Серия OMNI ADSL LAN

Маршрутизатор ADSL

Руководство пользователя

Версия 3.40

Сентябрь 2003

Авторское право

Непризнание иска

ZyXEL не принимает на себя ни в какой форме ответственность за применение или использование любого изделия, или программного обеспечения, описанного здесь. Также она никоим образом не передает лицензию на свои патентные права и патентные права других собственников. Кроме того, корпорация ZyXEL сохраняет право вносить изменения в любые описанные здесь изделия без уведомления. Информация в этом руководстве также может быть изменена без специального уведомления.

Товарные знаки

ZyNOS (Сетевая операционная система ZyXEL) является зарегистрированным товарным знаком ZyXEL Communications Inc. Использование других торговых знаков в этом издании носит сугубо информационный характер. Данные торговые знаки могут являться собственностью соответствующих владельцев.

Заключение FCC по помехам

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

- Данное устройство не может быть причиной недопустимых помех.
- Данное устройство может быть подвержено воздействию помех, включая помехи, которые могут вызвать нежелательные действия.

Данное оборудование было протестировано и признано соответствующим ограничениям, существующим для Класса B цифровых приборов согласно Части 15 Правил FCC. Данные ограничения разработаны для обеспечения разумной защиты против недопустимых помех при коммерческом использовании. Данное устройство генерирует, использует и может быть источником высокочастотного излучения, и если оно не будет устанавливаться и использоваться в соответствии с инструкциями, то может стать причиной недопустимых помех при радиосвязи.

Если данное устройство является причиной недопустимых помех при приеме теле/радиопередач, что можно определить путем выключения и включения устройства, то пользователь может попробовать скорректировать помехи одной или несколькими из нижеследующих мер:

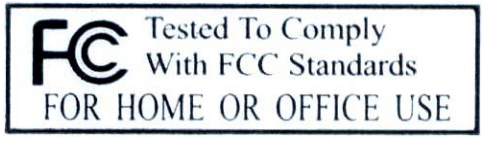
1. Переориентировать или переместить принимающую антенну.
2. Увеличить расстояние или защитную перегородку между оборудованием и принимающим устройством.
3. Подключить это оборудование к розетке контура, в который принимающее устройство не включено.
4. Обратиться за помощью к поставщику или опытному теле- или радиотехнику.

Уведомление 1

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

Сертификация

Более подробную информацию о продукте можно найти корпоративном сайте компании www.zyxel.com.



Ограниченные гарантийные обязательства корпорации ZyXEL

Корпорация ZyXEL гарантирует легальному конечному пользователю (покупателю), что данное изделие не имеет и в течение периода до двух лет со дня покупки не будет иметь дефектов, связанных с использованными материалами и производственным браком. В течение гарантийного периода и по подтверждении покупки, если изделие имеет признаки неисправности за счет производственного брака и/или использованных материалов, корпорация ZyXEL будет, по своему выбору, ремонтировать или заменять дефектные изделия или комплектующие без оплаты деталей или стоимости работы, и за все то, что будет полагать необходимым для восстановления надлежащего режима работы изделий или комплектующих. Любая замена будет включать как новые, так и восстановленные функционально эквивалентные составляющие аналогичной стоимости; выбор в данном случае за корпорацией ZyXEL. Данные гарантийные обязательства неприменимы в случае, если изделие модифицировано, неправильно употребляется, было вскрыто, повреждено вследствие форс-мажорных обстоятельств или неправильных условий эксплуатации.

Примечание

Покупатель, согласно данным гарантийным обязательствам, может выбрать только ремонт или замену. Данные гарантийные обязательства даны вместо всех прочих гарантийных обязательств, явных или неявных, включая любые неявные гарантийные обязательства годности для продажи или пригодности для использования для конкретных целей и задач. Корпорация ZyXEL не будет нести материальной ответственности перед покупателем за косвенный ущерб любого вида.

Для получения обслуживания по данным гарантийным обязательствам следует связаться с Сервисным центром ZyXEL; информация о номере разрешения на возврат (НРВ) содержится в Гарантийном талоне на данное оборудование. Изделия должны быть возвращены с предварительно оплаченным почтовым сбором. Рекомендуется застраховать каждое устройство на период пересылки. Любые возвращенные изделия без подтверждения факта покупки или с просроченной гарантией будут отремонтированы или заменены (по усмотрению корпорации ZyXEL), и клиенту будет выслан счет за работу и детали. Все отремонтированные или замененные изделия будут отправлены корпорацией ZyXEL по соответствующему обратному адресу с оплаченным почтовым сбором. Данные гарантийные обязательства предоставляют определенные законом права, а, кроме того, дополнительные права, которые могут быть различными в разных государствах.

Меры предосторожности

1. Для уменьшения риска возникновения пожара пользуйтесь только проводами AWG № 26 (американской системы калибровки проводов) или телефонными проводами большего сечения.

2. Запрещается пользоваться данным устройством вблизи воды, например, в сырых подвалах или рядом с плавательными бассейнами.

3. Не рекомендуется пользоваться данным устройством в грозу. Следует опасаться возможности поражения разрядом молнии.

Сервисная служба

При обращении в Сервисную службу будьте готовы предоставить следующую информацию:

- Модель изделия и серийный номер.
- Гарантия.
- Дата приобретения устройства.
- Краткое описание возникшей проблемы, а также, какие были предприняты действия по ее устранению.

СПОСОБ / МЕСТОНАХОЖДЕНИЕ	E-MAIL СЛУЖБА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ/ОТДЕЛ ПРОДАЖ	ТЕЛЕФОН/ФАКС	WEB-САЙТ/FTP-САЙТ	ОБЫЧНАЯ ПОЧТА
ПО ВСЕМУ МИРУ	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, Taiwan 300, R.O.C.
СЕВЕРНАЯ АМЕРИКА	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0858	www.us.zyxel.com ftp.zyxel.com	
СКАНДИНАВИЯ	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
ГЕРМАНИЯ	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

Содержание

Предисловие

Поздравляем Вас с приобретением маршрутизатора серии OMNI ADSL LAN.

OMNI ADSL легко инсталлируется и конфигурируется. Для задания конфигурации маршрутизатора OMNI ADSL воспользуйтесь средствами Web-конфигуратора, системного терминала управления (SMT) или интерфейса интерпретатора команд . Не все интерфейсы обеспечивают задание всех характеристик.

Не забудьте зарегистрировать маршрутизатор OMNI ADSL в режиме on-line на сайте компании www.zyxel.com для бесплатной подписки на получение информации и обновление программного обеспечения.

О данном Руководстве пользователя

Данное руководство предназначено для ознакомления с конфигурацией маршрутизатора OMNI ADSL при различных вариантах его использования. Разделы данного руководства, посвященные описанию Web-конфигуратора, содержат необходимую информацию о технических параметрах, задаваемых с его помощью. Разделы данного руководства, посвященные описанию системной консоли SMT, содержат необходимую информацию о параметрах конфигурации, которые не могут быть заданы с помощью Web-конфигуратора.

Сопроводительная документация

- Справочный компакт-диск

  См. документацию по техническому обслуживанию, находящуюся на CD, входящем в комплект поставки.

- Краткое руководство или ознакомительный курс

  Маршрутизаторы OMNI ADSL LAN H, OMNI ADSL LAN HW и OMNI ADSL LAN H-E поставляются с Кратким руководством. К моделям устройства OMNI ADSL LAN R и OMNI ADSL LAN R-E прилагается ознакомительный курс. Оба документа должны помочь вам быстро разобраться в устройстве маршрутизатора и приступить к его эксплуатации. В них содержится информация о подключении и указания о порядке начала работы. В кратком руководстве содержится дополнительная информация о мастер-программе и основных параметрах конфигурации устройства.

- Web-конфигуратор: помощь on-line
  Встроенные функции подсказки по дескрипторам отдельных экранов и доступ к дополнительной информации.

- Глоссарий ZyXEL и web-сайт
  См. сайт компании www.zyxel.com для доступа в режиме on-line к Глоссарию по терминологии вычислительных сетей и дополнительной технической документации..

Условные обозначения

- Опция “Enter”("Ввод") означает необходимость набора одного или более символов. Опция "Select“ или “Choose” ("Выбор") означает, что вам следует выбрать одну из предложенных опций.
- Заголовки и надписи меню SMT выполнены **полужирным шрифтом Times New Roman**. Определенные пункты меню выполнены **полужирным шрифтом Arial**. Названия команд и клавиш со стрелками заключены в квадратные скобки. [ENTER] обозначает клавишу "Enter" или клавишу возврата каретки. [ESC] обозначает клавишу Escape, а [SPACE BAR] обозначает клавишу пробела.
- Для описания последовательности выполнения операций при работе с мышью применяется выделение кавычками. Например, запись: “щелкните по иконке Apple, **панель управления,** а затем **модем**” означает, что вначале вы должны щелкнуть по иконке Apple, затем перевести курсор к папке **панель управления**, а затем щелкнуть по иконке**модем**.
- Для краткости в данном руководстве будут использоваться следующие сокращения "напр." вместо "например" и "т. е." вместо "то есть" и "другими словами".
- Далее в данном Руководстве продукты серии OMNI ADSL LAN могут обозначаться просто как OMNI ADSL. Это относится к обеим моделям ADSL, работающим в обычных телефонных сетях и в цифровых сетях ISDN, за исключением специально оговоренных случаев.
- К моделям OMNI ADSL с возможностями беспроводной связи относятся модели OMNI ADSL LAN H/HW.

В следующем разделе приводится необходимая информация о цифровых абонентских линиях DSL. Пропустите его и обращайтесь непосредственно к *Главе 1*, если вы хотите немедленно приступить к работе с маршрутизатором.

Руководство пользователя: обратная связь

Помогая нам, вы помогаете себе. Посылайте свои комментарии относительно содержания Руководства пользователя, вопросы и предложения по его улучшению электронной почтой по адресу: techwriters@zyxel.com.tw или обычной почтой в Группу технической документации по адресу: The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Спасибо.

Введение в DSL (цифровые абонентские линии)

Технология DSL (Digital Subscriber Line/Цифровая абонентская линия) улучшает производительность передачи данных по существующим проводам "витая пара", которые соединяют местные телефонные компании с большинством домашних и офисных телефонов. В то время как сам кабель может работать при более высоких частотах, переключающие устройства предназначены для блокировки сигналов частотой выше 4000 Гц с целью фильтрации помех на линии голосовой связи. Однако в настоящий момент идет активный поиск способа увеличения пропускной способности для облегчения доступа в сеть - а значит, технологий DSL.

Существует семь типов DSL-обслуживания в зависимости от скорости (от 16 кбит/с до 52 Мбит/с). Обслуживание либо симметричное (одинаковая скорость в обоих направлениях), либо асимметричное (объем входящего потока превышает объем исходящего потока). Ассиметричные услуги (ADSL) подходят, прежде всего, для пользователей Интернета, так как обычно больше информации загружается, чем выгружается. Например, простым нажатием кнопки в Web-браузере можно инициировать расширенный вариант загрузки, включающий графику и текст.

При возрастании скорости передачи данных, уменьшается расстояние, на которое передача может осуществляться. Это означает, что пользователи, которые находятся на определенном расстоянии от центральной телефонной станции, не смогут работать на высокой скорости.

Соединение DSL представляет собой двухточечный выделенный канал, что означает, что связь всегда установлена и вызов не требуется.

Что представляет собой ADSL?

ASDL представляет собой асимметричную технологию, что означает, что скорость исходящего потока данных намного больше, чем скорость входящего. Как уже было сказано, она прекрасно подходит для обычных сеансов связи в Интернете, при которых больше информации выгружается, например, с web-серверов, чем загружается. ADSL работает в более высоком диапазоне частот, чем диапазон частот голосовых услуг, поэтому обе системы могут пользоваться одним кабелем.

Part I:

Начало работы

Структура этого раздела организована как руководство для последовательного (пошагового) обучения, максимально облегчающее освоение маршрутизатора OMNI ADSL. Приводится описание основных функций и возможностей устройства, включая Web-конфигуратор, процедуры установки пароля и настройки экрана мастер-программы при первоначальной настройке маршрутизатора.

Chapter 1
Знакомство с OMNI ADSL

В настоящей главе описываются основные функции и способы применения OMNI ADSL.

1.1 Введение в серии OMNI ADSL LAN

OMNI ADSL конструктивно объединяет высокоскоростной (10/100 Мбит/с) автоматически согласующийся интерфейс ЛВС и высокоскоростной порт ADSL. OMNI ADSL отлично подходит для быстрой работы в Интернете и соединения локальных сетей с удаленными сетями. Благодаря интеграции DSL и NAT, в устройстве OMNI ADSL обеспечивается исключительно высокая скорость многопользовательского доступа в Интернет при минимальных расходах.

Модели OMNI ADSL LAN R и OMNI ADSL LAN R-E являются маршрутизаторами и представлены двумя моделями, предназначенными для работы в ассиметричных цифровых абонентских линий (ADSL), в обычных телефонных сетях (ROTS) и в цифровых сетях ISDN.

В состав маршрутизаторов OMNI ADSL LAN H и OMNI ADSL LAN HW входит четырехпортовый коммутатор со встроенной картой-слотом беспроводной связи PCMCIA. Маршрутизатор OMNI ADSL LAN H/HW поддерживает возможность беспроводного подключения к локальной вычислительной сети, позволяя пользователям насладиться оперативностью и комфортом такого сервиса в любом месте в пределах зоны охвата. OMNI ADSL LAN HW содержит карту беспроводной связи локальной вычислительной сети, отсутствующую у OMNI ADSL LAN H.

Устройство OMNI ADSL LAN H-E является маршрутизатором ADSL с четырьмя высокоскоростными портами ЛВС Ethernet с автоматическим определением и переключением скорости 10/100Base-T и высокоскоростным портом ADSL.

Пользуйтесь только специальным микропрограммным обеспечением, предназначенным для вашей модели маршрутизатора OMNI ADSL. См. предупредительную наклейку в нижней части устройства OMNI ADSL.

Графический интерфейса пользователя, работающий по принципу Web-браузера, обеспечивает удобное управление и полностью независим от операционной системы платформы, которую вы используете.

1.2 Характеристики OMNI ADSL

В следующих разделах приводится описание характеристик маршрутизаторов серии OMNI ADSL, имеющих отличия для разных моделей устройства. В данной таблице приведены только основные характеристики маршрутизаторов серии OMNI ADSL. Для получения более подробной информации см. приведенные ниже технические характеристики.

Технические характеристики разных моделей могут иметь отличия. Для получения информации о характеристиках, соответствующих Вашей модели OMNI ADSL, см. табл. *Технические характеристики моделей*.

Табл. 1-1 Технические характеристики моделей

МОДЕЛЬ OMNI ADSL / ХАРАКТЕРИСТИКИ	P650R	P650R-E	P650H/HW	P650H-E
Слот беспроводной связи			O	
Четырехпортовый коммутатор			O	O
Консольный порт	O		O	
Интерфейс ЛВС Ethernet с автоматическим переключением скорости потока данных 10/100 Мбит/с	O	O	O	O
Кнопка перезапуска	O	O	O	O
Выключатель питания	O	O	O	O
Стандарт сетевой безопасности IEEE 802.1x			O	
Перенаправление трафика	O		O	O
Межсетевой экран			O	O
Контент-фильтр			O	
VPN			O	
Управление пропускной способностью			O	
Маршрутизация на базе стратегии IP	O	O	O	O
Автоматическое распознавание и настройка периферийных устройств (UPnP)	O	O	O	O

Табл. 1-1 Технические характеристики моделей

МОДЕЛЬ OMNI ADSL / ХАРАКТЕРИСТИКИ	P650R	P650R-E	P650H/HW	P650H-E
Дистанционное управление	O		O	O
Централизованная регистрация сообщений				O

Условные обозначения: Символ “O” в столбце соответствующей модели обозначает наличие данной характеристики. Вместо него в таблице может быть приведено числовое значение характеристики, соответствующие конкретной модели. Информация, содержащаяся в данной таблице, достоверна на момент публикации, но может быть изменена без предварительного уведомления.

➢ Четырехпортовый коммутатор

Комбинация коммутатора и маршрутизатора придает модели OMNI ADSL черты экономически рационального и эффективного сетевого решения. К портам ЛВС маршрутизатора OMNI ADSL возможно подключение до четырех компьютеров без расходов на приобретение дополнительных концентраторов.

➢ Высокоскоростной доступ в Интернет

Маршрутизатор OMNI ADSL способен поддерживать скорость приема данных до 8 Мбит/с и скорость передачи данных 832 кбит/с. В устройстве OMNI для ADSL через обычную телефонную сеть также реализована возможность управления скоростью передачи данных.

➢ Стандарт IEEE 802.11b беспроводной ЛВС со скоростью передачи данных 11 Мбит/с

Беспроводная ЛВС со скоростью передачи данных 11 Мбит/с обеспечивает возможность создания мобильной и высокоскоростной сетевой среды для небольших и домашних офисов. Компьютеры, оборудованные адаптерами беспроводной ЛВС Ethernet, могут быть подключены к локальной вычислительной сети без каких-либо дополнительных проводов, при этом вы получите настоящее удовольствие от возможности доступа к высокоскоростным каналам. Данная функция имеется не во всех моделях.

➢ Поддержка протокола PPPoE (RFC2516)

PPPoE (Протокол "точка-точка" через Ethernet) эмулирует коммутируемое соединение. Это позволяет Интернет-провайдеру использовать возможности существующей сетевой конфигурации в сочетании с новейшими технологическими решениями, позволяющими увеличить полосу пропускания, такими как технология ADSL. Драйвер PPPoE в устройстве OMNI ADSL является "прозрачным" для любого

компьютера локальной сети, который "видит" только Ethernet и не распознают PPPoE, тем самым исключая необходимость управления клиентами PPPoE на отдельных компьютерах.

➢ IEEE 802.1x - стандарт сетевой безопасности

Маршрутизатор OMNI ADSL поддерживает стандарт сетевой безопасности IEEE 802.1x, повышающий надежность аутентификации пользователей. В маршрутизаторе имеется встроенная база данных, поддерживающая аутентификацию до 32 пользователей сети с помощью хэш-процедуры криптографической защиты MD5. В устройстве применяется EAP-совместимый RADIUS-сервер (RFC2138, 2139 - Remote Authentication Dial In User Service - Служба аутентификации удаленных пользователей по коммутируемым каналам связи) для аутентификации неограниченного числа абонентов сети, пользующихся протоколом EAP (Extensible Authentication Protocol - Расширенный протоколом аутентификации). EAP является протоколом аутентификации, поддерживающим различные способы аутентификации пользователей.

➢ Трансляция сетевых адресов (NAT)

Процедура трансляции сетевых адресов (NAT) позволяет осуществлять преобразование IP-адреса, использующегося внутри одной сети (например, частный IP-адрес локальной сети), в IP-адрес, известный пользователям другой сети (например, общедоступный IP-адрес глобальной сети Internet).

➢ Перенаправление трафика

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

➢ Межсетевой экран

В OMNI ADSL применяется сетевой экран (брандмауэр) с инспекцией пакетов с учетом состояния и с защитой от атак типа DoS (отказ от обслуживания). По умолчанию, если брандмауэр включен, весь входящий трафик, поступающий из глобальной сети в ЛВС, автоматически блокируется до получения специального разрешения из локальной сети. Межсетевой экран устройства OMNI ADSL поддерживает инспекцию протоколов TCP/UDP, обнаружение и предупреждение атак DoS, выдачу предупреждений в реальном масштабе времени, подготовку отчетов и ведение журналов.

➢ Функция IPSec VPN

Позволяет создать виртуальную частную сеть (VPN) для связи с деловыми партнерами и филиалами путем использования и шифрования данных для обеспечения надежной связи без затрат на выделенные линии между сайтами. Маршрутизатор OMNI ADSL VPN построен на основе стандарта IPSec и обладает полной совместимостью с другими виртуальными частными сетями (VPN), поддерживающими этот стандарт.

➢ Управление пропускной способностью

Управление пропускной способностью позволяет вам распределить сетевые ресурсы в соответствии с выбранной стратегией. Такая стратегия, основанная на возможностях распределения ресурсов пропускной способности, обеспечивает повышение эффективности реализации сетевых приложений реального времени, таких как межсетевой протокол передачи речевых сообщений (VoIP).

➢ Автоматическая настройка и подключение периферийных устройств (UPnP)

Маршрутизатор OMNI ADSL и другие устройства, поддерживающие протоколы TCP/IP и UPnP, могут быть динамично объединены в одну сеть с присвоением IP-адресов, что открывает доступ к их ресурсам для других абонентов сети.

➢ Интерфейс 10/100MB Ethernet/Fast Ethernet с автоматическим выбором скорости

Данная функция автоматического выбора скорости позволяет маршрутизатору OMNI ADSL определить скорость входящего потока данных и автоматически произвести соответствующую настройку без участия оператора. При этом обеспечивается передача данных со скоростью 10 Мбит/с или 100 Мбит/с в полудуплексном или дуплексном режиме, в зависимости от параметров сети Ethernet.

➢ Поддержка динамических DNS

Поддержка динамических DNS позволяет иметь статический псевдоним хоста для динамического распределения IP-адресов, что делает хост более легкодоступным из разных частей Интернет. Для доступа к данному виду сервиса необходимо пройти регистрацию и получить динамический адрес клиента DNS.

➢ Поддержка множества PVC (Permanent Virtual Circuits/Постоянные виртуальные каналы)

Маршрутизатор OMNI ADSL поддерживает до 8 постоянных виртуальных каналов (PVC).

➢ Стандарты ADSL

- Режим полной скорости (ANSI T1.413, Issue 2; G.dmt (G.992.1) с поддержкой скорости передачи данных в линии до 8 Мбит/с на прием и 832 кбит/с на передачу.
- G.lite (G.992.2), поддерживающий скорость передачи данных до 1,5 Мбит/с на прием и 512 кбит/с на передачу.
- Поддерживает многорежимный стандарт (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.994.1 и .996.1 (только для цифровых сетей ISDN); G.991.1;G.lite (G992.2)).

- Поддерживает функции тестирования F4/F5 методом обратной передачи данных, ячейки AIS и RDI OAM.
- ATM PVC Forum UNI 3.1/4.0
- Поддерживает до 8 постоянных виртуальных каналов (UBR, CBR, VBR).
- Множественные протоколы через AAL5 (RFC 1483)
- Протоколы PPP через AAL5 (RFC 2364).
- Протоколы PPP через Ethernet (RFC 2516).

➢ Поддержка DHCP

DHCP (Dynamic Host Configuration Protocol/Протокол динамического конфигурирования хост-машины) позволяет отдельным клиентам компьютерам сети получать конфигурацию TCP/IP при загрузке с центрального сервера DHCP. OMNI ADSL оснащен встроенным сервером DHCP, по умолчанию являющимся активным. Он может присвоить клиентам DHCP IP-адреса, IP шлюз по умолчанию и серверов DNS. Кроме того, OMNI ADSL может выступать в качестве фиктивного сервера DHCP (ретранслятора DHCP), ретранслируя клиентам назначенные IP-адреса от настоящего сервера DHCP.

➢ Псевдоним IP

Псевдоним IP позволяет разделить физическую сеть на основе одного интерфейса Ethernet на несколько логических сетей. OMNI ADSL поддерживает три логических интерфейса ЛВС через отдельный физический интерфейс Ethernet, при этом сам OMNI ADSL выступает в качестве шлюза для каждой ЛВС.

➢ Маршрутизация на базе стратегии IP (IPPR)

Как правило, маршрутизация основывается только на адресе назначения, поэтому маршрутизатор выбирает самый короткий путь для пересылки пакета. Маршрутизация на базе стратегии IP (IPPR) предоставляет возможность игнорировать схему маршрутизации, заданную по умолчанию, и изменить процесс пересылки пакета на базе стратегии, определенной сетевым администратором.

➢ Поддержка протоколов

- PPP (Point-to-Point Protocol/Протокол “точка-точка”) - протокол канального уровня.
  - Протоколы PPP через PAP (RFC 1334).
  - Протоколы PPP через CHAP (RFC 1994).
- TCP/IP (Протокол управления передачей/Межсетевой протокол) - протокол сетевого уровня.
- Прозрачная передача по мосту для неподдерживаемых протоколов сетевого уровня.

- RIP I/RIP II
- IGMP Proxy
- Поддержка ICMP
- Поддержка MIB II (RFC 1213)
- Функции протокола PPPoE
  - Контроль превышения времени ожидания
  - Набор по требованию

➢ Сетевая совместимость

Маршрутизатор OMNI ADSL совместим с большинством концентраторов ассиметричных цифровых абонентских линий (ADSL DSLAM), используемых провайдерами..

➢ Мультиплексирование

OMNI ADSL поддерживает мультиплексирование на базе VC и LLC.

➢ Инкапсуляция

Маршрутизаторы серии OMNI ADSL R поддерживают протокол PPPoA (RFC 2364 - PPP через уровень 5 адаптации ATM), инкапсуляцию (RFC 1483) через ATM, маршрутизацию с инкапсуляцией MAC (ENET ENCAP), а также PPP через Ethernet (RFC 2516).

➢ Сетевое управление

- Управление SMT (System Management Terminal/Системный терминал), основанное на системе меню
- Встроенный Web-конфигуратор
- CLI (Command Line Interpreter/Интерпретатор командной строки)
- Удаленный сеанс SMT через Telnet
- Возможность управления по протоколу SNMP
- Локальный сеанс SMT через консольный порт
- Сервер/Клиент DHCP
- Встроенные средства диагностики
- Системный журнал

- Сервер TFTP/FTP, обновление микропрограммного обеспечения, поддержка и восстановление конфигурации

➢ **Возможности диагностики**

- OMNI ADSL может выполнять различные тесты самодиагностики, предназначенные для проверки целостности следующих цепей:
  - Флэш-память
  - Цепь ADSL
  - ОЗУ
  - Порт локальной сети

➢ **Фильтры**

Функция фильтрации пакетов OMNI ADSL позволяет улучшить защиту и управление сетью.

➢ **Простота установки**

OMNI ADSL разработан таким образом, чтобы его установка была быстрой, простой и интуитивно-понятной.

➢ **Корпус**

Заключенный в новый компактный вентилируемый корпус, OMNI ADSL не занимает много места и легко устанавливается в любом уголке, даже небольшого офиса.

1.3 Область применения маршрутизаторов OMNI ADSL

Ниже приведены примеры, демонстрирующие наиболее подходящие области применения маршрутизаторов OMNI ADSL.

