатор получил время и дату от сервера даты и времени.
Time initialized by Time server	Маршрутизатор получил время и дату от сервера времени.
Time initialized by NTP server	Маршрутизатор получил время и дату от сервера NTP.
Connect to Daytime server fail	Произошел сбой при подключении маршрутизатора к серверу даты и времени.
Connect to Time server fail	Произошел сбой при подключении маршрутизатора к серверу времени.
Connect to NTP server fail	Произошел сбой при подключении маршрутизатора к серверу NTP.
Too large ICMP packet has been dropped	Маршрутизатор сбросил пакет ICMP, размер которого превышал допустимый.

Табл. 97 Сообщения по обслуживанию системы (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
SMT Session Begin	Начался сеанс управления SMT.
SMT Session End	Закончился сеанс управления SMT.

Табл. 98 Записи системных ошибок

СООБЩЕНИЕ	ОПИСАНИЕ
%s exceeds the max. number of session per host!	Произведена попытка создания сеанса NAT, которая превышает максимальное число записей в таблице сеансов NAT, допустимых для одного узла.
setNetBIOSFilter: calloc error	Произошел сбой при выделении памяти маршрутизатора для параметров фильтра NetBIOS.
readNetBIOSFilter: calloc error	Произошел сбой при выделении памяти маршрутизатора для параметров фильтра NetBIOS.
WAN connection is down.	Подключение к глобальной сети не работает. Доступ в сеть через этот интерфейс отсутствует.

Табл. 99 Записи фильтра пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
[TCP UDP ICMP IGMP Generic] packet filter matched (set: %d, rule: %d)	Произведена попытка доступа, которая соответствует настроенному правилу фильтра (указывается номер набора и номер правила) и выполнена блокировка или пересылка пакета в соответствии с правилом.

Табл. 100 Записи ICMP

СООБЩЕНИЕ	ОПИСАНИЕ
Packet without a NAT table entry blocked: ICMP	Маршрутизатор заблокировал пакет, для которого нет соответствующей записи в таблице NAT.
Router reply ICMP packet: ICMP	Маршрутизатор послал ответный пакет ICMP отправителю.

Табл. 101 Записи CDR

СООБЩЕНИЕ	ОПИСАНИЕ
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	Маршрутизатор получил запрос на установление соединения для выполнения вызова. "call" - номер вызова. "dev" - тип устройства (3 - коммутируемое соединение, 6 - PPPoE, 10 - PPTP). "channel" или "ch" - идентификатор канала вызова. Например, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 " означает, что маршрутизатор выполнял вызов сервера PPPoE 3 раза.
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	Установлено PPPoE, PPTP или коммутируемое соединение.
board %d line %d channel %d, call %d, %s C02 Call Terminated	Завершено PPPoE, PPTP или коммутируемое соединение.

Табл. 102 Записи PPP

СООБЩЕНИЕ	ОПИСАНИЕ
ppp:LCP Starting	Запущена стадия протокола управления каналом связи для PPP соединения.
ppp:LCP Opening	Открывается стадия протокола управления каналом связи для PPP соединения.
ppp:CHAP Opening	Открывается стадия протокола аутентификации по методу "вызов-рукопожатие" (Challenge Handshake Authentication) для PPP соединения.
ppp:IPCP Starting	Начинается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.
ppp:IPCP Opening	Открывается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.
ppp:LCP Closing	Открывается стадия протокола управления каналом связи (Link Control Protocol) для PPP соединения.
ppp:IPCP Closing	Закрывается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.

Табл. 103 Записи ICMP

ТИП	КОД	ОПИСАНИЕ
0		Эхо-ответ
	0	Сообщение с эхо-ответом
3		Адресат недоступен
	0	Сеть недоступна
	1	Узел недоступен

Табл. 103 Записи ICMP (продолжение)

ТИП	КОД	ОПИСАНИЕ
	2	Протокол недоступен
	3	Порт недоступен
	4	Пакет, который требует фрагментации, отброшен, так как имеет параметр DF (Don't Fragment - не фрагментировать)
	5	Ошибка в маршруте источника
4		Источник произвел сброс
	0	Шлюз может сбросить дейтаграммы Интернет, если он не имеет буферной памяти, достаточной для организации очереди дейтаграмм, чтобы передать их в следующую сеть по маршруту к сети получателя.
5		Перенаправление
	0	Перенаправление дейтаграмм для сети
	1	Перенаправление дейтаграмм для узла
	2	Перенаправление дейтаграмм для типа услуги и сети
	3	Перенаправление дейтаграмм для типа услуги и узла
8		Эхо
	0	Эхо-сообщение
11		Время истекло
	0	Время жизни пакета истекло в пути
	1	Время на повторную сборку фрагментов истекло
12		Неверный параметр
	0	Указатель показывает на ошибку
13		Временная метка
	0	Сообщение-запрос временной метки
14		Ответ с временной меткой
	0	Ответное сообщение с временной меткой
15		Запрос параметров
	0	Сообщение с запросом о параметрах
16		Ответ на запрос параметров
	0	Сообщение с ответом на запрос параметров

Табл. 104 Записи системного журнала

СООБЩЕНИЕ	ОПИСАНИЕ
<pre><Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category></pre>	<p>"Это сообщение посылается системой ("RAS" отображается в качестве системного имени, если оно не было присвоено), когда маршрутизатор генерирует запись в системном журнале. Эта функция устанавливается на странице: ГЛАВНОЕ МЕНЮ Web-конфигуратора->ЖУРНАЛЫ РЕГИСТРАЦИИ->Параметры журналов. Серьезность ошибки - это класс записи в системном журнале. Описание сообщений и записей определяются различными схемами записей в этом приложении. "devID" - это последние три символа MAC-адреса порта LAN маршрутизатора. "cat" - то же, что и категория в журналах маршрутизатора.</p>

В следующей таблице приводятся типы данных сообщений протокола ISAKMP (см. RFC-2408), и их обозначения в журнале. Более подробную информацию по каждому типу см. в RFC.

Табл. 105 Типы данных сообщений RFC-2408 ISAKMP

ОБОЗНАЧЕНИЕ В ЖУРНАЛЕ	ТИП ДАННЫХ
SA	Безопасное соединение
PROP	Предложение
TRANS	Преобразование
KE	Обмен ключами
ID	Идентификация
CER	Сертификат
CER_REQ	Запрос сертификата
HASH	Хеш
SIG	Подпись
NONCE	Сл. число
NOTFY	Уведомление
DEL	Удалить
VID	Идентификационный номер поставщика