1.3.1 Доступ в Интернет

OMNI ADSL является идеальным решением для получения высокоскоростного доступа в сеть Интернет. OMNI ADSL поддерживает используемый в Интернете протокол TCP/IP. Маршрутизатор OMNI ADSL совместим с аппаратурой большинства провайдеров ADSL, оборудованных концентраторами ассиметричных цифровых абонентских линий (DSLAM). DSLAM представляет собой стойку с линейными картами ADSL, данные с которых мультиплексируются в магистральный сетевой интерфейс/соединение (например: T1, OC3, DS3, ATM или Frame Relay). Подумайте об этом, как о достойной альтернативе модемной стойке для ADSL. Кроме того, в модели OMNI ADSL LAN H/HW вы можете установить дополнительно карту беспроводной связи PCMICA, что открывает

доступ беспроводных станций к ресурсам вашей сети. Типичный пример организации доступа в Интернет приведен ниже.

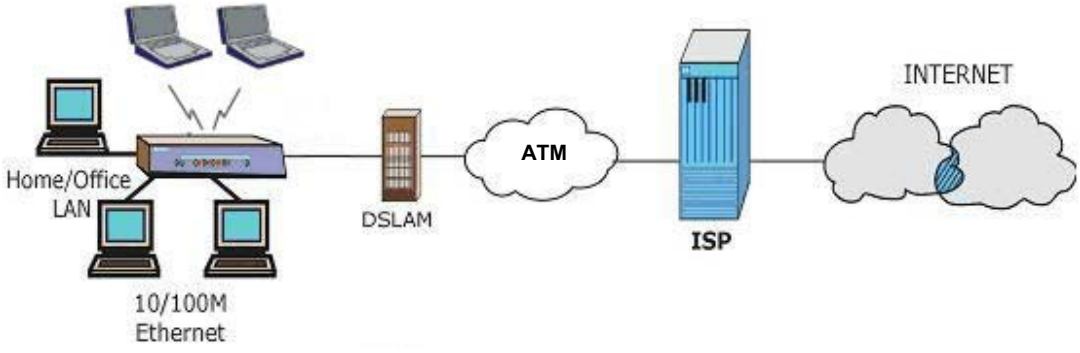


Рис. 1-1 Применение маршрутизатора OMNI ADSL для организации доступа в сеть Интернет

1.3.2 Применение для интеграции локальных сетей

При помощи маршрутизатора OMNI ADSL можно осуществить интеграцию двух удаленных локальных сетей с использованием линии ADSL. Типичный пример организации соединения локальных сетей приведен ниже.

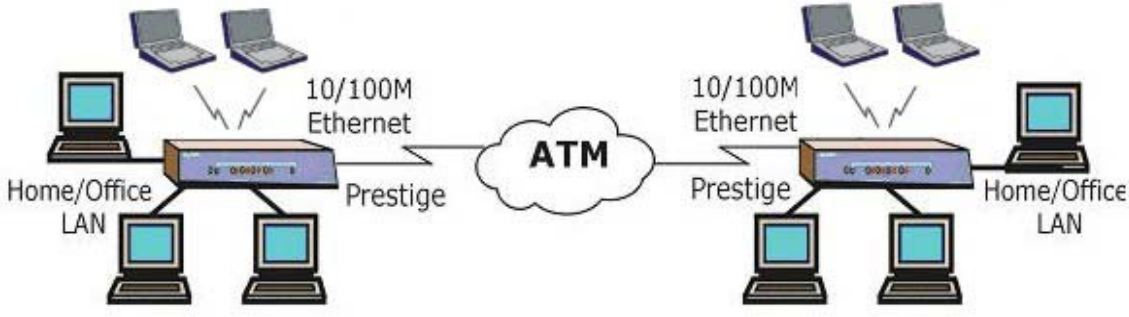


Рис. 1-2 Применение маршрутизатора OMNI ADSL для интеграции локальных вычислительных сетей (LAN-to-LAN)

Chapter 2
Web-конфигуратор: введение

В данной главе излагаются основы работы и настройки Web-конфигуратора.

2.1 Обзор функциональных возможностей Web-конфигуратора

Наличие встроенного Web-конфигуратора позволит, например, управлять работой маршрутизатора OMNI ADSL из любого места с помощью программы-браузера, такой как Microsoft Internet Explorer или Netscape Navigator. Пользуйтесь программами Internet Explorer (версии старше 6.0), Netscape Navigator (версии старше 7.0) с компонентами JavaScript. Рекомендуется установить разрешение экрана на вашем компьютере 1024x768 пикселов

2.2 Ознакомление с Web-конфигуратором маршрутизатора OMNI ADSL

Step 1. Убедитесь в правильности подключения маршрутизатора, пользуясь *Кратким руководством* или *Ознакомительным курсом*.

Step 2. Подготовьте вашу компьютерную сеть для подключения к маршрутизатору OMNI ADSL (см. *Краткий курс* или *Ознакомительный курс*).

Step 3. Запустите Web-браузер.

Step 4. Введите в качестве URL "192.168.1.1".

Step 5. На экране отображается окно **Enter Network Password (Ввести сетевой пароль)** . Наберите имя пользователя (по умолчанию - “admin”), пароль (по умолчанию - “1234”) и щелкните по **OK**.

Рис. 2-1 Окно ввода пароля

Step 6. Должно появиться окно **Карта сайта**.

OMNI ADSL автоматически отключается после пяти минут ожидания. В этом случае, просто повторите загрузку.

2.3 Настройка Web-конфигуратора

Ниже излагаются основы работы с Web-конфигуратором с помощью **Карты сайта**. Окна могут иметь незначительные отличия в разных моделях маршрутизатора OMNI ADSL.

- Выберите язык из раскрывающегося списка **Language (Язык)**.
- Щелкните по **Wizard Setup (Мастер-программа установки)**, открывающей доступ к другим окнам, необходимым для конфигурирования OMNI ADSL при первом запуске.
- Щелкните по ссылке, находящейся под иконкой **Дополнительная настройка** для установки дополнительных параметров настройки маршрутизатора OMNI ADSL.
- Щелкните по ссылке, находящейся под иконкой **Сопровождение** , для ознакомления со статистическими данными о работе маршрутизатора OMNI ADSL, загрузке микропрограммного обеспечения, создании резервной копии, восстановлении или загрузке файла конфигурации.
- Щелкните по **SITE MAP (КАРТА САЙТА)** для перехода к окну **Site Map (Карта сайта)**.
- Щелкните по **Logout (Конец сеанса)** на навигационной панели после окончания сеанса работы с управляющей программой OMNI ADSL.

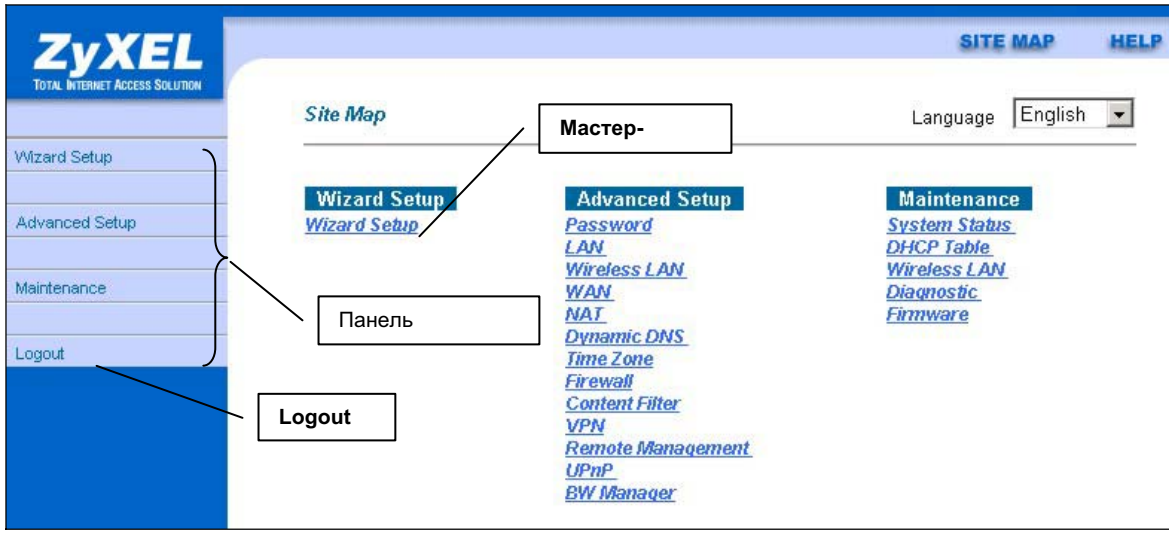


Рис. 2-2 Окно КАРТА САЙТА Web-конфигуратора

Щелкните по иконке HELP, расположенной в верхнем правом углу большинства экранов, для отображения встроенной справочной программы.

2.4 Изменение пароля

Настоятельно рекомендуем сменить пароль доступа к маршрутизатору.

Для изменения пароля доступа к OMNI ADSL щелкните по **Advanced Setup (Дополнительная настройка)**, а затем по **Password (Пароль)**. Появится окно следующего вида.

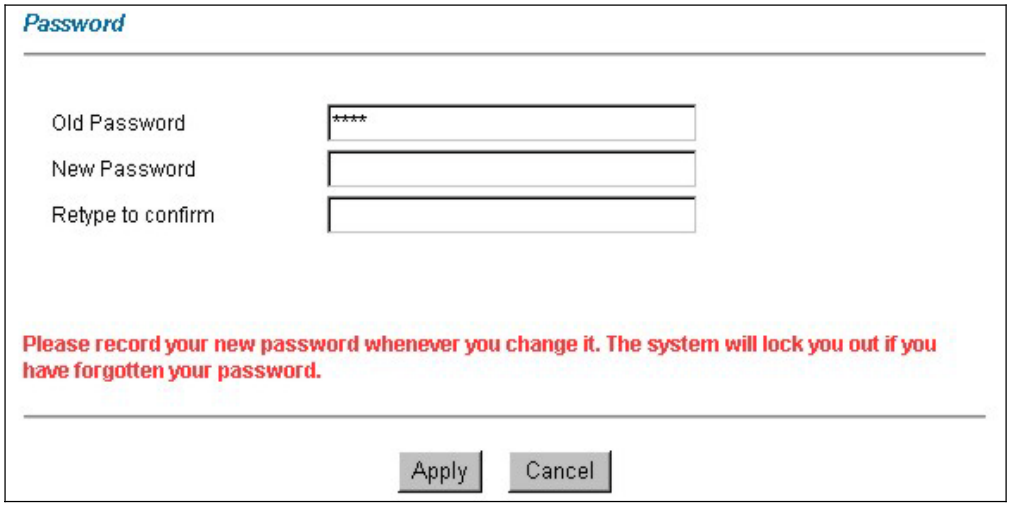


Рис. 2-3 Пароль

В следующей таблице приведены описания полей данного экрана.

Табл. 2-1 Пароль

ПОЛЕ	ОПИСАНИЕ
Old Password	Введите в этом поле существующий пароль (или пароль, заданный по умолчанию), которым вы пользуетесь для доступа к маршрутизатору.
New Password	Введите в этом поле новый пароль.
Retype to Confirm	Еще раз введите в этом поле новый пароль.
Apply	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Cancel	Щелкните по **Cancel (Отмена)** для возобновления работы по конфигурированию данного окна.

2.5 Перезапуск OMNI ADSL

Если вы забыли пароль или не можете получить доступ к маршрутизатору OMNI ADSL, следует загрузить файл конфигурации, поставляемый предприятием-изготовителем, или воспользоваться кнопкой перезапуска **RESET** на задней стороне устройства. При загрузке файла конфигурации, текущий файл конфигурации заменяется на файл конфигурации по умолчанию. Это означает, что вся созданная ранее конфигурация будет потеряна, а скорость консольного порта будет возвращена к

значению по умолчанию 9600 бит/с с 8 битами данных, без контроля четности, с одним стоп-битом и без управления потоком. Пароль доступа будет восстановлен в прежнем значении “1234”.

2.5.1 Использование кнопки перезапуска Reset

Step 1. Убедитесь в том, что светодиод **SYS** LED горит не мигая.

Step 2. Нажмите кнопку перезапуска **RESET**, держите в течение пяти секунд и затем отпустите. Если светодиод **SYS** LED начинает мигать, это означает, что настройки по умолчанию восстановлены, и происходит перезапуск OMNI ADSL .

2.5.2 Загрузка файла конфигурации через консольный порт

Данный метод применим только к моделям OMNI ADSL с консольным портом.

Step 1. Загрузите файл конфигурации, заданный по умолчанию, с корпоративного FTP-сайта компании ZyXEL, разархивируйте его и сохраните в папке.

Step 2. Выключите OMNI ADSL, запустите программу терминальной эмуляции и включите OMNI ADSL опять. При появлении запроса "Press Any key to enter Debug Mode within 3 seconds" нажмите любую клавишу. Произойдет переход в режим отладки.

Step 3. Наберите и введите комбинацию символов "atlc" после получения сообщения "Enter Debug Mode" ("Включение режима отладки").

Step 4. Дождитесь сообщения "Starting XMODEM upload", прежде чем активизировать загрузку Xmodem на своем терминале. Ниже приводится пример загрузки конфигурации Xmodem с использованием программы HyperTerminal.

Step 5. Щелкните по **Transfer**, а затем по **Send File**, чтобы вывести следующее окно.

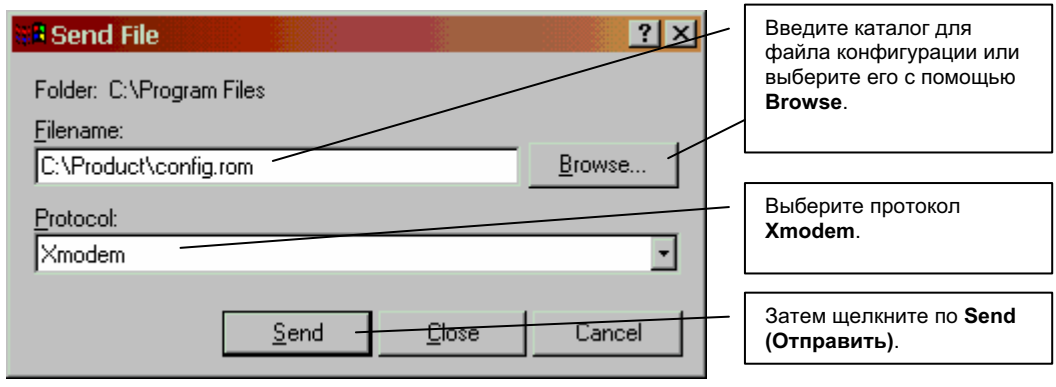


Рис. 2-4 Пример загрузки по Xmodem

Step 6. После того, как новое встроенное программное обеспечение будет успешно загружено, ввести "atgo"для перезапуска маршрутизатора.

Chapter 3
Мастер-программа установки

В данной главе содержится описание окон мастер-программы установки Web-конфигуратора.

3.1 Введение

Пользуйтесь мастер-программой установки для конфигурирования системы и ввода установок для подключения к сети Интернет, заполните *таблицу* Регистрационные данные абонента сети Интернет в *Кратком руководстве* или *Ознакомительном курсе.*. Интернет-провайдер может заранее сконфигурировать для Вас некоторые поля окна мастер-программы.

3.2 Инкапсуляция

Убедитесь в том, что вы пользуетесь методом инкапсуляции, рекомендованным вашим Интернет-провайдером. Маршрутизатором OMNI ADSL поддерживаются следующие методы.

3.2.1 Инкапсуляция ENET ENCAP

Протокол маршрутизации канального уровня с инкапсуляцией MAC (Encapsulated Routing Link Protocol) (ENET ENCAP) реализуется только с сетевым протоколом IP. Пакеты IP направляются от интерфейса Ethernet к интерфейсу WAN, а затем форматируются таким образом, чтобы они могли быть понятны в новой среде. Например, он инкапсулирует передаваемые кадры Ethernet в ячейки ATM. Протокол маршрутизации канального уровня с инкапсуляцией MAC требует указания IP-адреса шлюза в поле **Ethernet Encapsulation Gateway** второго экрана мастер-программы. Данную информацию вы можете получить у своего Интернет-провайдера.

3.2.2 PPP через Ethernet

Протокол PPPoE обеспечивает управление доступом и составление счетов пользователя аналогично способу, принятому в службах автоматической телефонной связи, пользующихся протоколом PPP. OMNI ADSL передает сеанс связи PPP через Ethernet (PPP через Ethernet, RFC 2516) от вашего компьютера в любой постоянный виртуальный канал ATM PVC (Permanent Virtual Circuit), связанный с концентратором доступа через ADSL, где завершается сеанс связи PPP. Один постоянный виртуальный канал может поддерживать неограниченное количество сеансов PPP, поступающих из вашей локальной сети. Для получения дополнительной информации о протоколе PPPoE см. приложение.

3.2.3 PPPoA

Аббревиатура PPPoA обозначает протокол PPP через уровень 5 адаптации ATM (AAL5). Этот протокол обеспечивает управление доступом и составление счетом пользователя аналогично способу, принятому в службах автоматической телефонной связи, пользующихся протоколом PPP. OMNI ADSL инкапсулирует сеанс связи PPP на основе RFC1483 и отправляет его через постоянный виртуальный канал ATM (асинхронного режима передачи) на концентратор DSLAM Интернет-провайдера. Для получения дополнительной информации о протоколе PPPoA см. RFC 2364, а для получения дополнительной информации о протоколе PPP см. RFC 1661 .

3.2.4 RFC 1483

RFC 1483 описывает два способа многопротокольной инкапсуляции через уровень 5 адаптации ATM (AAL5). Первый способ позволяет мультиплексировать несколько протоколов через единственный виртуальный канал ATM (мультиплексирование на базе LLC), а второй способ предполагает передачу каждого протокола через отдельный виртуальный канал ATM (мультиплексирование на базе VC). Для получения более подробной информации см. RFC.

3.3 Мультиплексирование

Существует два способа определить, какие протоколы передаются по виртуальному каналу (VC). Убедитесь, что вами используется метод мультиплексирования, рекомендованный Интернет-провайдером.

3.3.1 Мультиплексирование на базе VC

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

3.3.2 Мультиплексирование на базе LLC

В этом случае один виртуальный канал передает несколько протоколов с идентифицирующей информацией, которая содержится в заголовке каждого пакета. Несмотря на дополнительную загрузку канала и затраты на обработку, этот метод может оказаться предпочтительным там, где иметь отдельный виртуальный канал для каждого передаваемого протокола нерационально, напр., если оплата во многом зависит от количества одновременно задействованных виртуальных каналов.

3.4 VPI и VCI

Удостоверьтесь в том, что вы действительно пользуетесь присвоенными вам номерами идентификатора виртуального пути (VPI) и идентификатора виртуального канала (VCI). Допустимый диапазон для VPI - от 0 до 255, а для VCI - от 32 до 65535 (0 - 31 зарезервированы для локального управления трафиком ATM). Для получения дополнительной информации см. Приложения.

3.5 Конфигурация мастер-программы установки: первый экран

В **SITE MAP** щелкните по иконке **Wizard Setup** для вызова первого экрана мастер-программы.

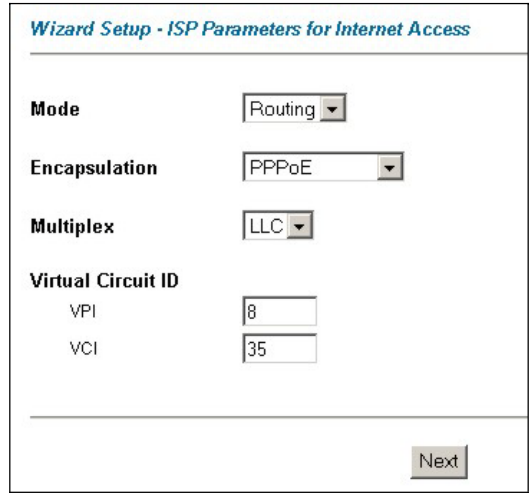


Рис. 3-1 Первый экран мастер-программы

В следующей таблице приведены описания полей данного экрана.

Табл. 3-1 Первый экран мастер-программы

ПОЛЕ	ОПИСАНИЕ

Табл. 3-1 Первый экран мастер-программы

ПОЛЕ	ОПИСАНИЕ
Mode	В раскрывающемся списке **Mode (Режим)**выберите **Routing (Маршрутизация)** (по умолчанию), если ваш Интернет-провайдер разрешает пользоваться одной учетной записью нескольким пользователям. В противном случае выберите **Bridge (Мост)**.
Encapsulation	Выберите поддерживаемый вашим Интернет-провайдером тип инкапсуляции из раскрывающегося списка **Encapsulation**. Выбор зависит от режима установленного вами в поле **Mode**. Если в поле **Mode** выбрана опция **Bridge**, здесь следует выбрать **PPPoA** или **RFC 1483**. Если в поле **Mode** выбрана опция **Routing**, здесь следует выбрать **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
Multiplex	В раскрывающемся списке **Multiplex** выберите метод мультиплексирования, поддерживаемый вашим Интернет-провайдером: на базе VC или на базе LLC.
Virtual Circuit ID	Идентификаторы виртуального пути (VPI) и виртуального канала (VCI) определяют виртуальную цепь. См. дополнительную информацию в Приложении.
VPI	Введите присвоенное значение идентификатора VPI. Это поле может быть уже сконфигурировано.
VCI	Введите присвоенное вам значение идентификатора VCI. Это поле может быть уже сконфигурировано.
Next	Щелкните по этой кнопке для вызова следующего экрана мастер-программы. Вид следующего экрана мастер-программы зависит от ранее сделанного выбора протокола. Щелкните по ссылке протокола для вызова следующего экрана мастер-программы для данного протокола.

3.6 IP-адрес и маска подсети

Точно так же, как адрес домов на улице включают название улицы, общее для всех, компьютеры в локальной сети имеют один общий сетевой номер.

Откуда именно берется этот номер, зависит от конкретной ситуации. Если Интернет-провайдер или сетевой администратор назначают блок зарегистрированных IP-адресов, то они же и указывают, какой следует выбрать IP-адрес и маску подсети.

Если Интернет-провайдер не предоставляет явным образом сетевой адрес, то вероятнее всего, открыт счет одиночного пользователя, и Интернет-провайдер назначает динамический IP-адрес при

установлении соединения. В этом случае рекомендуется выбрать IP-адрес из диапазона 192.168.0.0 - 192.168.255.0 и включить функцию трансляции сетевых адресов (NAT) маршрутизатора OMNI ADSL. Агентством по назначению имен и уникальных параметров протоколов Интернет (IANA) этот диапазон адресов зарезервирован специально для частного использования. Если не предписано иначе, не следует использовать номера за пределами этого диапазона. Если, например, выбрать в качестве сетевого номера 192.168.1.0, 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 задают номер сети, а остальные - определяют конкретный компьютер в этой сети.

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

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

3.7 IP Address Assignment (Назначение IP-адреса)

Статический IP-адрес представляет собой фиксированный IP-адрес, предоставленный Интернет-провайдером. Динамический IP-адрес не фиксирован и Интернет-провайдер каждый раз назначает новый IP-адрес. Функция счета одиночного пользователя должна быть отключена или включена, в зависимости от того, пользуетесь ли вы динамическим или статическим IP-адресом. Тем не менее, назначенный метод инкапсуляции оказывает влияние на выбор IP-адреса и шлюза ENET ENCAP.

3.7.1 Назначение IP-адреса с протоколом PPPoA или с инкапсуляцией PPPoE

Если используется динамический IP-адрес, то поля IP Address и ENET ENCAP Gateway недоступны (N/A). Если используется статический IP-адрес, следует заполнять *только* поле IP Address, и *не* заполнять поле ENET ENCAP Gateway.

3.7.2 Назначение IP-адреса с инкапсуляцией RFC 1483

В этом случае *необходимо* назначить статический IP-адрес при тех же требованиях к полям IP Address и ENET ENCAP Gateway, которые определены выше.

3.7.3 Назначение IP-адреса с инкапсуляцией ENET ENCAP

В этом случае может быть присвоен как статический, так и динамический IP-адрес. Для получения статического IP-адреса необходимо заполнить поля IP Address и ENET ENCAP Gateway fields в соответствии с указаниями Интернет-провайдера. Таким образом, при назначении динамического IP-

адреса OMNI ADSL выступает в качестве клиента DHCP с портом WAN, поэтому поля IP-адреса и шлюза ENET ENCAP становятся недоступными (N/A), так как их за устройством OMNI ADSL закрепляет сервер DHCP.

3.7.4 IP-адреса для частных сетей

Каждая машина, подключенная в сеть Интернет, должна иметь уникальный адрес. Если сеть изолирована от Интернет, напр., только внутри двух локальных сетей филиала, хост-машинам можно без проблем назначать произвольные IP-адреса. Тем не менее, Агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) специально для частных сетей зарезервировало следующие три блока IP-адресов:

```
10.0.0.0     –  10.255.255.255
172.16.0.0   –  172.31.255.255
192.168.0.0  –  192.168.255.255
```

Свой IP-адрес можно получить от IANA, Интернет-провайдера или от частной сети. Если Ваша организация является относительно небольшой, 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.

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

3.8 Полупостоянное соединение (PPP)

Полупостоянное соединение - это коммутируемая линия, на которой всегда установлено соединение, независимо от трафика. При установлении полупостоянного соединения OMNI ADSL сделает следующее: Во-первых, выключает тайм-аут простоя, а во-вторых, восстанавливает соединение каждый раз при включении и после разъединения. Очевидно, что такое полупостоянное соединение может быть очень дорого.

Полупостоянное соединение стоит устанавливать 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.

3.9 NAT

NAT (трансляция сетевых адресов - NAT, RFC 1631) - это трансляция IP-адреса хоста в пакете, например, трансляция адреса источника исходящего пакета, который используется в одной сети, в иной IP-адрес для другой сети.

3.10 Конфигурация мастер-программы установки: Второй экран

Вид второго экрана мастер-программы зависит от выбора режима и типа инкапсуляции. Все показанные экраны имеют режим маршрутизации. Заполните поля и щелкните по **Next (Далее)** для продолжения работы.

3.10.1 PPPoA

Выберите протокол **PPPoA** из раскрывающегося списка **Encapsulation (Инкапсуляция)** в первом экране мастер-программы, и вы увидите следующую картинку.

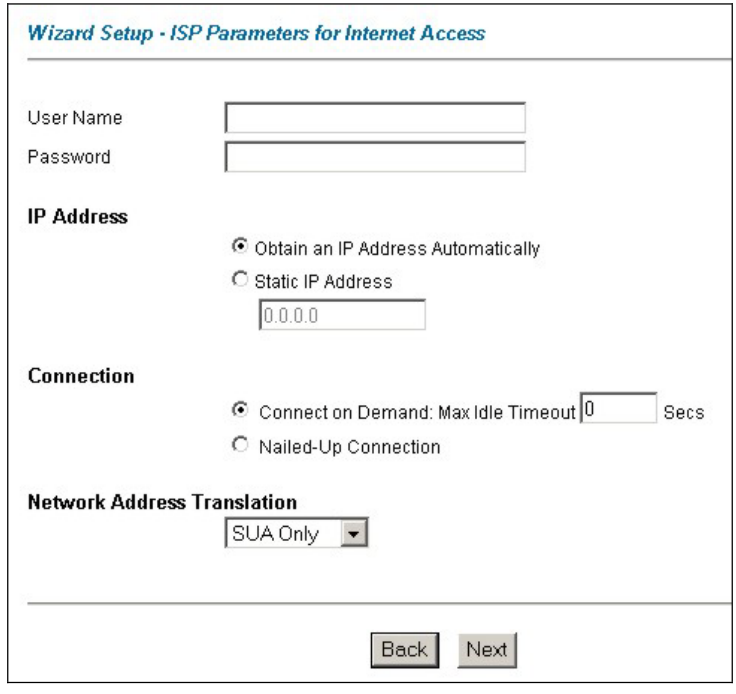


Рис. 3-2 Подключение к Интернету по протоколу PPPoA

В следующей таблице приведены описания полей данного экрана.

Табл.3-2 Подключение к Интернету по протоколу PPPoA

ПОЛЕ	ОПИСАНИЕ
User Name	Введите имя пользователя, присвоенное Вам Интернет-провайдером . Если присвоенное Вам имя пользователя имеет вид user@domain , где имя домена является идентификатором служебного имени, введите без ошибок имена обоих компонентов.
Пароль	Введите пароль, соответствующий данному имени пользователя.
IP Address	Данная опция является доступной, если вы выберете **Routing (Маршрутизация)** в поле **Mode (Режим)**. Статический IP-адрес представляет собой фиксированный IP-адрес, предоставленный Интернет-провайдером. Динамический IP-адрес не фиксирован. Он назначается каждый раз при подключении в сеть Интернет. Функциональная возможность получения счета одиночного пользователя реализуется как при назначении динамического, так и статического IP-адреса. Если используется динамический IP-адрес, щелкните по **Obtain an IP address automatically** (Автоматическое получение IP-адреса). В противном случае, щелкните по **Static IP Address (Статический IP-адрес)** и наберите присвоенный вам Интернет-провайдером IP-адрес в окне **IP Address (IP-адрес)** внизу.
Connection	Выберите опцию **Connect on Demand (Подключение по требованию)**, если хотите иметь постоянное подключение к сети Интернет и укажите время ожидания (в секундах) в поле **Max. Idle Timeout** (Макс. время простоя). По умолчанию действуют установки **Connection on Demand (Подключение по требованию)** со значением времени простоя "0", что означает отсутствие ограничений по продолжительности сеанса связи. Выберите опцию **Nailed-Up Connection (Полупостоянное соединение)** , если хотите иметь постоянное подключение к сети. В случае отключения от сети OMNI ADSL постарается автоматически восстановить соединение. Правило(-а) SMT меню 26 имеет(-ют) более высокий приоритет по отношению к параметрам настройки пользователя **Connection (Соединение)** .

Табл.3-2 Подключение к Интернету по протоколу PPPoA

ПОЛЕ	ОПИСАНИЕ
Network Address Translation	Данная опция является доступной, если в поле **Mode (Режим)** выбрано **Routing (Маршрутизация)** Выберите нужную опцию **None**, **SUA Only** или **Full Feature** из меню раскрывающегося списка. Для получения дополнительной информации см. главу Трансляция сетевых адресов (NAT) .
Back	Щелкните по **Back (Назад)**для возвращения к первому экрану мастер-программы.
Next	Щелкните по **Next (Далее)** для перехода к следующему экрану мастер-программы.

3.10.2 RFC 1483

Выберите RFC **1483 PPPoA** из раскрывающегося списка **Encapsulation (Инкапсуляция)** на первом экране мастер-программы и увидите следующее изображение.

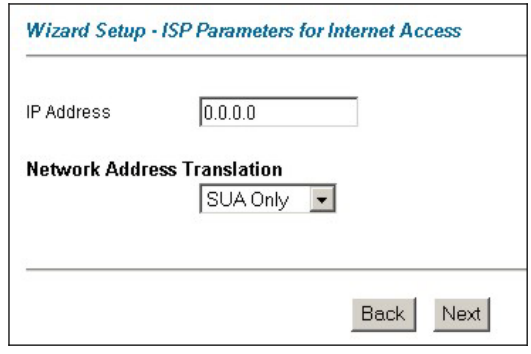


Рис. 3-3 Подключение к сети Интернет по протоколу RFC 1483

В следующей таблице приведены описания полей данного экрана.

Табл. 3-3 Подключение к сети Интернет по протоколу RFC 1483

ПОЛЕ	ОПИСАНИЕ

Табл. 3-3 Подключение к сети Интернет по протоколу RFC 1483

ПОЛЕ	ОПИСАНИЕ
IP Address	Данное поле является доступным, если в поле **Mode (Режим)**выбрана опция **Routing (Маршрутизация)** Наберите в этом поле присвоенный вам Интернет-провайдером IP-адрес.
Network Address Translation	Выберите нужную опцию **None**, **SUA Only** или **Full Feature** из раскрывающегося списка. См. главу Трансляция сетевых адресов (NAT) для получения дополнительной информации.
Back	Щелкните по **Back (Назад)**для возвращения к первому экрану мастер-программы.
Next	Щелкните по **Next (Дальше)** для перехода к следующему экрану мастер-программы.

3.10.3 Инкапсуляция ENET ENCAP

Выберите **ENET ENCAP** из раскрывающегося списка **Encapsulation (Инкапсуляция)** на первом экране мастер-программы, и Вы увидите следующее изображение.

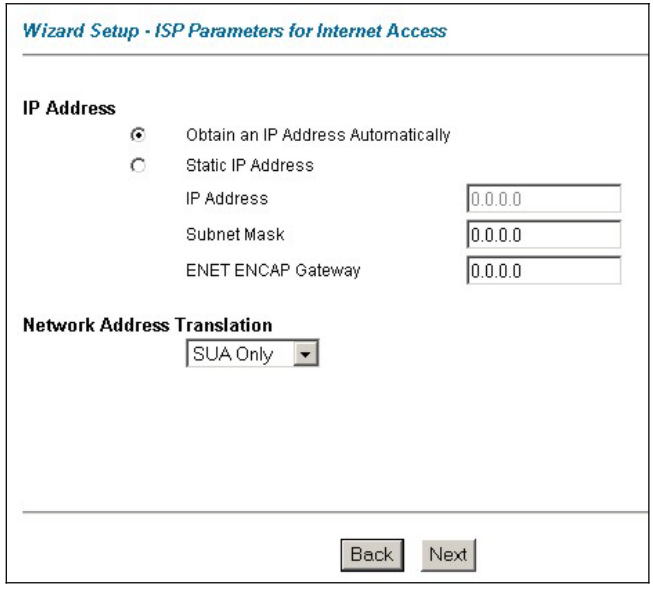


Рис. 3-4 Подключение к сети Интернет по протоколу ENET ENCAP

В следующей таблице приведены описания полей данного экрана.

Табл. 3-4 Подключение к сети Интернет по протоколу ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
IP Address	Статический IP-адрес представляет собой фиксированный IP-адрес, предоставленный Интернет-провайдером. Динамический IP-адрес не фиксирован. Он назначается каждый раз при подключении к сети Интернет. Функциональная возможность получения счета одиночного пользователя реализуется как при назначении динамического, так и статического IP-адреса. Если используется динамический IP-адрес, щелкните по **Obtain an IP address automatically** (автоматическое получение IP-адреса). В противном случае, щелкните по **Static IP Address (Статический IP-адрес)** и наберите присвоенный Вам Интернет-провайдером IP-адрес в окне **IP Address (IP-адрес)** внизу.
Subnet Mask	Введите код маски подсети в десятичном виде с разделительными точками. См. приложение *IP Subnetting IP-протоколы организации подсетей* для вычисления кода маски подсети, если намерены заниматься организацией подсетей.
ENET ENCAP Gateway	Необходимо указать IP-адрес шлюза (назначенный вашим Интернет-провайдером), если выбрана опция **ENET ENCAP** в поле **Encapsulation** во время работы с предыдущим экраном.
Network Address Translation	Выберите нужную опцию **None**, **SUA Only** или **Full Feature** из меню раскрывающегося списка. Для получения дополнительной информации см. главу Трансляция сетевых адресов (NAT) .
Back	Щелкните по **Back (Назад)** для возвращения к первому экрану мастер-программы.
Next	Щелкните по **Next (Далее)** для перехода к следующему экрану мастер-программы.

3.10.4 PPPoE

Выберите протокол **PPPoE** из раскрывающегося списка **Encapsulation (Инкапсуляция)** на первом экране мастер-программы, и увидите следующее изображение.

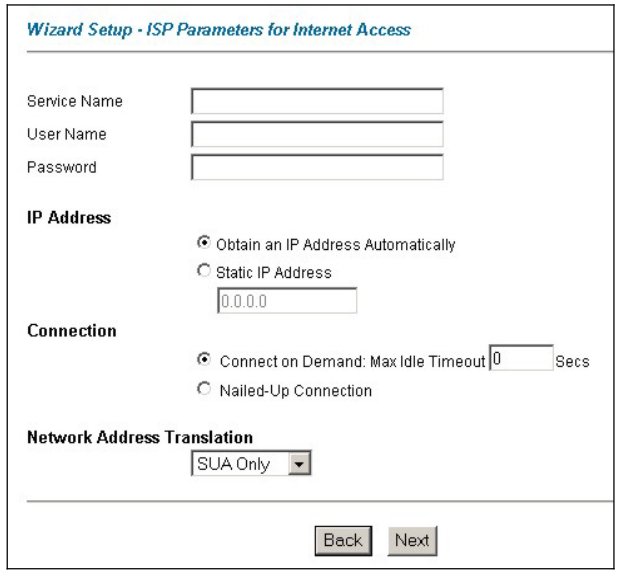


Рис. 3-5 Подключение к Интернету по протоколу PPPoE

В следующей таблице приведены описания полей данного экрана.

Табл. 3-5 Подключение к Интернету по протоколу PPPoE

ПОЛЕ	ОПИСАНИЕ
Service Name	Наберите здесь имя вашей службы PPPoE.
User Name	Заполните поля **User Name (Имя пользователя)** и **Password (Пароль)** только в случае, если пользуетесь **PPPoA** и **PPPoE** инкапсуляцией. Введите присвоенное Вам Интернет-провайдером имя пользователя. Если присвоенное вам имя пользователя имеет вид user@domain , где имя домена является идентификатором служебного имени, введите без ошибок имена обоих компонентов.
Password	Введите пароль, соответствующий данному имени пользователя.

Табл. 3-5 Подключение к Интернету по протоколу PPPoE

ПОЛЕ	ОПИСАНИЕ
IP Address	Статический IP-адрес представляет собой фиксированный IP-адрес, предоставленный Интернет-провайдером. Динамический IP-адрес не фиксирован. Он назначается каждый раз при подключении к сети Интернет. Функциональная возможность получения счета одиночного пользователя реализуется как при назначении динамического, так и статического IP-адреса. Если используется динамический IP-адрес, щелкните по **Obtain an IP address automatically** (Автоматическое получение IP-адреса). В противном случае, щелкните по **Static IP Address (Статический IP-адрес)** и наберите присвоенный Вам Интернет-провайдером IP-адрес в окне **IP Address (IP-адрес)** внизу.
Connection	Выберите опцию **Connect on Demand (Подключение по требованию)**, если не хотите иметь постоянное подключение к сети Интернет и укажите время ожидания (в секундах) в поле **Max. Idle Timeout** (Макс. время простоя). По умолчанию действуют установки **Connection on Demand (Подключение по требованию)** со значением времени простоя "0", что означает отсутствие ограничений по продолжительности сеанса связи. Выберите опцию **Nailed-Up Connection (Полупостоянное соединение)**, если хотите иметь постоянное подключение к сети. В случае отключения от сети, OMNI ADSL постарается автоматически восстановить соединение. Правило(-а) SMT меню 26 имеет(-ют) более высокий приоритет по отношению к параметрам настройки пользователя**Connection (Соединение)** .
Network Address Translation	Выберете нужную опцию **None**, **SUA Only** или **Full Feature** из меню раскрывающегося списка. Для получения дополнительной информации см. главу Трансляция сетевых адресов (NAT) .
Back	Щелкните по **Back (Назад)** для возвращения к первому экрану мастер-программы.
Next	Щелкните по **Next (Далее)** для перехода к следующему экрану мастер-программы.

3.11 DHCP Setup (Настройка DHCP)

DHCP (Dynamic Host Configuration Protocol - протокол динамического конфигурирования хост-машины, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получить при начальной загрузке конфигурацию TCP/IP с сервера. OMNI ADSL можно сконфигурировать как сервер DHCP или отключить эту опцию. При конфигурации в качестве сервера, OMNI ADSL

предоставляет клиентам конфигурацию TCP/IP. При отключении опции сервиса DHCP должен быть назначен другой сервер DHCP локальной сети или произведена настройка компьютера вручную.

3.11.1 Настройка IP-пула

OMNI ADSL имеет сконфигурированный пул из 32 IP-адресов для машин-клиентов, начиная с 192.168.1.33 до 192.168.1.64 . Такая конфигурация позволяет оставлять свободным 31 IP-адрес, от 192.168.1.2 до 192.168.1.32 (за исключением одного адреса для самого OMNI ADSL - 192.168.1.1), для назначения другим машинам, напр., для почтового сервера, FTP, telnet, web и других служб Интернета, которые могут потребоваться.

3.12 Конфигурация мастер-программы установки: Третий экран

Проверьте параметры настройки, как это показано на следующем рисунке. Для изменения в OMNI ADSL данных о локальной сети щелкните **Change LAN Configurations (Изменение конфигурации ЛВС)**. В противном случае щелкните по иконке **Save Settings (Сохранение настройки)** для сохранения параметров настройки и перейдите к разделу 3.13.

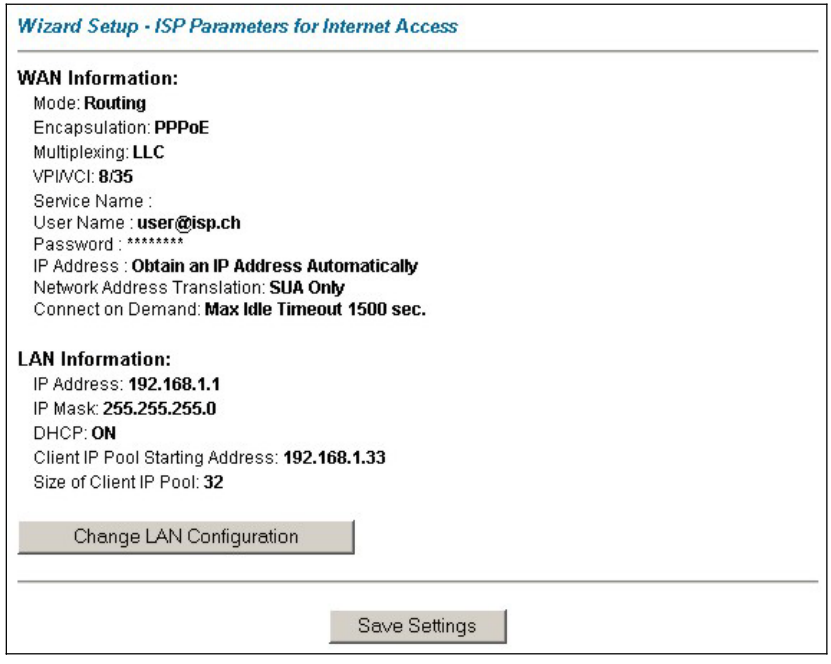


Рис. 3-6 Третий экран мастер-программы

Если хотите изменить в OMNI ADSL параметры настройки ЛВС, щелкните вкладку **Change LAN Configuration (Изменение конфигурации ЛВС)** для перехода к экрану, показанному на рисунке.

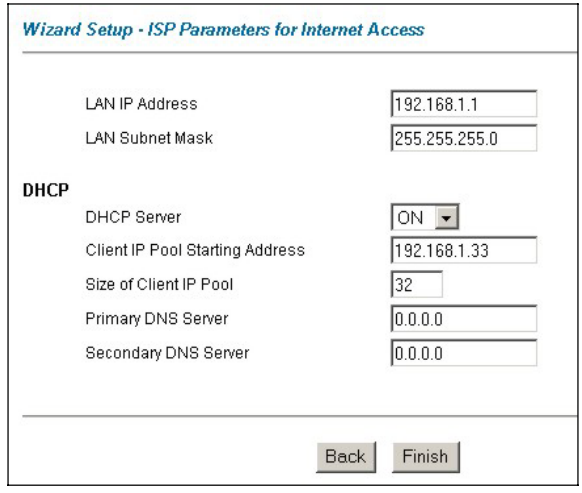


Рис. 3-7 Мастер-программа: конфигурация ЛВС

В следующей таблице приведены описания полей данного экрана.

Табл. 3-6 Мастер-программа: конфигурация ЛВС

ПОЛЕ	ОПИСАНИЕ
LAN IP Address	Введите IP-адрес OMNI ADSL в десятичном виде с разделительными точками, например, 192.168.1.1 (заданный изготовителем по умолчанию). **Если вы изменили IP-адрес OMNI ADSL в локальной сети, следует пользоваться новым IP-адресом, если хотите вновь получить доступ к Web-конфигуратору, .**
LAN Subnet Mask	Введите код маски подсети в десятичном виде с разделительными точками.
DHCP (Dynamic Host Configuration Protocol/Протокол динамического выбора конфигурации хост-машины)	

Табл. 3-6 Мастер-программа: конфигурация ЛВС

ПОЛЕ	ОПИСАНИЕ
DHCP Server	В раскрывающемся списке **DHCP Server** выберите опцию **On**, разрешающую маршрутизатору OMNI ADSL назначать IP-адреса, IP шлюза по умолчанию и серверов DNS для компьютерных систем, поддерживающих работу клиента DHCP. Выберите **Off** для отключения опции DHCP Server. Если пользуетесь опцией DHCP Server, выполните следующие установки:
Client IP Pool Starting Address	В этом поле задается первый адрес из пула непрерывных IP-адресов.
Size of Client IP Pool	В этом поле задается размер или счетчик пула непрерывных IP-адресов.
Primary DNS Server	Ввести IP-адреса серверов DNS. Серверы DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Secondary DNS Server	Как указано выше.
Back	Щелкните **Back (Назад)**для возвращения к предыдущему экрану.
Finish	Щелкните по **Finish** для сохранения параметров настройки и перехода к следующему экранному меню мастер-программы.

3.13 Конфигурация мастер-программы установки: Проверка соединения

OMNI ADSL автоматически выполняет проверку соединений с компьютерами, подключенными к портам ЛВС. Для проверки соединения OMNI ADSL с Интернет-провайдером щелкните **Start Diagnose (Начать диагностику)**. В противном случае щелкните по **Return to Main Menu (Возврат в главное меню)** для возвращения к экрану **Site Map (Карта сайта)** .

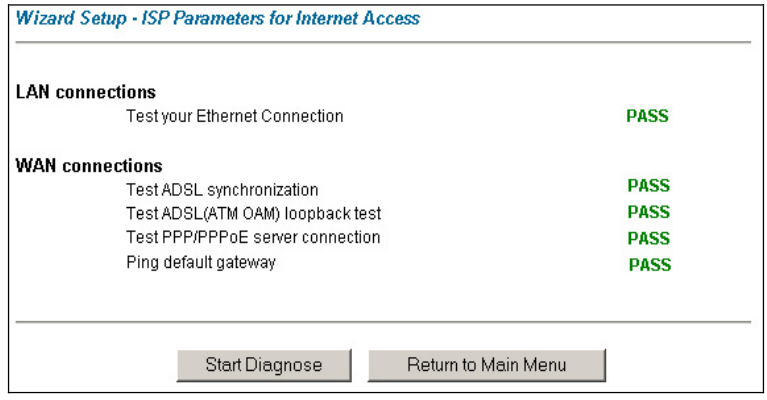


Рис. 3-8 Четвертый экран мастер-программы

3.14 Проверка подключения к сети Интернет

Запустите Web-браузер и обратитесь к сайту www.zyxel.com. Выход в Интернет является только началом проверки. Для ее завершения обратитесь к *Руководству пользователя*, где вы сможете ознакомиться с подробной информацией обо всех технических характеристиках и возможностях устройства OMNI ADSL. Если не удалось подключиться к сети Интернет, откройте снова Web-конфигуратор и проверьте правильность заданных с помощью мастер-программы параметров настройки.

Part II:

Локальная вычислительная сеть, беспроводная вычислительная сеть и глобальная вычислительная сеть

В настоящей части рассматриваются вопросы настройки ЛВС, беспроводной ЛВС и подключения к глобальной сети.

Chapter 4
Настройка локальной сети

В данной главе описывается, как выполнить конфигурирование настроек LAN.

4.1 Описание локальной вычислительной сети

Локальная сеть (Local Area Network) - это совместно используемая сеть связи, к которой может быть подключено большое количество компьютеров. Локальная сеть является компьютерной сетью, функционирующей в пределах ограниченной территории, обычно в пределах одного здания или его этажа. Экраны LAN помогут выполнить конфигурацию сервера DHCP локальной сети и организовать управление IP-адресами.

4.1.1 LAN, WAN и OMNI ADSL

Фактический физический канал определяет, являются ли порты OMNI ADSL портами локальной или глобальной сети. Ниже приведен пример с двумя отдельными IP-сетями: одной внутренней, локальной, и другой внешней - глобальной:

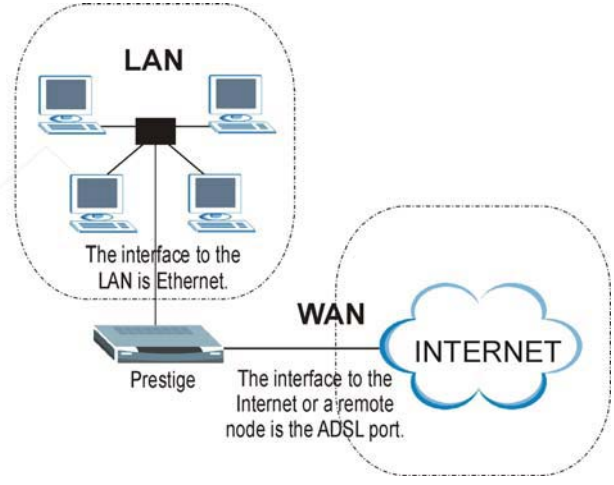


Рис. 4-1 Адресование в локальной и глобальной вычислительныхсетях

4.2 Адрес сервера DNS

DNS (Domain Name System/Служба имен доменов) предназначена для отображения имени домена на соответствующий IP-адрес и наоборот, напр., IP-адрес *www.zyxel.com* - 204.217.0.2. Сервер DNS

играет крайне важную роль, так как без него необходимо было бы точно знать IP-адрес машины, к которой нужно получить доступ. Адреса серверов DNS, которые задаются при настройке DHCP, передаются клиентским машинам вместе с назначенным IP-адресом и маской подсети.

Существует два способа распространения адресов серверов DNS Интернет-провайдером. Первый из них заключается в том, что Интернет-провайдер сообщает клиенту адреса сервера DNS обычно в виде информационного листка, уведомляющего клиента об адресе. Если Интернет-провайдер предоставил адрес серверов DNS, следует ввести его в поле **DNS Server** в экране **DHCP Setup**, в противном случае оставить это поле пустым.

Некоторые Интернет-провайдеры предпочитают передавать адреса серверов DNS после подключения, с использованием DNS-расширений протокола PPP IPCP (Протокол управления IP). Если Интернет-провайдер не предоставляет адреса серверов DNS в явной форме, значит, изменения для сервера DNS передаются посредством согласования IPCP. OMNI ADSL поддерживает расширение DNS-сервера IPCP посредством функции proxy-сервера DNS.

Если поля **Primary** и **Secondary DNS Server** в **DHCP Setup** не определены, т.е. оставлены значения 0.0.0.0, OMNI ADSL сообщает клиентам DHCP, что он является сервером DNS. Когда компьютер посылает запрос DNS на OMNI ADSL, то OMNI ADSL пересылает запрос на истинный сервер DNS, определенный с помощью IPCP и ретранслирует ответ назад компьютеру.

Следует отметить, что proxy-сервер DNS может работать только тогда, когда Интернет-провайдер использует DNS-расширения IPCP. Это не означает, что можно при любых обстоятельствах не включать серверы DNS в настройки DHCP. Если Интернет-провайдер предоставляет адреса серверов DNS в явной форме, следует убедиться, что эти IP-адреса введены в **DHCP Setup**. Таким образом, OMNI ADSL может быть связующим элементом между серверами DNS и компьютерами; кроме того, компьютеры могут обращаться к серверу DNS без вмешательства OMNI ADSL.

4.3 Назначение адресов сервером DNS

Следует пользоваться DNS (Службой имен доменов) для преобразования имени домена в соответствующий ему IP-адрес и наоборот. Сервер DNS играет крайне важную роль, так как без него нужно было бы точно знать IP-адрес компьютера, к которому необходимо получить доступ.

Существует два способа распространения адресов сервера DNS Интернет-провайдером.

1. Интернет-провайдер должен сообщить адреса серверов DNS. Обычно они содержатся в информационном листке, который вручается клиенту при подписании договора об абонентском обслуживании. Если адреса DNS-серверов получены от Интернет-провайдера, следует ввести их в поля DNS Server в DHCP Setup
2. Оставьте поля сервера DNS в DHCP SETUP не заполненными (например: 0.0.0.0). В этом случае OMNI ADSL будет выступать в качестве proxy-сервера DNS.

4.4 Настройка TCP/IP локальной сети

OMNI ADSL обладает возможностями встроенного сервера DHCP, что позволяет ему назначать IP-адреса и сервера DNS системам с поддержкой клиента DHCP.

4.4.1 Настройки изготовителя по умолчанию для локальной сети

Параметры локальной сети для OMNI ADSL, установленные изготовителем, имеют следующие значения:

- IP-адрес 192.168.1.1 с маской подсети 255.255.255.0 (24 бита).
- Активизированный сервер DHCP с 32 клиентскими IP-адресами, начиная с 192.168.1.33.

Данные параметры работоспособны в большинстве случаев. Если Ваш Интернет-провайдер предоставляет адрес(-а) сервера DNS в явной форме, обратитесь к встроенной справочной системе Web-конфигуратора для выяснения, какие поля должны быть заполнены.

4.4.2 IP-адрес и маска подсети

См. раздел *IP-адрес и маска подсети* в главе **Мастер-программа установки** для получения дополнительной информации.

4.4.3 Настройка RIP

RIP (Routing Information Protocol/Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Значение параметра в поле **RIP Direction** используется в управлении приемом и передачей пакетов RIP. Задайте следующие опции:

1. **Both -** OMNI ADSL будет периодически осуществлять циркулярную рассылку маршрутной таблицы и объединять получаемые данные RIP.
2. **In Only -** OMNI ADSL не будет передавать никакие пакеты RIP, но будет принимать все поступающие к нему пакеты RIP.
3. **Out Only -** OMNI ADSL будет передавать исходящие пакеты RIP, но не будет принимать никакие входящие пакеты RIP.
4. при установке **None**, OMNI ADSL не будет передавать никакие пакеты RIP, а входящие пакеты RIP будут игнорироваться.

Поле **Version** (Версия) управляет форматом и способом циркулярной рассылки пакетов RIP, которые посылает OMNI ADSL (оба формата распознаются им при получении). Формат **RIP-1** является общепринятым, однако формат RIP-2 содержит больше информации. Формат RIP-1 подходит для большинства сетей, если только сеть не имеет какой-либо специфической топологии.

RIP-2B и **RIP-2M** рассылают данные о маршрутизации в формате RIP-2; Их отличие заключается в том, что **RIP-2B** использует циркулярную рассылку для подсети, а **RIP-2M** многоадресную рассылку.

4.4.4 Multicast (Многоадресная рассылка)

Обычно передача пакетов IP происходит одним из двух способов - одноадресная рассылка (1 отправитель — 1 получатель) или циркулярная рассылка (1 отправитель — все компьютеры в сети). С помощью многоадресной рассылки происходит доставка IP-пакетов группе хост-машин в сети, то есть, не одной, но и не всем машинам в сети.

IGMP (Internet Group Multicast Protocol/Протокол многоадресной рассылки) - это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки - он не предназначен для передачи пользовательских данных. Версия 2 IGMP (RFC 2236) является усовершенствованным вариантом версии 1 (RFC 1112), однако версия 1 IGMP по-прежнему широко используется. Если необходимо получить более подробную информацию о взаимодействии версии 1 и 2 протокола IGMP, см. разделы 4 и 5 RFC 2236. IP-адрес класса D используется для идентификации группы хост-машин и имеет значения в диапазоне от 224.0.0.0 до 239.255.255.255. Адрес 224.0.0.0 не назначается ни одной группе и используется компьютерами, осуществляющими многоадресную рассылку IP. Адрес 224.0.0.1 используется для запросов и назначается постоянной группе, в которую входят все хост-машины IP (включая шлюзы). Все хосты должны объединяться в группу 224.0.0.1 для того, чтобы участвовать в многоадресной рассылке. Адресная группа 224.0.0.2 закреплена за маршрутизаторами, участвующими в многоадресной рассылке.

OMNI ADSL поддерживает как версию 1 IGMP (**IGMP-v1**), так и версию 2 IGMP (**IGMP-v2**). При запуске OMNI ADSL запрашивает все сети, к которым он непосредственно подключен, с целью определения их принадлежности к группе. В дальнейшем OMNI ADSL будет периодически обновлять эту информацию. Функция многоадресной рассылки IP может быть включена/отключена на интерфейсах LAN/WAN Web-конфигуратора (**LAN**; **WAN**). Для отключения многоадресной рассылки IP на этих интерфейсах выберите опцию **None**.

4.5 Настройка конфигурации ЛВС

Щелкните **LAN** для вызова следующего экрана.

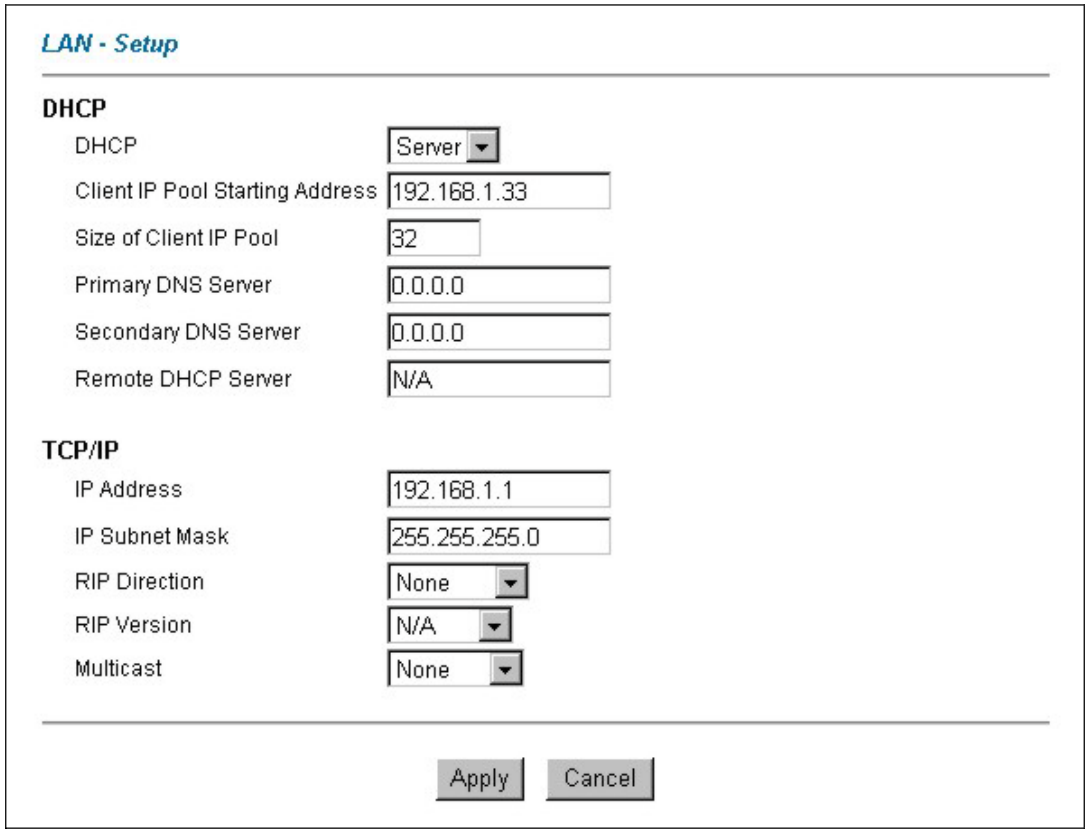


Рис. 4-2 Локальная вычислительная сеть

В следующей таблице приведены описания полей данного экрана.

Табл. 4-1 Локальная вычислительная сеть

ПОЛЕ	ОПИСАНИЕ
DHCP	

Табл. 4-1 Локальная вычислительная сеть

ПОЛЕ	ОПИСАНИЕ
DHCP (Dynamic Host Configuration Protocol/Протокол динамического выбора конфигурации хост-машины)	Если в данном поле установлено **Server**, то OMNI ADSL может назначать IP-адреса, IP-шлюз (по умолчанию) и адреса серверов DNS для Windows 95, Windows NT и других систем, поддерживающих клиентов DHCP. Если установлена опция **None**, функция сервера DHCP отключается. Если установлена опция **Relay**, OMNI ADSL выступает в качестве фиктивного сервера DHCP и ретранслирует запросы и ответы DHCP между удаленным сервером и клиентами. В этом случае следует ввести IP-адрес действительного удаленного сервера DHCP в поле Remote DHCP Server. Если используется DHCP, необходимо задать следующие параметры:
Client IP Pool Starting Address	В этом поле задается первый адрес из пула непрерывных IP-адресов.
Size of Client IP Pool	В этом поле задается размер или счетчик пула непрерывных IP-адресов.
Primary DNS Server	Ввести IP-адреса серверов DNS. Серверы DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Secondary DNS Server	Как указано выше.
Remote DHCP Server	Если в указанном выше поле **DHCP** установлено **Relay**, следует ввести сюда IP-адрес действительного удаленного сервера DHCP.
TCP/IP	
IP Address	Введите IP-адрес вашего маршрутизатора OMNI ADSL в десятичном виде с разделительными точками, например, 192.168.1.1 (установленный изготовителем по умолчанию).
IP Subnet Mask	Введите присвоенный Интернет-провайдером код маски подсети (если он есть).
RIP Direction	Выберите направление RIP из перечня: **None**, **Both**, **In Only** и **Out Only**.
RIP Version	Выберите версию RIP из перечня: **RIP-1**, **RIP-2B** и **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol/Протокол многоадресной рассылки) - это протокол сеансового уровня, используемый для установления принадлежности к группе многоадресной рассылки. OMNI ADSL поддерживает обе версии протокола IGMP (**IGMP-v1**) и **IGMP-v2**. Выберите опцию **None** для их отключения.

Табл. 4-1 Локальная вычислительная сеть

ПОЛЕ	ОПИСАНИЕ
Apply	Щелкните по этой кнопке для сохранения данных параметров настройки OMNI ADSL.
Cancel	Щелкните по этой кнопке для сброса содержимого полей экрана.

Chapter 5
Настройка беспроводной LAN

В данной главе рассматривается, как выполнить конфигурацию настройки LAN на маршрутизаторе OMNI ADSL. Содержание данной главы относится только к моделям OMNI ADSL LAN H и OMNI ADSL LAN HW.

5.1 Описание беспроводных ЛВС

В этом разделе дается краткое описание беспроводных ЛВС и их базовых конфигураций. Беспроводная ЛВС может быть как простой одноранговой сетью, состоящей из двух компьютеров с сетевыми радиокартами, так и сложной сетью, в состав которой входит большое число компьютеров с сетевыми радиокартами, подключенных к точкам доступа проводных ЛВС, выполняющих функции моста для сетевого трафика.

Работа с экранами беспроводной LAN (WLAN) возможна только при наличии в составе маршрутизаторов сетевых радиокарт.

5.1.1 Дополнительные требования по установке при использовании стандарта 802.1x

- Компьютер должен иметь сетевую радиокарту стандарта IEEE 802.11b и Web-браузер, поддерживающий JavaScript и функции сетевого теледоступа Telnet.
- Компьютер беспроводной станции должен иметь программное обеспечение, отвечающее требованиям стандарта IEEE 802.1x. В настоящее время им отвечает операционная система Windows XP.
- Дополнительный сетевой RADIUS-сервер для аутентификации и учета работы удаленных пользователей.

5.1.2 Канал

Частотный диапазон, использующийся беспроводными устройствами стандарта IEEE 802.11b, называется каналом. Доступность каналов зависит от географического местоположения Вашей сети. Необходимо иметь возможность выбора каналов (применительно к региону), так чтобы можно было пользоваться другим каналом (отличным от канала соседней точки доступа) для уменьшения помех. Помехи и ухудшение качества связаны с наложением частот радиосигналов, поступающих от разных точек доступа.

Тем не менее, возможно частичное перекрытие частотных диапазонов близких каналов. Для предупреждения помех, вызванных перекрытием частотных диапазонов, точка доступа должна

использовать канал, отстоящий не менее чем на пять каналов от канала, используемого соседней точкой доступа. Например, если в регионе имеется 11 каналов, а в ближайшей точке доступа используется 1-й канал, то следует выбрать каналы от 6-го до 11-го.

5.1.3 Идентификатор ESS

ESS обозначает группу точек доступа или беспроводных шлюзов, подключенных к проводной ЛВС той же подсети. Идентификатор ESS является уникальным для каждой группы. Все точки доступа и беспроводные шлюзы, а также связывающиеся с ними станции беспроводной связи одной группы, должны иметь общий идентификатор ESS (ESSID).

5.1.4 Передача сигналов RTS/CTS

Появление скрытого узла связано с ситуацией, когда две станции с общей точкой доступа работают в одном частотном диапазоне, но их рабочие зоны не совпадают. Приведенный ниже рисунок служит иллюстрацией такого случая. Обе станции (STA) находятся в рабочей зоне точки доступа (AP) или радиошлюза, но вне рабочих зон друг друга, так что они не могут "слышать" друг друга и не "знают", занят ли данный канал в настоящее время. Таким образом, они могут рассматриваться как "невидимые" друг для друга.

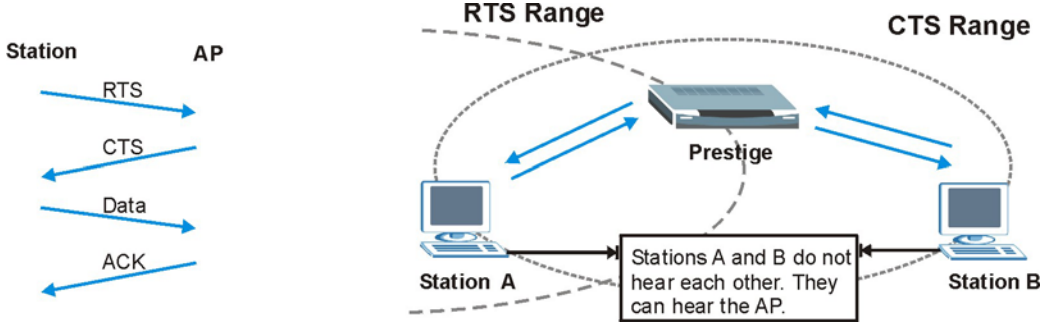


Рис. 5-1 Передача сигналов RTS/CTS

Когда станция A начинает передачу данных в адрес OMNI ADSL, она может не иметь информации о том, что канал уже занят станцией B. При одновременной передаче данных от двух станций и одновременном их поступлении в точку доступа может возникнуть конфликт, сопровождающийся потерей сообщений обеих станций.

Сигналы RTS/CTS предназначены для предотвращения конфликтов, обусловленных наличием скрытых узлов. В сигналах **RTS/CTS** содержится информация о наибольшем размере кадра, который может быть отправлен до получения подтверждения на передачу сигналов RTS (Request To Send/Запрос на передачу)/CTS (Clear to Send/Разрешение передачи).

Если размер кадра данных превышает заданные размеры сигналов **RTS/CTS** (от 0 до 2432 байт), то станция, передающая этот кадр, должна вначале отправить в точку доступа сообщение RTS с запросом разрешения на передачу. В ответ из точки доступа отправляется сообщение CTS в адрес всех работающих с ней станций для извещения о необходимости задержаться с передачей данных. Этим сообщением также подтверждается и резервируется запрошенный станцией временной интервал на передачу.

Со станций могут передаваться кадры, размером меньше заданных сообщениями**RTS/CTS,** непосредственно в точку доступа без квитирования сообщений RTS/CTS.

Опцию **RTS/CTS** следует установить только в случае, если вероятность существования скрытых узлов в сети и "стоимость" повторных попыток передачи кадров большого размера, превышают объем служебной информации при квитировании RTS/CTS.

Если размеры сообщений **RTS/CTS** превышают **Fragmentation Threshold/Допустимые размеры фрагментов** (см. ниже), то квитирование окажется невозможным, поскольку кадры будут подвергаться фрагментации до размеров сообщений **RTS/CTS**.

Установление ограничений на размер сообщений RTS позволяет уменьшить объемы передаваемой служебной информации, но может вызвать снижение пропускной способности сети вместо ее повышения.

5.1.5 Допустимые размеры фрагментов

Допустимым размером фрагментов называется максимальный размер поля данных кадра (от 256 до 2432 байт), который может передаваться в беспроводной сети, прежде чем OMNI ADSL выполнит фрагментацию пакета в меньшие по размеру кадры данных.

Большое значение **допустимых размеров фрагментов** рекомендуется для сетей, не подверженных влиянию помех, в то время как небольшое значение может быть рекомендовано для нагруженных сетей или сетей, подверженных влиянию помех.

Если размеры сообщений **RTS/CTS** превышают **Fragmentation Threshold/Допустимые размеры фрагментов** (см. ниже), то получение разрешения на сеанс связи окажется невозможным, поскольку кадры будут подвергаться фрагментации до размеров сообщений **RTS/CTS**.

5.2 Уровни защиты

Защита беспроводной сети является жизненно важной функцией, обеспечивающей защиту радиоканалов, по которым осуществляется связь между беспроводными станциями, точками доступа и проводной вычислительной сетью.

На приведенном ниже рисунке показаны уровни защиты беспроводной сети, поддерживаемые маршрутизатором OMNI ADSL. Высший уровень защиты основывается на протоколе EAP (Extensible Authentication Protocol/Расширенный протокол аутентификации), предназначенный для аутентификации и применения динамического обмена ключами по протоколу WEP (Wired Equivalent

Privacy). Он предполагает взаимодействие с RADIUS-сервером в глобальной сети или ЛВС для выполнения задач аутентификации применительно к беспроводным станциям.

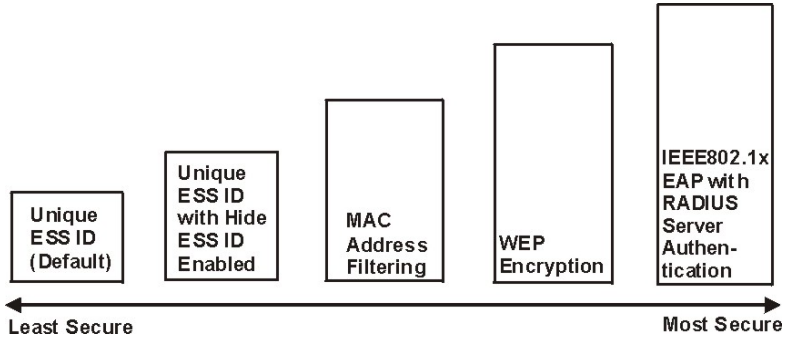


Рис. 5-2 Уровни защиты беспроводной связи маршрутизатора OMNI ADSL

При отключенной защите беспроводной связи сеть становится открытой для доступа любого радиоустройства, работающего в данном диапазоне.

Для установки настроек защиты беспроводной ЛВС следует пользоваться Web-конфигуратором. См. раздел об использовании Web-конфигуратора OMNI ADSL для ознакомления с его работой.

5.3 Криптографическая защита данных по протоколу WEP

Протокол криптографической защиты WEP предназначен для шифрования методом скремблирования (псевдослучайного искажения) поля данных, передающихся между беспроводными станциями и точками доступа для предупреждения несанкционированного доступа. Шифруются как одноадресные, так и многоадресные рассылки в сети. И в беспроводных станциях, и в точках доступа должны применяться одинаковые WEP-ключи для шифрования данных и их дешифровки.

OMNI ADSL позволяет установить до 4-х 64-битовых или 128-битовых WEP-ключей, но каждый раз будет применяться только один ключ.

5.4 Подключение сетевой радиокарты PCMCIA

Для работы в беспроводных сетях используйте сетевые радиокарты PCMCIA серии ZyAIR .

Step 1. Выключите OMNI ADSL.

Запрещается вставлять и вынимать сетевую радиокарту во время работы устройства OMNI ADSL.

Step 2. Отыщите слот с маркировкой **Wireless LAN** на устройстве OMNI ADSL.

Step 3. Направьте контактный разъем в сторону слота так, чтобы сторона со светодиодом была обращена вверх, и вставьте в него сетевую радиокарту ZyAIR.

Вставляйте радиокарту в слот без нажима, не допуская перегибов и перекосов платы.

Step 4. Включите OMNI ADSL. Должен загореться светодиод **WLAN** LED.

5.5 Настройка беспроводной ЛВС

Если выполняется настройка конфигурации устройства OMNI ADSL на компьютере, подключенном к беспроводной ЛВС, с изменением параметров настройки ESSID или WEP, то после нажатия кнопки Apply для подтверждения настроек соединение по радиоканалу будет отключено. Нужно будет поменять настройки беспроводной связи на компьютере для того, чтобы они соответствовали новым настройкам OMNI ADSL.

Щелкните по вкладкам **Wireless LAN (Беспроводная ЛВС)**, **Wireless (Беспроводная связь)** для того чтобы открыть экран **Wireless** .

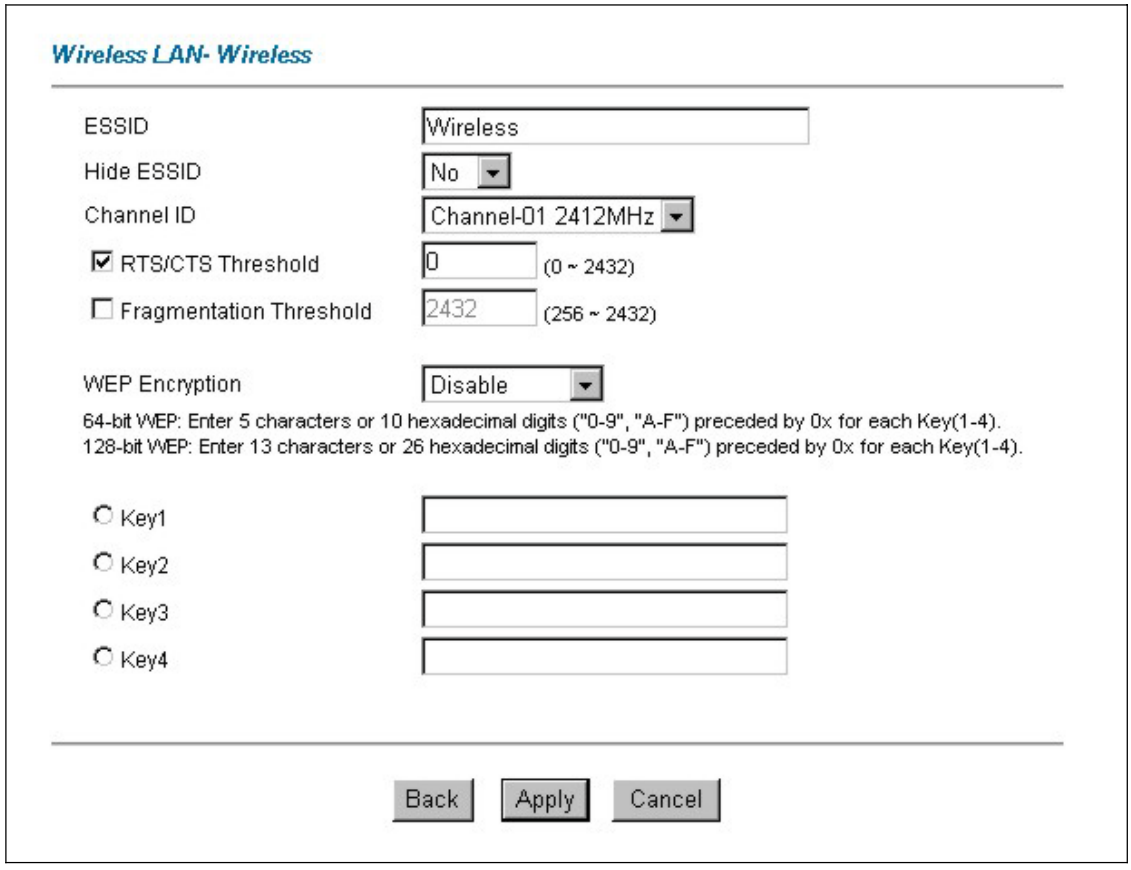


Рис. 5-3 Экран Wireless

В следующей таблице приведены описания полей данного экрана.

Табл. 5-1 Беспроводная связь

ПОЛЕ	ОПИСАНИЕ
ESSID	Идентификатор ESS (ESSID) является уникальным именем для идентификации устройства OMNI ADSL в беспроводной ЛВС. Беспроводные станции, подключенные к OMNI ADSL, должны иметь общий ESSID. Введите идентифицирующее имя (до 32 символов).

Табл. 5-1 Беспроводная связь

ПОЛЕ	ОПИСАНИЕ
Hide ESSID	Выберите **Yes** для того чтобы "спрятать" ESSID, чтобы какая-нибудь станция не могла получить доступ к ESSID пассивным сканированием. Выберите **No** для того чтобы ESSID остался видимым, чтобы станция могла получить доступ к ESSID пассивным сканированием.
Channel ID	Частотный диапазон, использующийся беспроводными устройствами стандарта IEEE 802.11b, называется каналом. Выберите канал из раскрывающегося списка.
RTS/CTS Threshold	Допустимый размер сообщения RTS (количество байтов) для включения квитирования RTS/CTS. Данные с размером кадра больше этой величины будут использоваться для квитирования RTS/CTS. Установка значения этого параметра больше максимального значения MSDU (MAC service data unit) приведет к отключению квитирования RTS/CTS. Установка значения данного параметра равным нулю приведет к отключению квитирования RTS/CTS . Введите значение от 0 до 2432.
Fragmentation Threshold	Допустимые размеры (количество байтов) фрагментации передаваемых сообщений. Это максимальный размер фрагмента данных, который может быть отправлен. Введите значение от 256 до 2432.
WEP Encryption	Процедура WEP (Wired Equivalent Privacy) осуществляет шифрование кадров, передаваемых в беспроводной сети. Выберите **Disable**, что разрешает всем компьютерам беспроводной сети связываться с точками доступа без шифрования. Выберите **64-bit WEP** или **128-bit WEP** для включения криптографической защиты данных.
Key 1 to Key 4	При шифровании данных применяются WEP-ключи. При передаче данных маршрутизатор OMNI ADSL и беспроводные станции должны пользоваться общими WEP-ключами . Если выбрана опция **64-bit WEP**, введите любые 5 ASCII-символов или 10 шестнадцатеричных символов ("0-9", "A-F"). Если выбрана опция **128-bit WEP**, введите любые 13 ASCII-символов или 26 шестнадцатеричных символов ("0-9", "A-F"). Можно установить одновременно четыре ключа, но всякий раз будет использоваться только один из них. Значение ключа по умолчанию равно 1.

Табл. 5-1 Беспроводная связь

ПОЛЕ	ОПИСАНИЕ
Back	Щелкните **Back** для возвращения к главному экрану настройки беспроводной LAN.
Apply	Щелкните по кнопке **Apply (Применить)** для сохранения внесенных изменений.
Cancel	Щелкните по кнопке **Cancel (Отмена)** для возобновления работы по конфигурированию данного экрана.

5.6 Настройка фильтра MAC

Экран фильтра MAC позволяет сделать настройку OMNI ADSL, открывающую/закрывающую (Allow Association/Deny Association) доступ до 32 устройств к ресурсам OMNI ADSL. Каждое устройство Ethernet обладает уникальным MAC-адресом. MAC-адрес присваивается устройству на предприятии-изготовителе и состоит из шести пар шестнадцатеричных символов, например: 00:A0:C5:00:00:02. При настройке с помощью этого экрана необходимо знать MAC-адреса устройства.

Для изменения настроек фильтра MAC устройства OMNI ADSL, щелкните по вкладкам **Wireless LAN**, **MAC Filter**, открывающим доступ к экрану **MAC Filter**. Появится экран следующего вида.

.

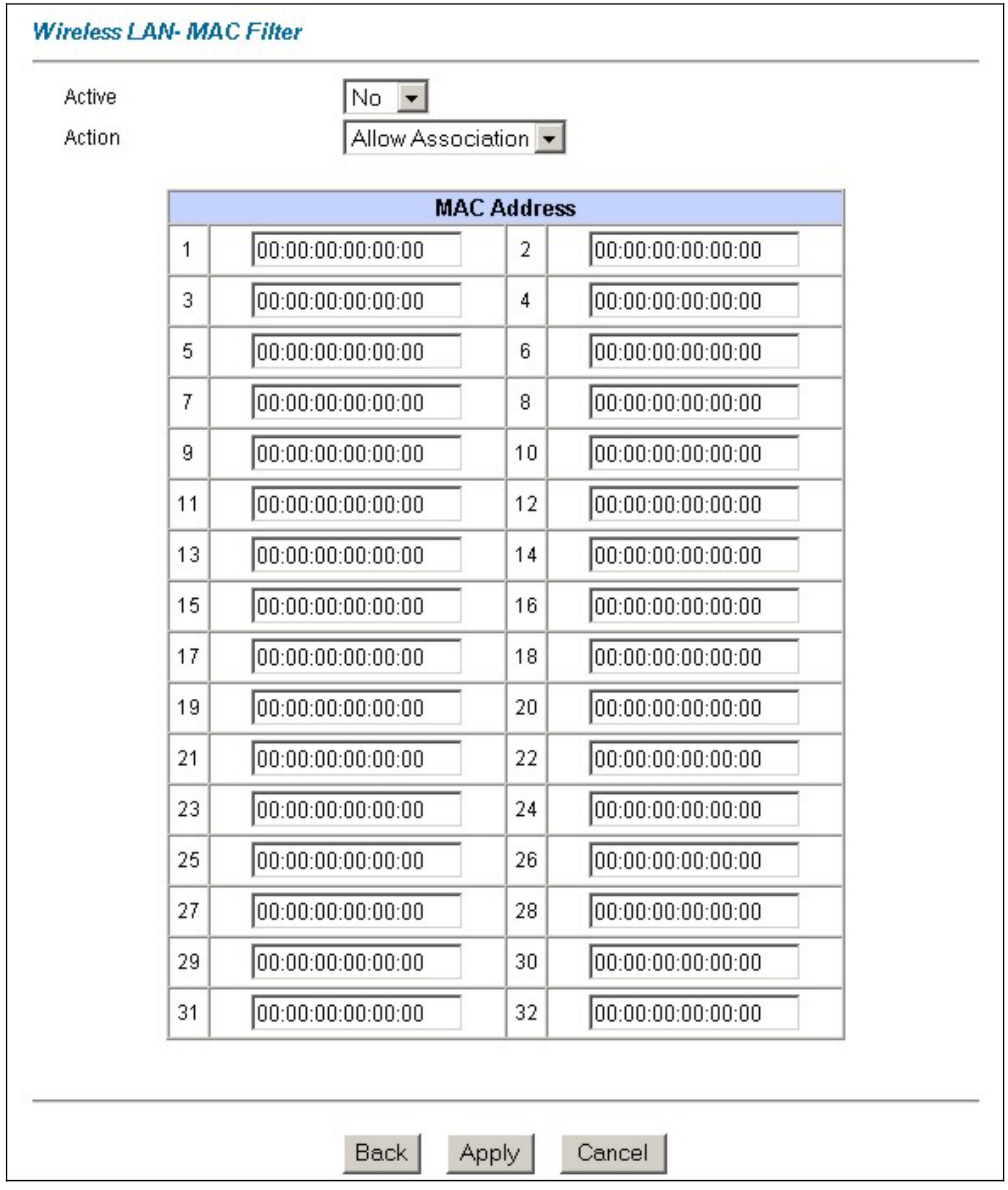


Рис. 5-4 Фильтр MAC-адреса

В следующей таблице приведены описания полей данного экрана.

Табл. 5-2 Фильтр MAC-адреса

ПОЛЕ	ОПИСАНИЕ
Active	Выберите **Yes** в раскрывающемся списке для включения опции фильтрации MAC-адреса.
Action	Выберите действие фильтра применительно к списку MAC-адресов на столе фильтра MAC-адресов. Выберите **Deny Association** для закрытия доступа к маршрутизатору. MAC-адресам, отсутствующим в списке, доступ к маршрутизатору будет разрешен. Выберите Allow **Association** для разрешения доступа к маршрутизатору. MAC-адресам, отсутствующим в списке, доступ к маршрутизатору будет запрещен.
MAC Address	Введите в эти адресные поля значения MAC-адресов (в формате XX:XX:XX:XX:XX:XX) беспроводных станций, которым разрешен или запрещен доступ к ресурсам устройства OMNI ADSL.
Back	Щелкните по **Back (Назад)** для возвращения к главному экран настройки беспроводной LAN.
Apply	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Cancel	Щелкните по **Cancel (Отмена)** для повторной настройки данного экрана.

5.7 Стандарт 802.1x

Стандарт IEEE 802.1x описывает улучшенные методы защиты применительно к аутентификации беспроводных станций и управлению ключами криптографической защиты. Аутентификация может выполняться с использованием локальной базы данных о пользователях сети, являющейся внутренней по отношению к устройству OMNI ADSL (аутентифицируется до 32 пользователей), или внешним RADIUS-сервером (аутентифицируется неограниченное количество пользователей).

5.8 Введение в RADIUS

В основу протокола RADIUS положена модель клиент-сервер, поддерживающая аутентификацию и учет, где точка доступа является клиентом, а сервер - RADIUS-сервером. RADIUS-сервер, наряду с другими, выполняет следующие задачи:

- **Аутентификация**

  Определяет идентичность пользователей.

- **Учет**

  Выполняет функции мониторинга активности клиентов сети.

Использованием службы RADIUS является простой обмен пакетами, в котором OMNI ADSL выступает как ретранслятор сообщений между беспроводной станцией и сетевым RADIUS-сервером.

Виды RADIUS-сообщений

Для аутентификации пользователей в процессе обмена данными между точкой доступа и RADIUS-сервером используются следующие виды сообщений:

- **Access-Request (доступ-запрос)**

  Посылается точкой доступа для запроса на аутентификацию.

- **Access-Reject (доступ-отказ)**

  Посылается RADIUS-сервером с запретом доступа.

- **Access-Accept (доступ-разрешение)**

  Посылается RADIUS-сервером для разрешения доступа.

- **Access-Challenge (доступ-оклик)**

  Посылается RADIUS-сервером с запросом дополнительной информации для разрешения доступа. Точка доступа посылает соответствующий ответ, поступивший от пользователя, и посылает другое сообщение Access-Request.

При обмене данными между точкой доступа и RADIUS-сервером для организации учета работы пользователей применяются следующие виды RADIUS-сообщений:

- **Accounting-Request (учет-запрос)**

  Посылается точкой доступа для запроса данных учета.

- **Accounting-Response (учет-ответ)**

  Посылается RADIUS-сервером для того чтобы показать, что он приступил или завершил выполнение процедур учета.

Для обеспечения защиты сети точка доступа и RADIUS-сервер пользуются общим секретным ключом, в качестве которого используется общий для них пароль. Значение ключа не может передаваться по сети. В дополнение к этому, для защиты сети от несанкционированного доступа, информация о пароле при обмене шифруется.

5.8.1 Описание протокола аутентификации EAP

Протокол EAP (расширенный протокол идентификации) является протоколом аутентификации верхнего транспортного уровня стандарта IEEE802.1x, предназначенного для поддержки множественных видов аутентификации пользователей. Использование протокола EAP точкой доступа при взаимодействии с EAP-совместимым RADIUS-сервером помогает беспроводной станции и RADIUS-серверу при выполнении аутентификации.

Выбор вида аутентификации зависит от характеристик RADIUS-сервера или точки доступа. OMNI ADSL с RADIUS-сервером поддерживает следующие протоколы аутентификации: EAP-TLS, EAP-TTLS и DEAP. См. приложение *Виды аутентификации протокола EAP* для ознакомления с описанием четырех основных видов аутентификации.

Маршрутизатор OMNI ADSL, совместно с RADIUS-сервером и локальной базой данных о пользователях, поддерживает алгоритм MD5 (Message-Digest Algorithm 5) протокола EAP.

На рисунке показано выполнение аутентификации при задании RADIUS-сервера и точки доступа.

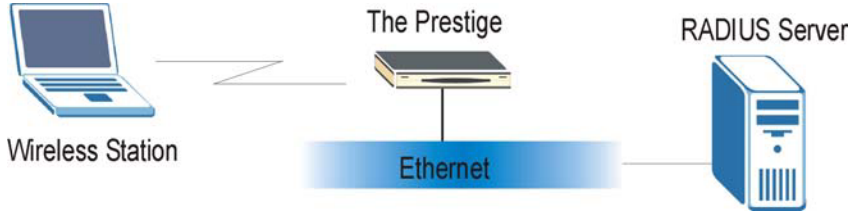


Рис.5-5 Аутентификация с использованием протокола EAP

Ниже приводится более подробное общее описание работы протокола аутентификации EAP стандарта IEEE 802.1x. В качестве примера приведена последовательность операций при выполнении аутентификации с помощью алгоритма EAP-MD5, см. приложение Стандарт IEEE 802.1x.

Step 1. Беспроводная станция посылает в адрес устройства OMNI ADSL сообщение “start”("начало работы").

Step 2. OMNI ADSL отправляет сообщение “request identity”("запрос об идентификации") в адрес беспроводной станции для получения соответствующей информации.

Step 3. Беспроводная станция в ответ передает информацию, необходимую для идентификации, включая имя пользователя и пароль.

Step 4. RADIUS-сервер проверяет данные о пользователе в соответствии с информацией, хранящейся в базе данных настроек пользователя, и принимает решение об аутентификации беспроводной станции.

5.9 Настройка протокола 802.1x

Для изменения настроек аутентификации устройства OMNI ADSL щелкните по **Wireless LAN (Беспроводная ЛВС)**, **802.1x**. Появится экран следующего вида.

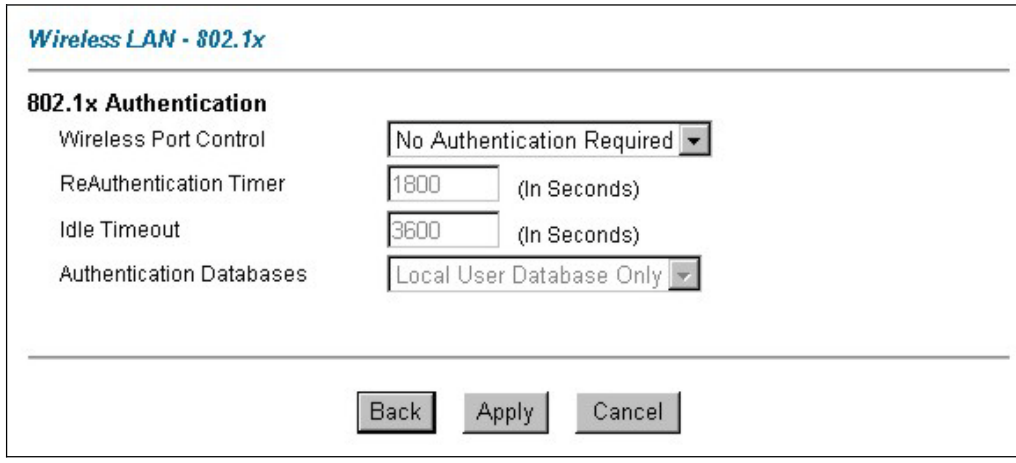


Рис. 5-6 Настройка параметров протокола 802.1x

В следующей таблице приведены описания полей данного экрана.

Табл. 5-3 Настройка параметров протокола 802.1x

ПОЛЕ	ОПИСАНИЕ
Wireless Port Control	Для управления доступом беспроводной станции к проводной сети выберите соответствующий способ управления из раскрывающегося списка. Выберите одну из следующих опций: **No Authentication Required (Аутентификация не требуется)**, **Authentication Required (Требуется аутентификация)** и **No Access Allowed (Доступ не разрешен)**. **No Authentication Required** открывает доступ всем беспроводным станциям к проводной сети без ввода имени пользователя и пароля. Данная установка задается по умолчанию. **Authentication Required** означает, что доступ в проводную сеть разрешен только при предъявлении всеми беспроводными станциями имени пользователя и пароля. **No Access Allowed** закрывает доступ всех беспроводных станций к проводной сети.

Табл. 5-3 Настройка параметров протокола 802.1x

ПОЛЕ	ОПИСАНИЕ
ReAuthentication Timer	Определяет как часто беспроводные станции должны подтверждать имя пользователя и пароль для сохранения подключения. Эти поля будут активизированы только при выборе опции **Authentication Required** в поле **Wireless Port Control**. Введите значение временного интервала от 10 до 9999 секунд. По умолчанию значение временного интервала принимается равным **1800** секунд (30 минут). **Если аутентификация беспроводной станции осуществляется с обращением к RADIUS-серверу, то значение счетчика запросов об аутентификации RADIUS-сервера имеет более высокий приоритет.**
Idle Timeout	OMNI ADSL автоматически производит отключение неработающей беспроводной станции от проводной сети через определенное время . Беспроводной станции необходимо повторно предъявить имя пользователя и пароль для получения разрешения на доступ к проводной сети. Эти поля будут активизированы только при выборе опции **Authentication Required** в поле **Wireless Port Control**. По умолчанию значение временного интервала принимается равным **3600** секунд (1 час).

Табл. 5-3 Настройка параметров протокола 802.1x

ПОЛЕ	ОПИСАНИЕ
Authentication Databases	Эти поля будут активизированы только при выборе опции **Authentication Required** в поле **Wireless Port Control**. База данных аутентификации содержит регистрационные сведения о беспроводных станциях. Локальная база данных о пользователях является встроенной базой данных устройства OMNI ADSL. RADIUS-сервер является для нее внешним. Из раскрывающегося списка следует выбрать, какую базу данных маршрутизатора OMNI ADSL должен использовать (первой) для аутентификации беспроводной станции. Перед определением приоритетности, убедитесь в правильности подключения соответствующей базы данных. Выберите опцию **Local User Database Only (Только локальная база данных о пользователе)** для того чтобы OMNI ADSL выполнил проверку имени пользователя и пароля беспроводной станции, пользуясь только встроенной базой данных о пользователях устройства OMNI ADSL. Выберите опцию **RADIUS Only (Только RADIUS-сервер)** для того, чтобы OMNI ADSL выполнил проверку имени пользователя и пароля беспроводной станции, пользуясь только базой данных о пользователях на указанном RADIUS-сервере. Выберите опцию **Local first, then RADIUS (Вначале локальная БД, а затем БД RADIUS-сервера)** для того, чтобы OMNI ADSL при аутентификации беспроводной станции вначале выполнил проверку, пользуясь своей базой данных. Если имя пользователя в базе данных не обнаружено, то OMNI ADSL приступает к проверке по базе данных на указанном RADIUS-сервере. Выберите опцию **RADIUS first, then Local (Вначале БД RADIUS-сервера, а затем локальной БД)** для того, чтобы OMNI ADSL при аутентификации беспроводной станции вначале выполнил проверку, пользуясь базой данных RADIUS-сервера. Если имя пользователя в базе данных RADIUS-сервера не обнаружено или пароль не совпадает с хранящимся в базе данных RADIUS-сервера, OMNI ADSL не будет обращаться для проверки к локальной базе данных пользователей и аутентификация прерывается. Если RADIUS-сервер недоступен для устройства OMNI ADSL, то он выполняет проверку, пользуясь своей локальной базой данных о пользователях.
Back	Щелкните по **Back (Назад)** для того чтобы вернуться к главному экрану настройки беспроводной LAN.
Apply	Щелкните по **Apply (Применить)** для сохранения данных настроек маршрутизатора Presige.

Табл. 5-3 Настройка параметров протокола 802.1x

ПОЛЕ	ОПИСАНИЕ
Cancel	Щелкните по кнопке **Cancel (Отмена)** для возобновления работы по конфигурированию данного экрана.

5.10 Настройка параметров аутентификации пользователя ЛВС

Организация хранения сведений о настройках пользователя в ЛВС позволяет устройству OMNI ADSL выполнять аутентификацию без обращения к RADIUS-серверу. Однако число пользователей, которые могут быть идентифицированы таким образом, ограничено.

Для внесения изменений в записях локальной базы данных о пользователях устройства OMNI ADSL щелкните по вкладке **Wireless LAN**, **Local User Database**. Появится экран следующего вида.

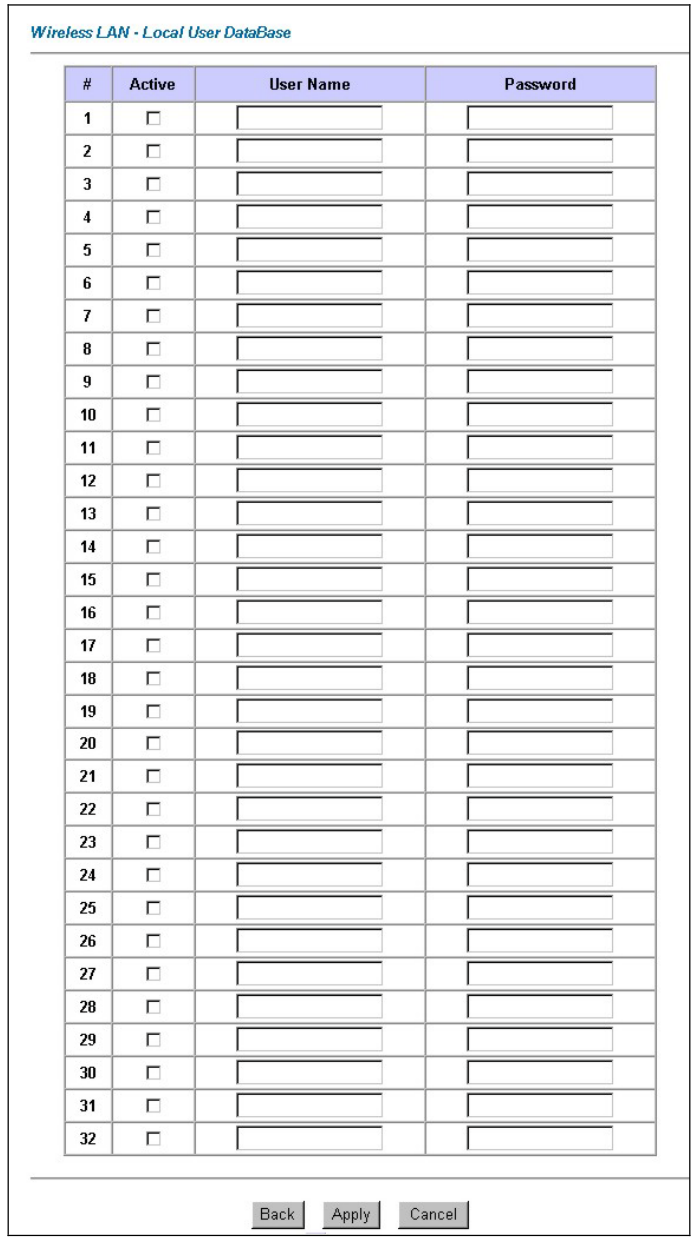


Рис. 5-7 Локальная база данных о пользователях

В следующей таблице приведены описания полей данного экрана.

Табл. 5-4 Локальная база данных о пользователях

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер локальной учетной записи пользователя.
Active	Поставьте метку в этом окошке для отображения параметров пользователя.
User Name	Введите имя пользователя, использующееся в его параметрах.
Password	Введите пароль (до 31 символа), использующийся в его параметрах.
Back	Щелкните **Back** для того чтобы вернуться к главному экрану настройки беспроводной LAN.
Apply	Щелкните по кнопке **Apply (Применить)** для сохранения введенных параметров в устройстве Presige.
Cancel	Щелкните по кнопке **Cancel (Отмена)** для возобновления работы по конфигурированию данного экрана.

5.11 Настройка RADIUS-сервера

Поскольку была установлена опция EAP authentication (аутентификация с использованием протокола EAP), необходимо указать внешний сервер, который будет выполнять аутентификацию и вести учет работы удаленных пользователей.

Для установки настроек RADIUS-серверов в устройстве OMNI ADSL щелкните по **WIRELESS LAN**, **RADIUS**. Появится экран следующего вида.

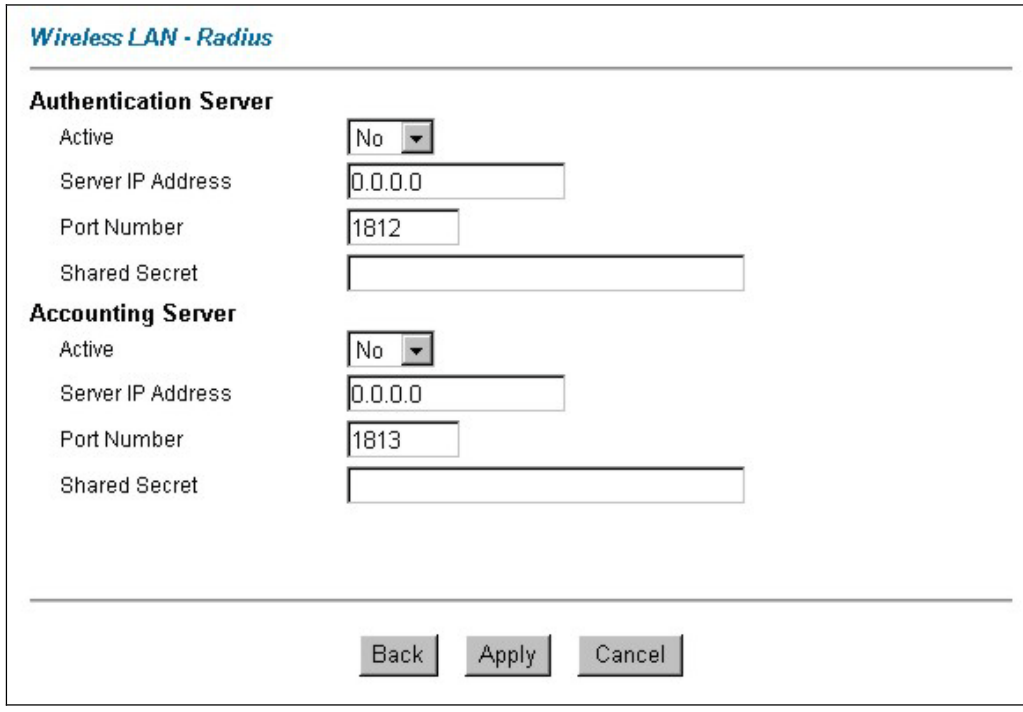


Рис. 5-8 Настройка установок RADIUS-сервера

В следующей таблице приведены описания полей данного экрана.

Табл. 5-5 Настройка установок RADIUS-сервера

ПОЛЕ	ОПИСАНИЕ
Authentication Server (Сервер аутентификации)	
Active	Выберите опцию **Yes** из раскрывающегося списка для включения процедуры аутентификации пользователя с помощью внешнего сервера аутентификации.
Server IP Address	Введите в десятичном виде с разделительными точками IP-адрес внешнего сервера аутентификации.

Табл. 5-5 Настройка установок RADIUS-сервера

ПОЛЕ	ОПИСАНИЕ
Port Number	По умолчанию номер порта RADIUS-сервера аутентификации принимается равным **1812**. Не следует менять этот параметр без получения дополнительных инструкции и необходимой информации у Вашего системного администратора.
Shared Secret	Введите пароль (до 31 буквенно-цифровых символа), который будет использоваться как общий ключ внешним сервером аутентификации и точкой доступа. Значение ключа не может передаваться по сети.Значение ключа должно быть одинаковым для внешнего сервера аутентификации и устройства OMNI ADSL.
Accounting Server (Сервер учета работы пользователей)	
Active	Выберите опцию **Yes** из раскрывающегося списка для включения процедуры аутентификации пользователя с помощью внешнего сервера учета работы пользователей.
Server IP Address	Введите в десятичном виде с разделительными точками IP-адрес внешнего сервера учета работы пользователей.
Port Number	По умолчанию номер порта RADIUS-сервера учета работы пользователей принимается равным **1813**. Не следует менять этот параметр без получения дополнительных инструкции и необходимой информации у Вашего системного администратора.
Shared Secret	Введите пароль (до 31 буквенно-цифровых символа), который будет использоваться как общий ключ внешним сервером учета работы пользователей и точкой доступа. Значение ключа не может передаваться по сети. Значение ключа должно быть одинаковым для внешнего сервера учета работы пользователей и устройства OMNI ADSL.
Back	Щелкните по **Back (Назад)** для возвращения к главному экрану настройки беспроводной LAN.
Apply	Щелкните по **Apply (Применить)** для сохранения данных настроек устройства Presige.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возобновления работы по конфигурированию данного экрана.

Chapter 6
Настройка подключения к глобальной сети

В этой главе описывается процесс настройки подключения к глобальной сети.

6.1 Описание подключения к глобальной сети

Под подключением к глобальной сети подразумевается подключение к любой другой сети или к сети Интернет.

См. главу *Мастер-программа установки* для получения дополнительной информации о полях экрана WAN.

6.2 Инкапсуляция PPPoE

OMNI ADSL поддерживает протокол PPPoE (Point-to-Point Protocol over Ethernet, протокол PPP через Ethernet). PPPoE - это проект стандарта IETF (RFC 2516), регламентирующий порядок взаимообмена персонального компьютера (PC) с широкополосным модемом (при DSL, кабельном, беспроводном и др. способах подключения). Опция **PPPoE** используется применительно к коммутируемому соединению с использованием протокола PPPoE.

Для провайдера услуг PPPoE предлагает доступ и метод аутентификации, подходящий для существующих систем управления доступом (например, RADIUS). Пользователю предлагается способ регистрации и аутентификации, поддерживаемый программным обеспечением для удаленного доступа к сети компании Microsoft, поэтому для пользователей Windows не требуется изучения какой-либо дополнительной информации.

Одним из преимуществ PPPoE является то, что он открывает возможность доступа к нескольким службам сети. Этот вид сервиса известен как, так называемый, динамический выбор обслуживания. Это позволяет провайдеру услуг легко создавать и предоставлять конкретным пользователям новые услуги IP.

С точки зрения функционирования, PPPoE значительно экономит усилия, прилагаемые как с Вашей стороны, так и со стороны Интернет-провайдера или оператора связи, так как не требует специальной настройки широкополосного модема пользователя.

В случае установки PPPoE непосредственно в маршрутизаторе OMNI ADSL (а не на отдельных компьютерах), компьютеры локальной сети не требуют установки программного обеспечения PPPoE,

поскольку эта часть задачи выполняется OMNI ADSL. К тому же, при наличии трансляции сетевых адресов (NAT) доступ будут иметь все компьютеры локальной сети.

6.3 Инкапсуляция PPTP

Протокол туннелирования между узлами (Point-to-Point Tunneling Protocol, PPTP) - сетевой протокол, обеспечивающий безопасную передачу данных от удаленного клиента частному серверу, создавая Виртуальную частную сеть (VPN) при использовании сети на базе TCP/IP

Протокол PPTP обеспечивает возможность создания сетей с функцией on-demand, мультипротокольных и виртуальных частных сетей через такие общедоступные сети, как Интернет.

6.4 Формирование трафика

Функция формирования трафика представляет собой соглашение между владельцем сети и абонентом, предназначенное для регулировки средней скорости и "пульсации", или колебаний скорости передачи данных через сеть ATM. Данное соглашение помогает устранить перегрузку каналов, что важно для передачи данных в реальном времени, напр., аудио- и видеоданных.

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

Поддерживаемая скорость ячеек (SCR) - это средняя скорость ячеек при пульсирующем трафике по принципу "включено-выключено", а также один из параметров пульсирующего трафика. Скорость SCR не может превышать скорость PCR. В системе по умолчанию принимается значение - 0 ячеек/с.

Под максимальным размером пакета (MBS) подразумевается максимальное количество ячеек, которое может быть отправлен со скоростью PCR. После того как объем переданных данных достигнет MBS, скорость передачи ячеек уменьшается ниже значения SCR пока средняя скорость передачи вновь не станет равной SCR. В течение этого времени также можно будет передавать большее количество ячеек (до MBS) на скорости PCR.

Если значение PCR, SCR или MBS установлено по умолчанию на "0", то система назначит максимальное значение, коррелирующее со скоростью передачи данных на линии.

Следующая схема иллюстрирует взаимосвязь, существующую между PCR, SCR и MBS.

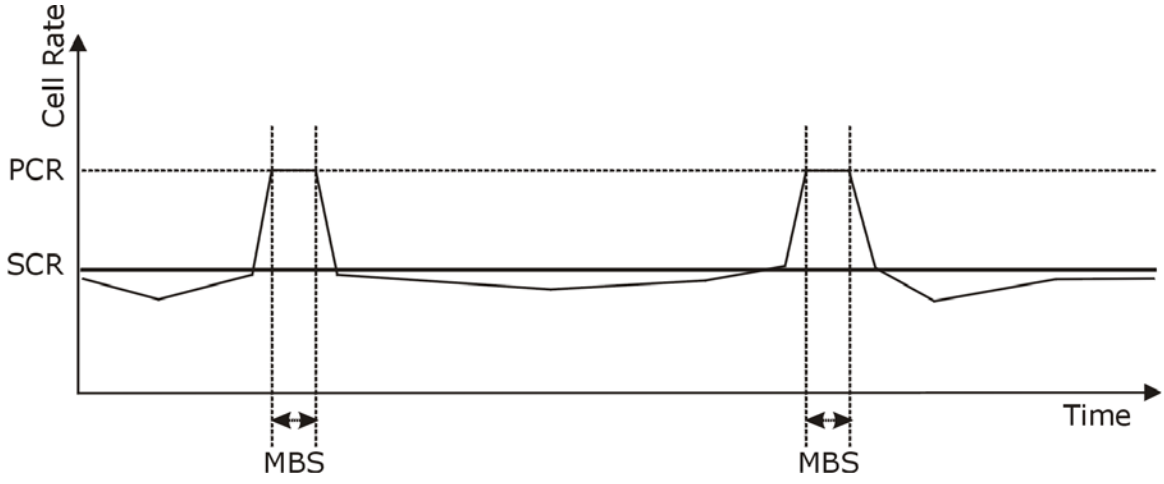


Рис. 6-1 Пример формирования трафика

6.5 Задание установок подключения к глобальной сети

Для изменения настроек подключения OMNI ADSL к удаленным узлам глобальной сети щелкните закладку **WAN (Глобальная вычислительная сеть)**. Вид экрана зависит от типа инкапсуляции.

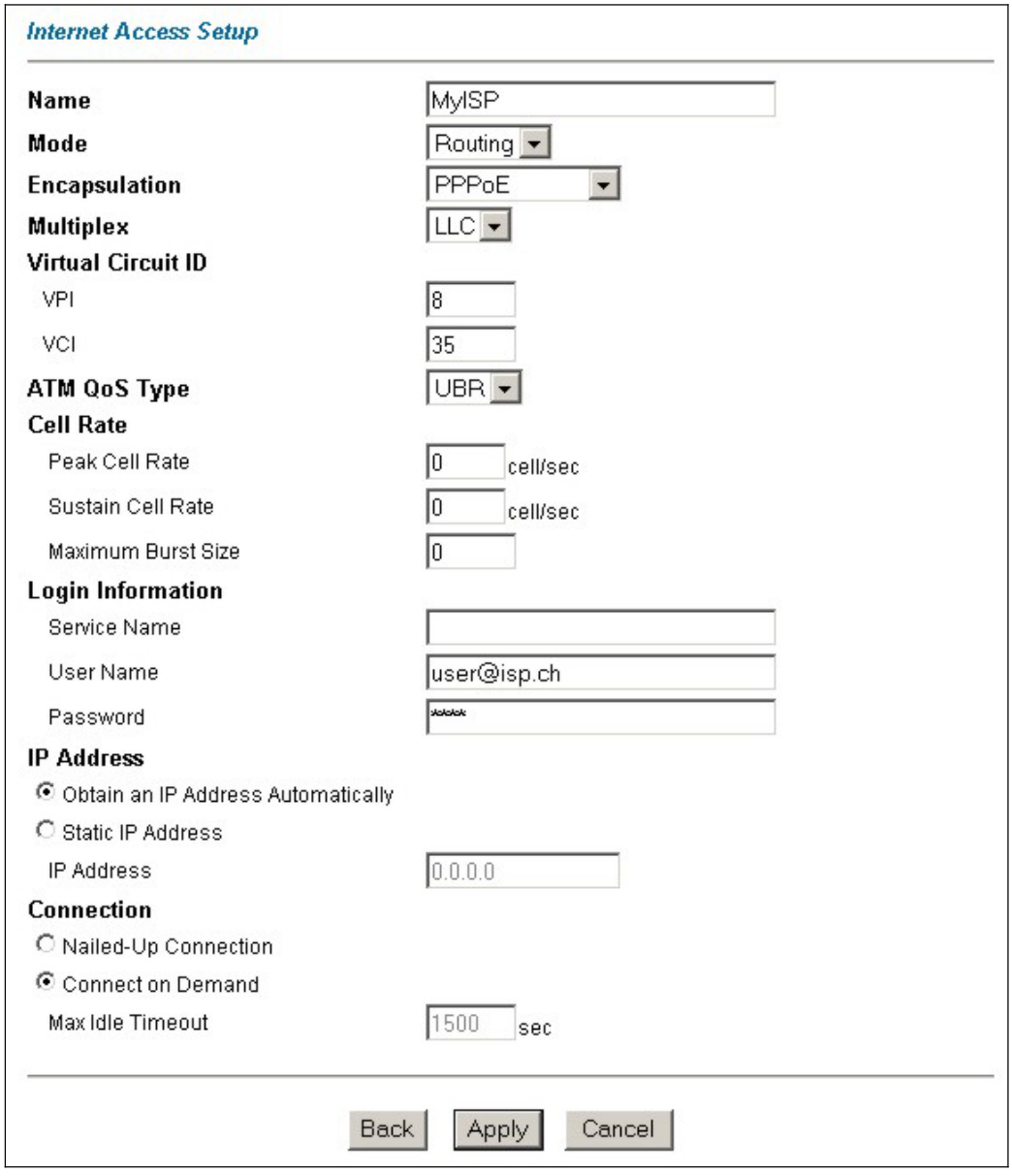


Рис. 6-2 Настройка доступа в Интернет

В следующей таблице приведены описания полей данного экрана.

Табл. 6-1 Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя Интернет-провайдера, например, MyISP. Эти сведения необходимы только в целях идентификации.
Mode	Выберите опцию **Routing (Маршрутизация)** (по умолчанию) из раскрывающегося списка, если Ваш Интернет-провайдер разрешает пользоваться одной учетной записью нескольким пользователям. В противном случае выберете **Bridge (Мост)**.
Encapsulation	Выберите способ инкапсуляции, использующийся Вашим Интернет-провайдером из раскрывающегося списка. Выбор зависит от режима установленного в поле **Mode**. Если выбрана опция **Bridge** в поле **Mode**, выберите также **PPPoA** или **RFC 1483**. Если выбрана опция **Routing** в поле **Mode**, выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
Multiplex	Выберите способ мультиплексирования, использующийся Вашим Интернет-провайдером из раскрывающегося списка. Выберите **VC** или **LLC**.
Virtual Circuit ID	Идентификаторы виртуального пути (VPI) и виртуального канала (VCI) определяют виртуальную цепь. См. дополнительную информацию в Приложении.
VPI	Допустимый диапазон значений VPI - от 0 до 255. Введите присвоенное значение VPI.
VCI	Допустимый диапазон значений для VCI - от 32 до 65535 (значения от 0 до 31 зарезервированы для задач локального управления трафиком ячеек ATM). Введите присвоенное значение идентификатора VCI.
ATM QoS Type	Выберите опцию **CBR** (Continuous Bit Rate) при назначении фиксированной (в режиме постоянного доступа) полосы частот для передачи потока голосовых сообщений или потока данных. Выберите опцию **UBR** (Unspecified Bit Rate) для приложений не столь чувствительным к временным ограничениям, таким как электронная почта. Выберите опцию **VBR** (Variable Bit Rate) для передачи потока пакетов данных, когда данная полоса частот используется также другими приложениями. Опция **VBR** имеется не во всех моделях.

Табл. 6-1 Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ
Cell Rate	Установка значения скорости передачи ячеек часто помогает установить перегрузку трафика, что отрицательно сказывается на скорости передачи данных реального времени, таких как аудио и видео данные.
Peak Cell Rate	Для определения значения пиковой скорости ячеек (PCR) разделите скорость передачи в линии DSL (бит/с) на 424 (размер ячейки ATM). Это будет максимальная скорость, с которой отправитель может передавать ячейки. Наберите это значение PCR.
Sustain Cell Rate	Значение поддерживаемой скорости ячеек (SCR) устанавливает среднюю скорость передачи ячеек (в течение длительного времени). Введите величину SCR (она должна быть меньше PCR).
Maximum Burst Size	Максимальный размер пакта (MBS) означает максимальное количество ячеек, которые могут быть переданы с пиковой скоростью. Ввести MBS (должно быть меньше 65535).
Login Information	(только при инкапсуляции PPPoA и PPPoE encapsulation)
Service Name	(только применительно к протоколу PPPoE) Наберите в этом поле имя вашей службы PPPoE.
User Name	Введите присвоенное Интернет-провайдером имя пользователя. Если присвоенное имя имеет вид user@domain , где имя домена является идентификатором служебного имени, то введите без ошибок имена обоих компонентов адреса.
Password	Введите пароль, присвоенный данному имени пользователя (см. выше).
IP Address	Статический IP-адрес представляет собой фиксированный IP-адрес, предоставленный Интернет-провайдером. Динамический IP-адрес не фиксирован. Он назначается каждый раз при подключении к сети Интернет. Параметры учетной записи отдельного пользователя могут использоваться как в динамическом, так и в статическом IP-адресе. Если используется динамический IP-адрес, щелкните по кнопке **Obtain an IP address automatically (Автоматическое получение IP-адреса).** В противном случае, щелкните по **Static IP Address (Статический IP-адрес)** и наберите присвоенный Интернет-провайдером IP-адрес в окне **IP Address (IP-адрес)** внизу.

Табл. 6-1 Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ
Connection (только при инкапсуляции PPPoA и PPPoE)	Правило(-а) SMT меню 26 имеет(-ют) более высокий приоритет по отношению к параметрам настройки пользователя **Connection (Соединение)** .
Nailed-Up Connection	Выберите опцию **Nailed-Up Connection (Полупостоянное соединение)** , если необходимо иметь постоянное подключение к сети. В случае отключения от сети OMNI ADSL постарается автоматически восстановить соединение.
Connect on Demand	При отсутствии необходимости иметь постоянное подключение к сети Интернет выберите опцию **Connect on Demand (Подключение по требованию)**, и укажите время ожидания (в секундах) в поле **Max. Idle Timeout (Тайм-аут простоя).**
Max Idle Timeout	Укажите значение тайм-аута простоя в поле **Max Idle Timeout** , если выбрана опция **Connect on Demand**. По умолчанию задается "0", что означает отсутствие ограничений по продолжительности сеанса связи в сети Интернет.
Subnet Mask (только при инкапсуляции ENET ENCAP)	Введите код маски подсети в десятичном виде с разделительными точками. См. приложение *IP Subnetting (IP-протоколы организации подсетей)* для вычисления кода маски подсети, если у Вас используется организация подсетей.
ENET ENCAP Gateway (только при инкапсуляции ENET ENCAP)	Необходимо указать IP-адрес шлюза (поддерживаемый Вашим Интернет-провайдером), если выбрана опция **ENET ENCAP** в поле **Encapsulation**.
Back	Щелкните по **Back (Назад)**для возвращения к предыдущему экрану.
Apply	Щелкните по кнопке **Apply** для сохранения изменений настройки.
Cancel	Щелкните по кнопке **Cancel (Отмена)** для повторной настройки данного экрана.

Part III:

NAT(трансляция сетевых адресов), динамический DNS (сервер доменных имен) и часовой пояс

В этой части руководства рассматриваются вопросы настройки службы трансляции сетевых адресов (NAT), динамического сервера доменных имен (Dynamic DNS) и установки часового пояса.

Chapter 7
Трансляция сетевых адресов (NAT)

В данной главе описано, как выполнить настройку службы трансляции сетевых адресов (NAT) устройства OMNI ADSL.

7.1 Описание службы NAT

NAT (трансляция сетевых адресов - Network Address Translation, RFC 1631) - это трансляция IP-адреса хоста в пакете, например, трансляция адреса источника исходящего пакета, который используется в одной сети, в иной IP-адрес для другой сети.

7.1.1 Определения NAT

Inside/outside (внутренний/внешний) указывает на местонахождение хоста относительно OMNI ADSL, например, рабочие станции абонентов являются внутренними узлами, а web-сервера в Интернете - внешними.

Global/local (глобальный/локальный) указывает IP-адрес хоста в пакете при прохождении пакета через маршрутизатор, например, локальный адрес относится к IP-адресу узла при прохождении пакета внутри локальной сети, соответственно глобальный адрес означает IP-адрес того же узла при прохождении того же пакета в глобальной сети.

Следует отметить, что inside/outside относится к позиции хоста, а global/local к его IP-адресу, который используется в пакете. Таким образом, внутренний локальный адрес (ILA) - это IP-адрес внутреннего узла в пакете при пересылке пакета внутри локальной сети, а внутренний глобальный адрес (IGA) - это IP-адрес того же внутреннего узла при нахождении пакета уже в глобальной сети. В следующей таблице представлена данная информация в сжатом виде.

Табл. 7-1 Определения NAT

ПАРАМЕТР	ОПИСАНИЕ
Inside	Означает хост в локальной сети.
Outside	Означает хост в глобальной сети.
Local	Относится к адресу пакета (источника или пункта назначения) при пересылке пакета внутри локальной сети.
Global	Относится к адресу пакета (источника или пункта назначения) при пересылке пакета внутри глобальной сети.

NAT не изменяет IP-адрес (локальный или глобальный) внешнего **хоста**.

7.1.2 Назначение трансляции сетевых адресов

Говоря простыми словами, NAT изменяет IP-адрес источника в пакете, принимаемом от абонента (внутренний локальный адрес) на другой (внутренний глобальный адрес) до того как передать этот пакет далее в глобальную сеть. При получении ответа NAT транслирует адрес назначения (внутренний глобальный адрес) обратно во внутренний локальный адрес, перед тем как пакет будет передан на исходный внутренний хост. Отметим, что IP-адрес (локальный или глобальный) внешнего хоста не меняется.

Глобальный IP-адрес для внутренних хостов может быть как статически, так и динамически присвоен Интернет-провайдером. Кроме того, можно назначить серверы, например, web-сервер и сервер Telnet в вашей локальной сети и сделать их доступными для внешних пользователей. При отсутствии назначенных серверов OMNI ADSL будет фильтровать все входящие запросы, препятствуя, таким образом, попыткам несанкционированного доступа в вашу сеть. Дополнительные сведения о трансляции IP-адресов см. в *RFC 1631*, "Транслятор сетевых IP-адресов *(NAT)*".

7.1.3 Как работает NAT

Каждый пакет имеет два адреса – адрес источника и адрес назначения. Для исходящих пакетов значение ILA (внутреннего локального адреса) является адресом в ЛВС, а значение IGA (внутреннего глобального адреса) - адресом источника в глобальной вычислительной сети. Для входящих пакетов значение ILA является адресом назначения в ЛВС, а значение IGA - адресом назначения в глобальной вычислительной сети. Служба NAT преобразует частные (локальные) IP-адреса в уникальные адреса глобальной сети, необходимые для связи с хостами в других сетях. Таким образом, происходит замена оригинального IP-адреса источника (а также номер порта источника TCP или UDP при преобразовании типа Many-to-One и Many-to-Many Overload) в каждом пакете и затем передача его в Интернет. OMNI ADSL отслеживает первоначальные адреса и номера портов, поэтому входящие ответные пакеты получают восстановленные значения. Это иллюстрирует следующий рисунок.

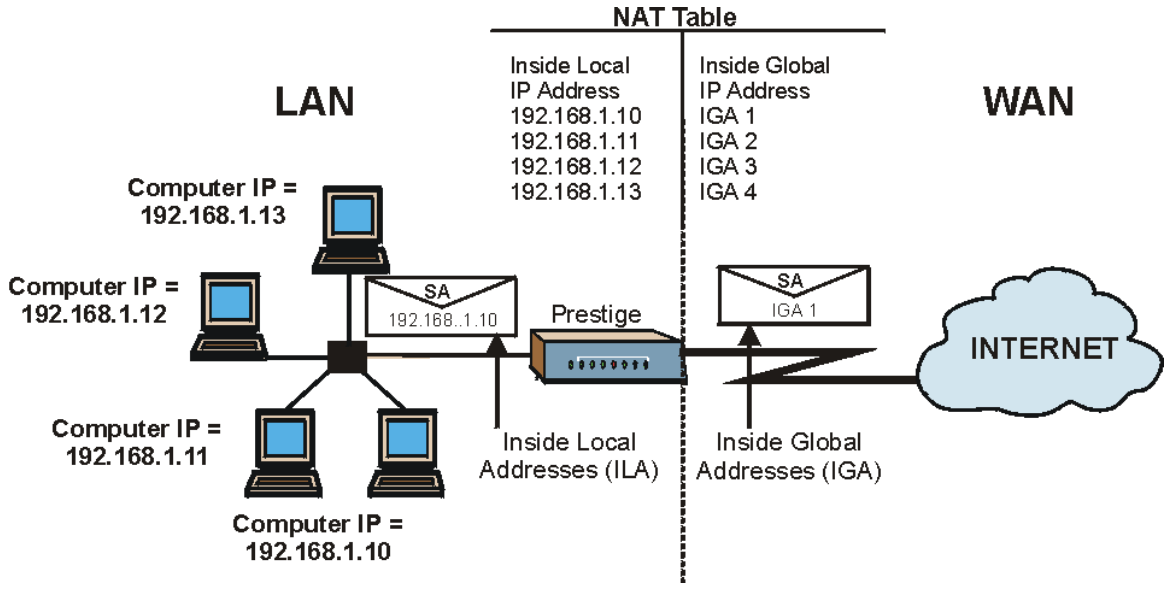


Рис 7-1 Как работает NAT

7.1.4 Пример трансляции сетевых адресов

На следующем рисунке показано возможное использование трансляции сетевых адресов в ситуации, когда три внутренних локальных сети (логические локальные сети, использующие псевдоним IP) через OMNI ADSL могут связываться с тремя отдельными глобальными сетями. Другие примеры даны в конце этой главы.

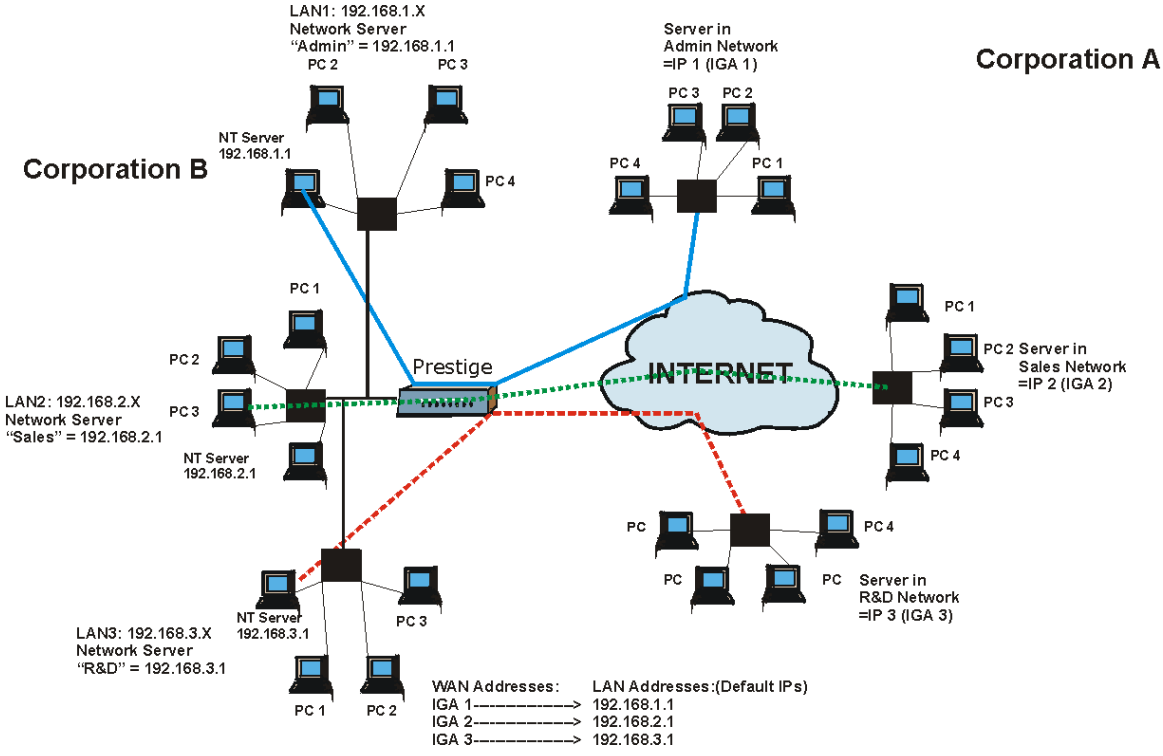


Рис 7-2 Трансляция сетевых адресов в случае псевдонимов IP

7.1.5 Типы преобразования сетевых адресов

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

1. **One to One (Один-в-один)**: В этом режиме OMNI ADSL преобразует один локальный IP-адрес в один глобальный IP-адрес.
2. **Many to One (Много-в-один)**: В этом режиме OMNI ADSL преобразует несколько локальных IP-адресов в один глобальный IP-адрес. Это эквивалентно SUA (т.е. PAT - трансляция адреса порта), функции "получение счета одиночного пользователя", разработанной корпорацией ZyXEL, которая поддерживалась предыдущими версиями маршрутизаторов ZyXEL (в нынешних версиях соответствует функции **SUA Only**).
3. **Many to Many Overload:** В этом режиме OMNI ADSL преобразует несколько локальных IP-адресов в коллективные глобальные IP-адреса.

4. **Many-to-Many No Overload**: В этом режиме OMNI ADSL преобразует каждый локальный IP-адрес в уникальный глобальный IP-адрес.
5. **Server (Сервер)**: Этот режим позволяет назначить внутренние серверы различного типа в обход NAT и открыть к ним доступ со стороны внешнего мира.

При использовании типов преобразования One-to-One **и** Many-to-Many No Overload **номера портов** не **меняются.**

В следующей таблице даны все типы преобразования.

Табл. 7-2 Типы преобразования сетевых адресов

ТИП	ПРЕОБРАЗОВАНИЕ IP	СОКРАЩЕНИЕ В SMT
One-to-One	ILA1←→ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M:1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M:M Ov
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M:M No OV
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server (Сервер)

7.2 Сравнение режимов SUA (Счет одиночного пользователя) и NAT

SUA (Single User Account, Счет одиночного пользователя) является реализацией ZyNOS подмножества NAT, которая поддерживает два типа преобразования, **Many-to-One** и **Server**. OMNI ADSL также поддерживает трансляцию типа **Full Feature** - преобразование нескольких глобальных

IP-адресов в несколько частных IP-адресов клиентов и серверов в локальной сети, использующих варианты преобразования согласно *Табл. 7-2*.

1. **Если OMNI ADSL имеет только один общедоступный IP-адрес в глобальной сети, выбрать режим** SUA Only**.**
2. **Если OMNI ADSL имеет несколько общедоступных IP-адресов в глобальной сети, выбрать** Full Feature**.**

7.3 Сервер SUA

Набор серверов SUA - это список внутренних (за NAT в локальной сети) серверов, например, web или FTP, к которым можно открыть доступ со стороны внешнего мира притом, что благодаря серверу SUA вся внутренняя сеть воспринимается внешним миром как один компьютер.

Можно задать один номер порта или диапазон номеров для пересылки и локальный IP-адрес требуемого сервера. Номер порта идентифицирует услугу; например, подключение к сервису глобальной сети осуществляется через порт 80, а к сервису FTP через порт 21. В некоторых случаях, таких как доступ к неизвестным службам или когда один сервер может поддерживать несколько видов сервиса (например, FTP и Web-услуги), было бы лучше указать диапазон значений номеров портов. Можно назначить IP-адрес сервера, соответствующий номеру порта или диапазону номеров портов.

Часто местные Интернет-провайдеры широкополосного доступа не разрешают своим пользователям предоставлять серверное обслуживание (например, Web или FTP). Ваш Интернет-провайдер может периодически проверять наличие серверов и приостанавливать обслуживание при нахождении активных услуг с Вашей стороны. За уточнениями обращайтесь к Вашему Интернет-провайдеру.

IP-адрес сервера принятый по умолчанию

В дополнение к функциям заданных серверов, NAT поддерживает по умолчанию IP адрес сервера. Сервер, назначенный по умолчанию, принимает пакеты через порты, не заданные в этом экране.

Если вами не задан IP-адрес сервера по умолчанию, то все пакеты, полученные через порты не заданные в этом экране, будут сброшены.

7.3.1 Переадресация порта: услуги и номера портов

Набор серверов NAT - это список внутренних (за NAT в локальной сети) серверов, например, web или FTP, к которым можно открыть доступ со стороны внешнего мира притом, что благодаря NAT вся внутренняя сеть воспринимается внешним миром как один компьютер.

Для пересылки входящих запросов на обслуживание серверу (серверам) локальной сети используется страница **SUA Server**. Можно ввести один или несколько номеров портов для пересылки и локальный IP-адрес выбранного сервера. Номер порта идентифицирует услугу; например, подключение к сервису глобальной сети осуществляется через порт 80, а к сервису FTP - через порт 21. В некоторых

случаях, таких как доступ к неизвестным службам или когда один сервер может поддерживать несколько видов сервиса (например, FTP и Web-услуги), было бы лучше указать диапазон значений номеров портов.

В дополнение к функциям заданных серверов, NAT поддерживает функцию сервера по умолчанию. Запрос на услугу, для которой не существует явным образом определенного сервера, пересылается на сервер по умолчанию. Если сервер по умолчанию не определен, запрос на услугу просто сбрасывается.

Часто местные Интернет-провайдеры широкополосного доступа не разрешают своим пользователям предоставлять серверное обслуживание (например, Web или FTP). Интернет-провайдер может периодически проверять наличие серверов и приостанавливать обслуживание при нахождении активных услуг с Вашей стороны. За уточнениями обращайтесь к Вашему Интернет-провайдеру.

В следующей таблице приведены наиболее часто используемые номера портов. Дополнительную информацию по номерам портов можно получить в RFC 1700.

Табл. 7-3 Услуги и номера портов

УСЛУГИ	НОМЕР ПОРТА
ECHO	7
FTP (Протокол передачи файлов)	21
SMTP (Простой протокол пересылки почты)	25
DNS (Служба доменных имен)	53
Finger	79
HTTP (Протокол передачи гипертекста или WWW, Web)	80
POP3 (Почтовый протокол)	110
NNTP (Сетевой протокол передачи новостей)	119
SNMP (Простой протокол управления сетью SNMP)	161
Прерывание SNMP	162

Табл. 7-3 Услуги и номера портов

УСЛУГИ	НОМЕР ПОРТА
PPTP (Туннельный протокол "точка-точка")	1723

7.3.2 Конфигурирование серверов за SUA (пример)

Пусть необходимо назначить порты 22-25 одному серверу, порт 80 другому, а по умолчанию назначить IP-адрес сервера 192.168.1.35, как показано на следующем рисунке.

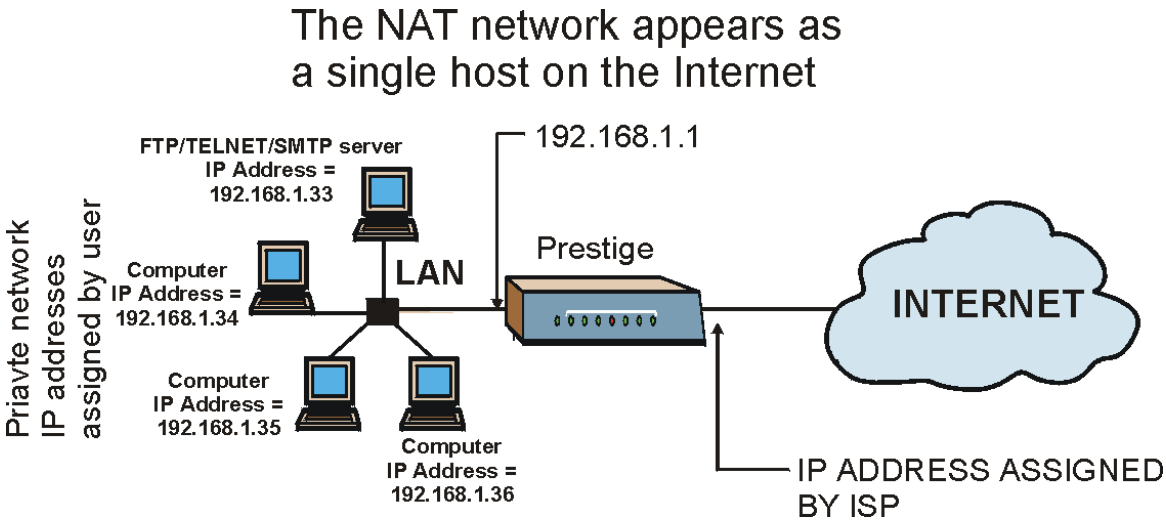


Рис. 7-3 Пример работы нескольких серверов за NAT

7.4 Выбор режима NAT

Щелкните **NAT** для инициализации следующего экрана.

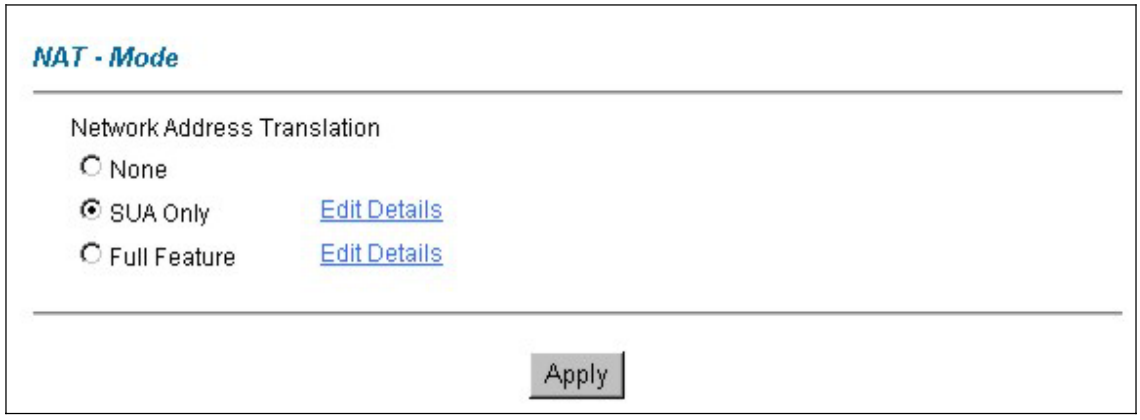


Рис. 7-4 Режим NAT

В следующей таблице приведены описания полей данного экрана.

Табл. 7-4 Режим NAT

ПОЛЕ	ОПИСАНИЕ
None	Выберите эту кнопку для отключения NAT.
SUA Only	Выберите эту кнопку, если имеется хотя бы один общедоступный IP-адрес в глобальной сети для устройства OMNI ADSL. В OMNI ADSL используется набор преобразования адресов 1 для экрана **NAT - Edit SUA/NAT Server Set**.
Edit Details	Щелкните по этой ссылке для перехода к экрану **NAT - Edit SUA/NAT Server Set**.
Full Feature	Выберите эту кнопку, если имеется несколько общедоступных IP-адресов в глобальной сети для устройства OMNI ADSL.
Edit Details	Щелкните по этой ссылке для перехода к экрану **NAT - Address Mapping Rules** .
Apply	Щелкните **Apply** для сохранения конфигурации.

7.5 Конфигурирование сервера SUA

Если не был назначен ни один IP-адрес в наборе серверов 1 (сервер по умолчанию), то все пакеты, полученные через порты не заданные в этом экране, будут сброшены.

Щелкните **NAT**, выберите **SUA Only** и щелкните **Edit Details** для того чтобы открыть следующий экран.

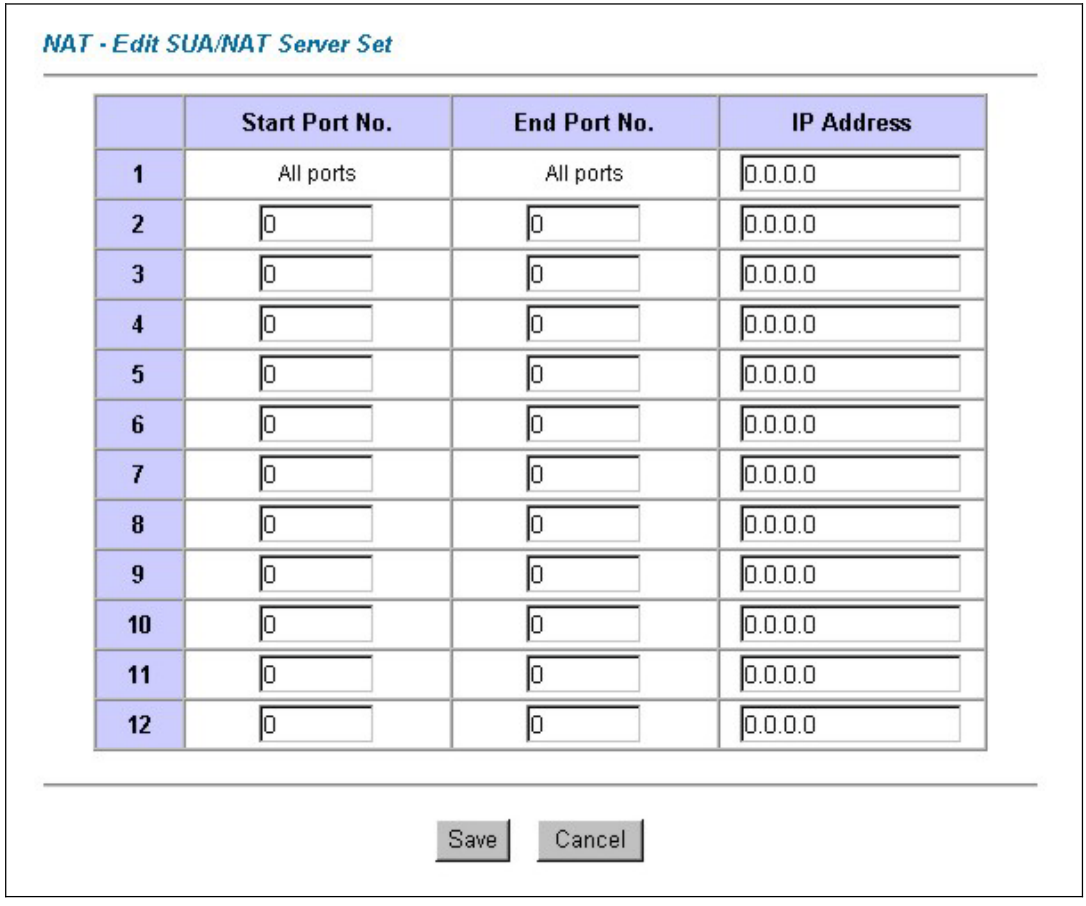


Рис. 7-5 Редактирование набора серверов SUA/NAT

В следующей таблице приведены описания полей данного экрана.

Табл. 7-5 Редактирование набора серверов SUA/NAT

ПОЛЕ	ОПИСАНИЕ
Start Port No.	Введите в это поле номер порта. Для переадресации только одного порта, введите его же в поле **End Port No.**. Для переадресации серии портов введите в этом поле номер начального порта и номер конечного порта в поле **End Port No.**.

Табл. 7-5 Редактирование набора серверов SUA/NAT

ПОЛЕ	ОПИСАНИЕ
End Port No.	Введите в это поле номер порта. Для переадресации только одного порта, введите его же в предыдущее поле **Start Port No.**, а затем введите его в этом поле. Для переадресации серии портов введите номер последнего порта в серии, который начинается с номера порта в предыдущем поле **Start Port No.**.
IP Address	Введите в этом поле IP-адрес Вашего сервера.
Save	Щелкните по кнопке Save **(Сохранить)** для сохранения внесенных изменений.
Cancel	Щелкните **Cancel (Отмена)** для возврата к предыдущей конфигурации.

7.6 Конфигурирование преобразования адресов

Задание очередности правил необходимо, т.к. OMNI ADSL применяет эти правила в порядке, определенном пользователем. При нахождении правила, удовлетворяющего текущему пакету, Presige выполняет соответствующее действие, при этом остальные правила игнорируются. Если перед очередным заданным правилом имеются пустые, то это правило сдвигается на соответствующее количество пустых номеров. Например, если в текущем наборе уже заданы правила с 1 по 6 и необходимо задать правило под номером 9. На экране новое правило будет под номером 7, а не 9. Теперь, если исключить правило под номером 4, правила с номерами от 5 до 7 будут "подняты", так что старые правила 5, 6 и 7 станут новыми правилами 4, 5 и 6.

Для изменения установок переадресования маршрутизатора OMNI ADSL, щелкните **NAT**, выберите **Full Feature** и щелкните **Edit Details** для вызова следующего экрана.

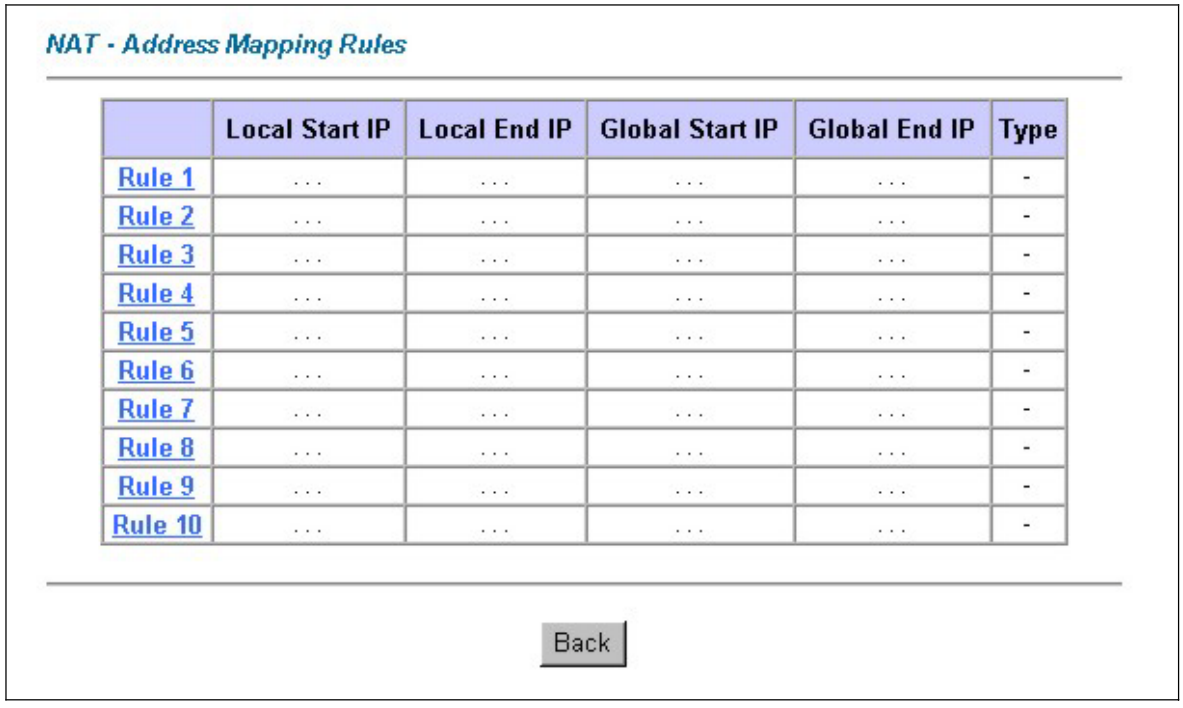


Рис. 7-6 Правила преобразования адресов

В следующей таблице приведены описания полей данного экрана.

Табл. 7-6 Правила преобразования адресов

ПОЛЕ	ОПИСАНИЕ
Local Start IP	Начальный внутренний локальный IP-адрес (ILA). Локальные IP-адреса являются **недоступными** при **распределении портов** сервера.
Local End IP	Конечный внутренний локальный IP-адрес (ILA). Если ваше правило распространяется на все локальные IP-адреса, то введите 0.0.0.0 как **локальный начальный IP-адрес** и 255.255.255.255 как **локальный конечный IP-адрес**. Данное поле является недоступным (**N/A**) для преобразований типа **One-to-One** и **Server**.
Global Start IP	Начальный внутренний глобальный IP-адрес (IGA). Введите в поле код 0.0.0.0, если имеется динамический IP-адрес, назначенный Интернет-провайдером. Это возможно только применительно к преобразованиям типа **Many-to-One** и **Server**.

Табл. 7-6 Правила преобразования адресов

ПОЛЕ	ОПИСАНИЕ
Global End IP	Конечный внутренний глобальный IP-адрес (IGA). Это поле недоступно (**N/A**) для типов преобразования **One-to-One**, **Many-to-One** и **Server**.
Type	**1-1**: В режиме One-to-One локальный IP-адрес преобразовывается в глобальный IP-адрес. Следует отметить, что номера портов не изменяются при преобразовании сетевых адресов типа One-to-one. **M-1**: В режиме Many-to-one несколько локальных IP-адресов преобразовывается в один глобальный IP-адрес, что эквивалентно SUA (т.е. PAT - преобразованию адресов портов) и функциональной возможности получения счета одиночного пользователя, которая поддерживалась только предыдущими моделями маршрутизаторов компании ZyXEL. **M-M Ov** (Overload): В режиме Many-to-Many Overload несколько локальных IP-адресов преобразуются в коллективные глобальные IP-адреса. **MM No** (No Overload): В режиме Many-to-Many No Overload каждый локальный IP-адрес преобразуется в уникальный глобальный IP-адрес. **Server (Сервер)**: Этот режим позволяет назначить внутренние серверы различного типа в обход NAT и открыть к ним доступ со стороны внешнего мира.
Back	Щелкните по **Back (Назад)**для возвращения к экрану **NAT Mode**.

7.7 Редактирование правила преобразования адресов

Для того чтобы отредактировать какое-либо правило преобразования адресов, щелкните соответствующую ссылку на экране **NAT Правила преобразования адресов** для вызова экрана следующего типа.

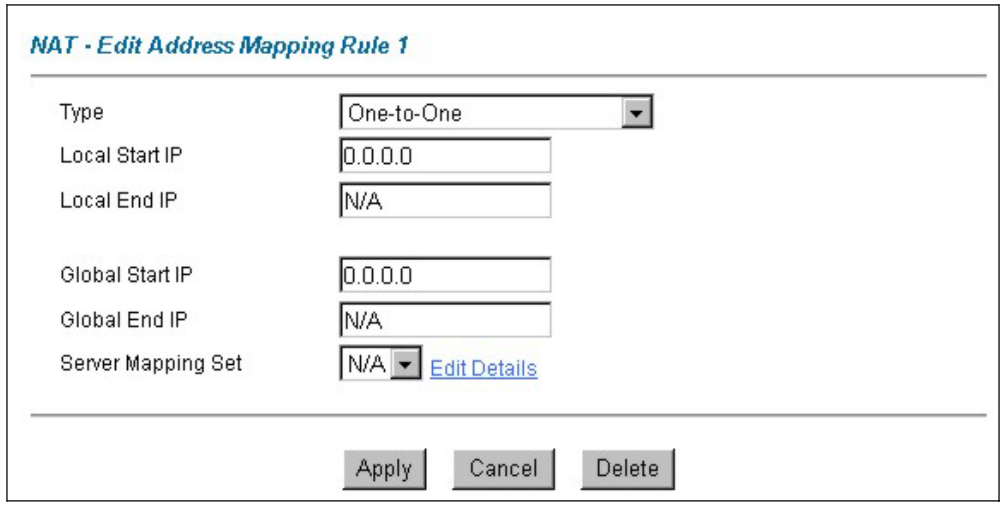


Рис. 7-7 Редактирование правила преобразования адресов

В следующей таблице приведены описания полей данного экрана.

Табл. 7-7 Редактирование правила преобразования адресов

ПОЛЕ	ОПИСАНИЕ
Type	Выберите один из следующих типов распределения портов. 1. **One-to-One**: В режиме One-to-One локальный IP-адрес преобразовывается в глобальный IP-адрес. Следует отметить, что номера портов не изменяются при преобразовании сетевых адресов типа One-to-One. 2. **Many-to-One**: В режиме Many-to-One несколько локальных IP-адресов преобразовывается в один глобальный IP-адрес, что эквивалентно SUA (т.е. PAT - преобразованию адресов портов) и функциональной возможности получения счета одиночного пользователя, которая поддерживалась предыдущими моделями маршрутизаторов компании ZyXEL. 3. **Many-to-Many Overload**: В режиме Many-to-Many Overload несколько локальных IP-адресов преобразуются в коллективные глобальные IP-адреса. 4. **Many-to-Many No Overload**: В режиме Many-to-Many No Overload каждый локальный IP-адрес преобразуется в уникальный глобальный IP-адрес. 5. **Server**: Этот режим позволяет назначить внутренние серверы различного типа в обход NAT и открыть к ним доступ со стороны внешнего мира.
Local Start IP	Начальный локальный IP-адрес (ILA). Локальные IP-адреса являются **недоступными** при **распределении портов** сервера.

Local End IP	Конечный локальный IP-адрес (ILA). Если Ваше правило распространяется на все локальные IP-адреса, то введите 0.0.0.0 как **локальный начальный IP-адрес** и 255.255.255.255 как **локальный конечный IP-адрес**. Данное поле является недоступным (**N/A**) для преобразования типа **One-to-One** и **Server**.
Global Start IP	Начальный глобальный IP-адрес (IGA). Введите в это поле код 0.0.0.0, если у вас имеется присвоенный Интернет-провайдером динамический IP-адрес.
Global End IP	Конечный глобальный IP-адрес (IGA). Это поле недоступно (**N/A**) для типов преобразования **One-to-One**, **Many-to-One** и **Server**.
Server Mapping Set (Настройка набора серверов)	Возможно только когда **Type** установлен в **Server**. Выберите число от 1 до 10 из раскрывающегося списка для выбора набора серверов на экране **NAT - Address Mapping Rules**.
Edit Details (Редактирование элементов)	Щелкните по этой ссылке для перехода к экрану **NAT - Edit SUA/NAT Server Set** для редактирования набора серверов, который был выбран в поле **Server Mapping Set**.
Apply	Щелкните по кнопке **Apply (Применить)** для сохранения внесенных изменений.
Отмена	Щелкните по кнопке **Cancel (Отмена)** для возвращения к ранее сохраненным настройкам.
Удалить	Щелкните по кнопке **Delete (Удалить)** для выхода из экрана без сохранения настроек.

Chapter 8
Настройка динамического сервера доменных имен

В этой главе обсуждается как сконфигурировать OMNI ADSL для работы с динамическим сервером доменных имен (динамическим DNS).

8.1 Динамический DNS

Динамический DNS позволяет выполнять обновление текущих динамических адресов с помощью одной из многих служб динамических DNS, для того чтобы любой мог Вас отыскать (в NetMeeting, CU-SeeMe и т.п.). Доступ к FTP-серверу или web-сайту с вашего компьютера возможен также при использовании DNS-подобных адресов (например, myhost.dhs.org, где myhost - имя по вашему выбору), которые остаются постоянными, вместо IP-адреса, который меняется каждый раз при следующем подключении. Ваши друзья и близкие всегда смогут вас найти, не зная Вашего IP-адреса.

Прежде всего необходимо зарегистрировать учетную запись динамического DNS на сайте www.dyndns.org. Это относится к пользователям, получившим динамический IP-адрес со своего ISP или DHCP-сервера и тем не менее желающим иметь имя домена. Провайдер выдает пароль или ключ.

8.1.1 Шаблон подстановки DYNDNS

Если использовать шаблон подстановки в имени Вашего хоста, то имени *.yourhost.dyndns.org будет соответствовать тот же IP-адрес, что и yourhost.dyndns.org. Данная функция полезна, например, в случае когда необходимо использовать имя www.yourhost.dyndns.org и при этом иметь доступным имя Вашего хоста.

Если используется частный IP-адрес глобальной сети, использование динамического DNS невозможно.

8.2 Конфигурирование динамического DNS

Для изменения настроек работы OMNI ADSL с динамическим DNS щелкните **Dynamic DNS**. Появится следующий экран.

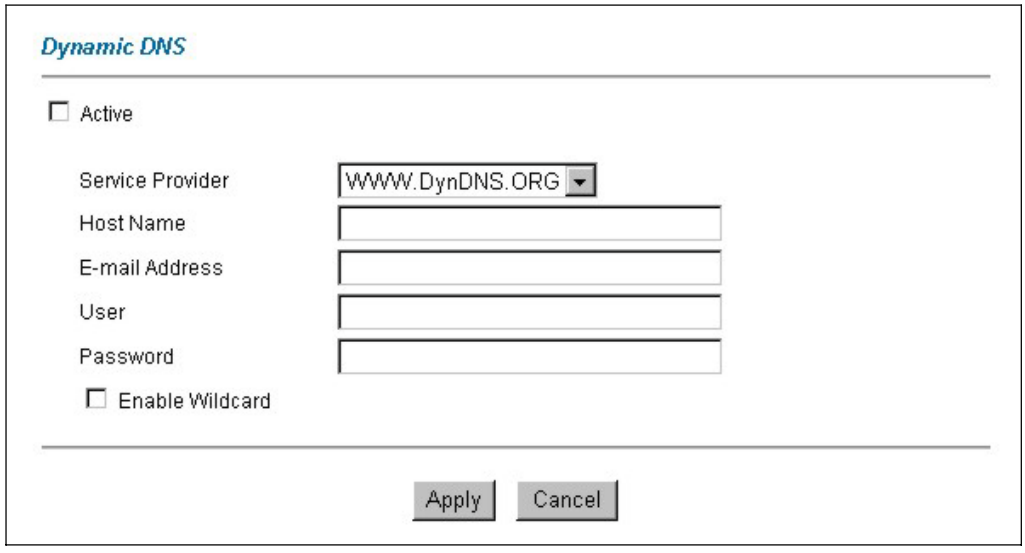


Рис. 8-1 Динамический DNS

В следующей таблице приведены описания полей данного экрана.

Табл. 8-1 Динамический DNS

ПОЛЕ	ОПИСАНИЕ
Active (Активно)	Поставьте отметку в этом окошке для работы с динамическим DNS.
Service Provider (Провайдер услуг)	Выберите имя Вашего провайдера услуг динамических DNS.
Host Name (Имя хоста)	Введите имя домена, присвоенное устройству OMNI ADSL провайдером динамической DNS.
E-mail Address (Адрес электронной почты)	Введите адрес Вашей электронной почты.
User (Пользователь)	Введите имя пользователя.
Password (Пароль)	Введите присвоенный Вам пароль.

Табл. 8-1 Динамический DNS

ПОЛЕ	ОПИСАНИЕ
Enable Wildcard (Разрешить групповой символ)	Поставьте отметку в этом окошке для включения DYNDNS Wildcard.
Apply (Применить)	Щелкните по кнопке **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возвращения к ранее сохраненным настройкам.

Chapter 9
Установка времени и даты

Для задания установок времени и даты в устройстве OMNI ADSL пользуйтесь данным экраном. Эта глава относится не ко всем моделям Presige.

9.1 Настройка параметров часового пояса

Для изменения настроек времени и даты в Pestige щелкните по**Time Zone (Часовой пояс)** (или **Time and Data (Время и дата**). Появится экран следующего вида. Для выставления времени в устройстве OMNI ADSL в соответствии с местным часовым поясом необходимо пользоваться следующим экраном.

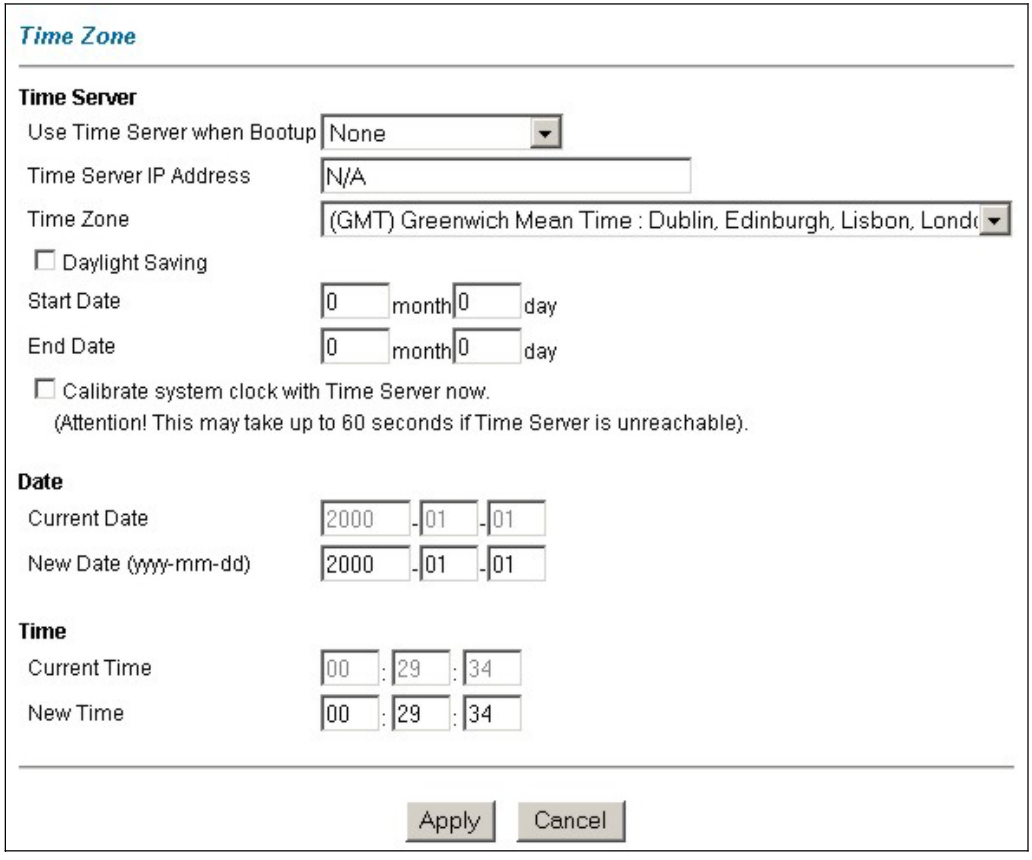


Рис. 9-1 Время и дата

В следующей таблице приведены описания полей данного экрана.

Табл. 9-1 Время и дата

ПОЛЕ	ОПИСАНИЕ
Time Server (Сервер точного времени)	

Табл. 9-1 Время и дата

ПОЛЕ	ОПИСАНИЕ
Use Time Server when Bootup (or Use Protocol when Bootup) (Использовать сервер точного времени при загрузке или использовать при загрузке протокола)	Использовать сервисный протокол, посылаемый сервером времени, при включении OMNI ADSL. Серверы могут поддерживать не все протоколы все время, поэтому необходимо обратиться к Интернет-провайдеру/сетевому администратору или методом подбора найти работающий протокол. Основным отличием между протоколами является используемый формат. Формат **Daytime (RFC 867)** - это формат вида день/месяц/год/часовой пояс сервера. В формате **Time (RFC 868)** отображается 4-байтовое целое число, представляющее собой суммарное время в секундах, начиная с 00.00 1 января 1970 г. По умолчанию используется формат **NTP (RFC 1305),** аналогичный формату времени (RFC 868). Выберите **None** для выставления времени и даты вручную.
Time Server IP Address (or IP Address or URL) (IP-адрес сервера точного времени или IP-адрес или URL)	Введите IP-адрес сервера времени. Если не располагаете точной информацией, следует обратиться к Интернет-провайдеру или системному администратору.
Time Zone (or Time and Date) (Часовой пояс или Время и дата)	Выберите местный часовой пояс. Это позволит установить расхождение во времени между местным часовым поясом и Гринвичским временем (GMT).
Daylight Savings	Выберите эту опцию, если пользуетесь летним временем. Летнее время - период поздней весны-ранней осени, когда во многих странах стрелки часов переводятся на час вперед, чтобы добавить час светлого времени суток.
Start Date (Дата начала)	Введите месяц и день перехода на летнее время, если выбрана опция **Daylight Savings**.
End Date (Дата окончания)	Введите месяц и день перехода на летнее время, если выбрана опция **Daylight Savings**.

Табл. 9-1 Время и дата

ПОЛЕ	ОПИСАНИЕ
Calibrate/Synchronize system clock with Time Server now (Сверка/синхронизация внутреннего системного времени с сервером точного времени)	Щелкните по этой кнопке для того чтобы OMNI ADSL мог подключиться к серверу времени (который был сконфигурирован перед этим) для выставления часов внутреннего системного времени. Пожалуйста, подождите (до 60 секунд) пока OMNI ADSL завершит поиск сервера точного времени. Если он не может отыскать сервер точного времени, пожалуйста, проверьте настройку протокола сервера времени и его IP-адрес. Если IP-адрес был введен правильно, постарайтесь выполнить проверку соединения с ним, например, эхо-тестированием.
Date (Дата)	
Current Date (Текущая дата)	В этом поле отображается дата, установленная в устройстве OMNI ADSL. Всякий раз при загрузке этой страницы OMNI ADSL выполняет проверку синхронизации времени с сервером времени.
New Date (yyyy-mm-dd)	В этом поле отображается дата последнего обновления с обращением к серверу времени. Если выбрана опция **None** в поле **Use Time Server when Bootup**, введите в нем новую дату, а затем щелкните кнопку **Apply**.
Time (Время)	
Current time (Текущее время)	В этом поле отображается дата, установленная в устройстве OMNI ADSL. Всякий раз при загрузке этой страницы OMNI ADSL выполняет проверку синхронизации времени с сервером времени.
New Time (Новое время)	В этом поле отображается время последнего обновления с обращением к серверу времени. Если выбрана опция **None** в поле **Use Time Server when Bootup**, введите в нем новое время, а затем щелкните кнопку **Apply (Применить)**.
Apply	Щелкните по кнопке **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возвращения к ранее сохраненным настройкам.

Part IV:

Межсетевой экран и контент-фильтр

В данной части приводится общее описание типов межсетевых экранов и межсетевого экрана OMNI ADSL в частности, а также дается объяснение порядка выбора услуг и сетевых регистрационных журналов и приводятся примеры правил настройки межсетевого экрана и контент-фильтров.

Chapter 10
Межсетевые экраны

В данной главе приводится необходимая информация о межсетевых экранах и представляется межсетевой экран устройства OMNI ADSL. Содержание данной главы относится к моделям OMNI ADSL LAN H/HW и OMNI ADSL LAN H-E.

10.1 Описание межсетевого экрана

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

10.2 Типы

Существует три основных типа межсетевых экранов:

1. Межсетевые экраны с фильтрацией пакетов
2. Межсетевые экраны прикладного уровня
3. Межсетевые экраны с инспекцией пакетов с учетом состояния

10.2.1 Межсетевые экраны с фильтрацией пакетов

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

10.2.2 Межсетевые экраны прикладного уровня

Межсетевые экраны прикладного уровня ограничивают доступ, выступая в качестве агентов для внешних серверов. В связи с тем, что они используют программы, написанные для конкретных услуг

Интернет, таких как HTTP, FTP и telnet, они могут инспектировать пакеты на предмет достоверности прикладных данных. У шлюзов прикладного уровня имеется рад преимуществ общего характера, по сравнению с режимом (по умолчанию) разрешения передачи прикладного трафика непосредственно к внутренним хост-машинам:

i. Функция намеренного сокрытия информации не позволяет внешним системам получить имена внутренних хостов через DNS, так как шлюз прикладного уровня - единственный хост, имя которого должно быть известно внешним системам.

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

10.2.3 Межсетевые экраны с инспекцией пакетов с учетом состояния

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

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

10.3 Введение в описание межсетевого экрана ZyXEL

Межсетевой экран маршрутизатора OMNI ADSL относится к типу экранов с инспекцией пакетов с учетом состояния и разработан для защиты от атак типа Denial of Service (отказ от обслуживания) с активацией из меню SMT 21.2 или с помощью web-конфигуратора. Задача межсетевого экрана OMNI ADSL - обеспечить безопасное подключение частной локальной сети (LAN) к сети Интернет. OMNI ADSL также можно использовать для предотвращения несанкционированного копирования, уничтожения или видоизменения данных или журнальных событий, что может быть важно с точки зрения безопасности локальной сети. OMNI ADSL также обладает возможностями фильтрации пакетов.

OMNI ADSL устанавливается между ЛВС и глобальной сетью Internet. Это позволяет ему выступать в качестве защитного шлюза для данных, пересылаемых из локальной сети в Интернет и наоборот.

В устройстве OMNI ADSL имеется один порт ISDN и один порт ЛВС Ethernet, которые физически разделяют сеть на две области.

- Порт ISDN подключен к глобальной сети Интернет.
- Порт (локальной сети) подключается к компьютерной сети, для которой необходимо обеспечить защиту от внешнего мира. Компьютеры сети будут иметь доступ к Интернет-услугам, таким как электронная почта, FTP, и WWW. Тем не менее, "входящий доступ" (возможность пересылки информации из сети Интернет во внутреннюю сеть системы) не будет разрешена до тех пор, пока не будет выполнена настройка дистанционного управления или не созданы правила работы межсетевого экрана, позволяющие удаленному хосту пользоваться определенным видом сервиса.

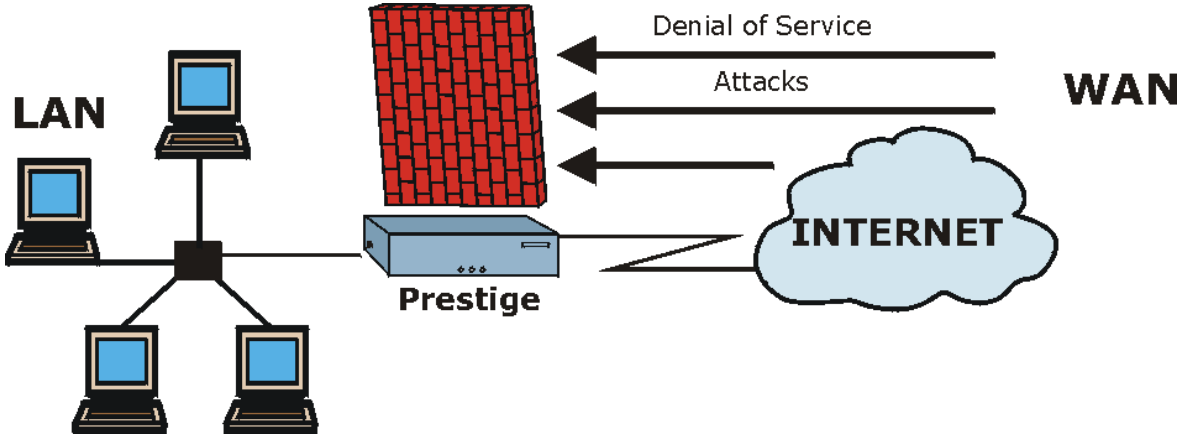


Рис. 10-1 Применение межсетевого экрана маршрутизатора OMNI ADSL

10.4 Отказ от обслуживания

Атаки типа Denials of Service (DoS, отказ от обслуживания) направлены на устройства и сети, подключаемые к Интернету. Эти атаки предназначены не для несанкционированного получения информации, а имеют своей целью вывести из строя какое-либо устройство или сеть, таким образом лишая пользователя дальнейшего доступа к ресурсам сети. Предварительные настройки устройства OMNI ADSL выполнены таким образом, чтобы автоматически распознавать и пресекать все известные атаки типа DoS.

10.4.1 Первичные сведения

Компьютеры получают доступ к информации по сети Интернет, благодаря использованию общего языка, получившего название TCP/IP. В свою очередь, TCP/IP, представляет собой набор прикладных протоколов, предназначенных для выполнения определенных функций. “Добавочный номер”, называющийся "порт TCP" или "порт UDP" идентифицирует эти протоколы, такие как HTTP (Web), FTP (протокол передачи данных), POP3 (E-Mail) и т.д. Например, для Web-трафика по умолчанию используется порт TCP 80.

При взаимодействии компьютеров в Интернете используется модель клиент-сервер, в которой сервер "прослушивает" через конкретный порт TCP/UDP запросы на информацию, поступающие от удаленных клиентских компьютеров сети. Например, web-сервер, обычно, "слушает" порт 80. Следует отметить, что хотя компьютером по назначению используется один порт, такой как порт 80 для подключения к глобальной сети, другие порты также являются активными. Недостаточная тщательность человека, осуществляющего настройку и управление данным компьютером, делает возможной атаку хакера через незащищенный порт.

Некоторые общие порты IP:

Табл. 10-1 Общие порты IP

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

10.4.2 Типы атак DoS

Существуют четыре категории атак типа DoS:

1. Атаки, использующие недостатки реализации TCP/IP.
2. Атаки, использующие слабые места спецификации TCP/IP.
3. "Лобовые" атаки, наполняющие сеть бесполезными данными.
4. IP Spoofing.

1. Атаки "**Ping of Death**" и "**Teardrop**" используют недостатки реализации TCP/IP на различных компьютерных и хост-системах.

1-a Атака Ping of Death использует утилиту эхо-тестирования ("ping") для создания IP-пакета, превышающего максимальный размер в 65,536 байт, разрешенный спецификацией IP. Пакет большого размера посылается в систему, что вызывает ее отказ, зависание или перезагрузку.

1-b Атака вида Teardrop использует слабости повторного восстановления пакета IP из фрагментов. При передаче данных в сети IP-пакеты разбиваются на более мелкие фрагменты. Каждый фрагмент выглядит как первоначальный пакет IP, но содержит поле смещения, несущее информацию, например, о том, что "Данный фрагмент несет байты с 200 по 400 первоначального (нефрагментированного) пакета IP." Программа Teardrop создает серию IP-фрагментов с перекрывающимися полями смещения. Когда при достижении адресата пакет восстанавливается из фрагментов, это может привести к остановке, зависанию и перезагрузке системы.

2. Слабости спецификации TCP/IP могут пропустить атаки "**SYN Flood**" и "**LAND**". Эти атаки происходят во время получения подтверждения об установлении связи (квитирования), которое инициирует сеанс связи между двумя приложениями.

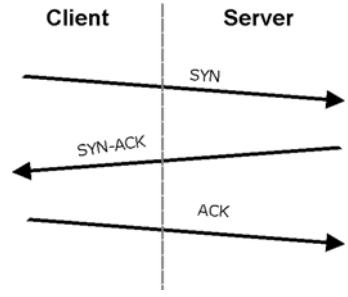


Рис. 10-2 Трехстороннее квитирование

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

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

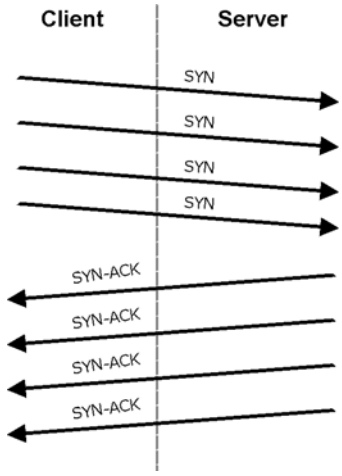


Рис. 10-3 SYN Flood

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

3. Атака типа **"грубая сила"**, например "Smurf", использует особенность спецификации IP, известную как направленная рассылка или циркулярная рассылка для подсети, для того, чтобы затопить атакуемую сеть бесполезными данными. Хакер, использующий этот вид атаки, затопляет маршрутизатор пакетами - эхо-запросами протокола ICMP (протокол управляющих сообщений в сети Интернет). Так как IP-адрес назначения каждого пакета является broadcast-адресом сети, маршрутизатор рассылает такой пакет ICMP всем хостам сети. Если хост-машин много, это приводит к большому объему трафика состоящего из запросов и откликов эха ICMP. Если хакер меняет фальшивые IP-адреса источника эхо-запроса ICMP, то в результате трафик ICMP переполнит не только сеть -"посредник", но и сеть-"жертву". Такое затопление широковещательным трафиком использует весь имеющийся ресурс пропускной способности, делая связь с системой недоступной.

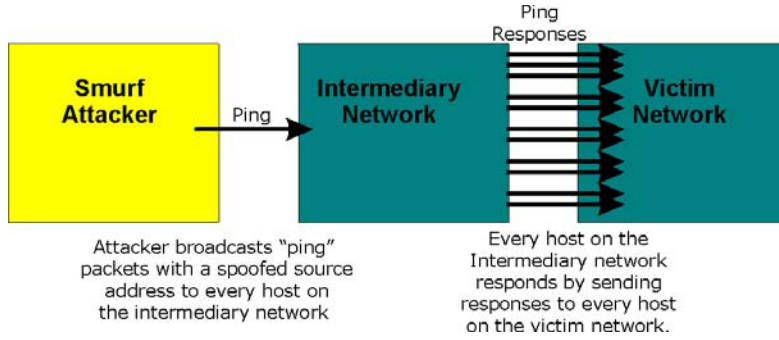


Рис. 10-4 Атака Smurf

- Уязвимость ICMP

Протокол ICMP является протоколом, который выдает сообщение об обнаруженных ошибках и работает совместно с протоколом IP. Имеются следующие команды ICMP, генерирующие предупреждения:

Табл. 10-2 Команды ICMP, генерирующие предупреждения

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Недопустимые команды (NetBIOS и SMTP)

Ниже даны единственные разрешенные команды NetBIOS - все остальные недопустимы.

Табл. 10-3 Допустимые команды NetBIOS

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:

KEEPALIVE:

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

Табл. 10-4 Допустимые команды SMTP

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

- Traceroute

Traceroute - это утилита, предназначенная для определения маршрута, проходимого пакетом между двумя конечными точками. Иногда, при некорректной установке межсетевого экрана, у хакера появляется возможность проследить, как экран собирает сведения о топологии сети, находящейся за ним.

4. Часто атаки DoS включают в себя способ, известный как "**IP Spoofing**" (подмена IP). IP Spoofing может использоваться с целью проникновения в системы, для исключения возможности идентифицировать хакера или увеличения эффекта атаки DoS. IP Spoofing применяется для получения несанкционированного доступа к компьютерам путем создания ситуации, когда межсетевой экран или маршрутизатор получают информацию о том, что обмен данными происходит якобы с надежной (в отношении безопасности) сетью. При использования данного способа хакер должен видоизменить заголовки пакетов так, чтобы складывалось впечатление, что пакеты поступают с надежного хост-компьютера и должны беспрепятственно пропускаться сетевым экраном или маршрутизатором. OMNI ADSL блокирует все попытки подмены IP.

10.5 Инспекция пакетов с учетом состояния

Инспекция с учетом состояния означает, что поля пакетов сравниваются с теми пакетами, которые уже считаются достоверными. Например, при доступе к внешнему серверу, proxy-сервер запоминает параметры первоначального запроса, такие как номер порта и адреса источника и назначения. Такое "запоминание" называется *сохранением состояния.* Когда внешняя система отвечает на запрос, межсетевой экран сравнивает параметры получаемых пакетов с параметрами сохраненного состояния и принимает решение о допуске. В маршрутизаторе OMNI ADSL инспекция пакетов с учетом состояния используется для защиты частной локальной сети от хакеров и вандалов в Интернете. По умолчанию, в ZyWALL, по результатам инспекции пакетов с учетом состояния, разрешается передача данных в Интернет из локальной сети и блокируется весь обратный трафик. В кратком изложении, функция инспекции пакетов с учетом состояния:

- Разрешает сеансы связи с глобальной сетью Интернет со стороны ЛВС.
- Запрещает сеансы связи с локальной сетью со стороны глобальной.

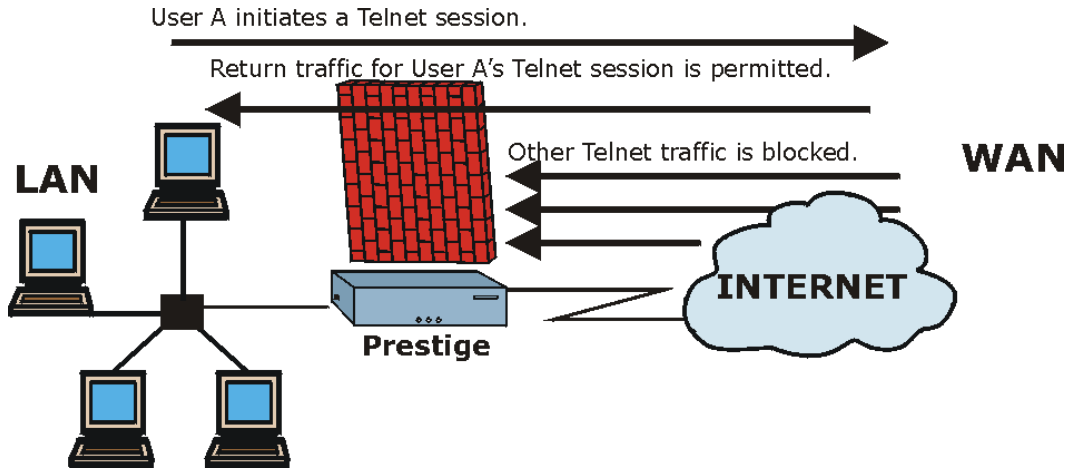


Рис. 10-5 Инспекция пакетов с учетом состояния

Предыдущий рисунок иллюстрирует применение установленных по умолчанию правил межсетевого экрана OMNI ADSL, а также работу системы инспекции с учетом состояния. Пользователь A может инициировать Telnet-соединение из локальной сети, и ответы на его запросы разрешены. Однако всякий иной трафик Telnet, поступающий из глобальной сети, блокируется.

10.5.1 Процесс инспекции пакетов с учетом состояния

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

1. Пакет поступает из локальной сети (где находится межсетевой экран) в глобальную сеть.
2. Происходит проверка пакета со списком контроля исходящего доступа для данного интерфейса и дается разрешение (пакет с отказом сбрасывается уже на данном этапе).
3. Происходит инспекция пакета в соответствии с правилом работы межсетевого экрана для выявления и записи информации о состоянии подключения для данного пакета. Эта информация записывается в виде нового элемента таблицы состояний, созданной для данного подключения. При отсутствии определенного правила межсетевого экрана для данного пакета, и если он не является атакой, то действие, выполняемое в отношении данного пакета, определяется содержанием поля **The default action for packets not matching following rules** (Действие по умолчанию для пакетов, не удовлетворяющих следующим правилам) (см. *Figure 12-4*).

4. В зависимости от полученной информации о состоянии, в соответствии с правилами работы межсетевого экрана, создается временная запись в списке контроля доступа, помещаемом в начале расширенного списка контроля входящего доступа для интерфейса WAN. Эта временная запись в списке контроля доступа предназначена для разрешения пропуска входящих пакетов в том же соединении, что и уже инспектированные исходящие пакеты.
5. Исходящий пакет пересылается через данный интерфейс.
6. Далее, входящий пакет достигает интерфейса. Этот пакет является частью соединения, уже установленного исходящим пакетом. Происходит сверка входящего пакета со списком контроля входящего доступа и дается разрешение, так как ранее была добавлена временная запись в список контроля доступа.
7. Пакет проверяется на соответствие по правилам работы межсетевого экрана, а таблица состояний для данного соединения по необходимости обновляется. На основании обновленной информации о состоянии временные записи расширенного списка контроля входящего доступа могут быть изменены, чтобы разрешать пропускать только пакеты, действительные для текущего состояния данного соединения.
8. Проверяются дополнительные входящие или исходящие пакеты для данного соединения, таким образом обновляется таблица состояний и соответственно, временные записи в списке контроля исходящего доступа; пакеты пересылаются через интерфейс.
9. При прекращении связи или истечении времени ожидания, таблица состояний для данного соединения и временные записи в списке контроля доступа удаляются.

10.5.2 Инспекция с учетом состояния и правил маршрутизатора OMNI ADSL

Правила, установленные по умолчанию, могут быть расширены за счет создания дополнительных, или игнорироваться. Например, можно создать правило, которое будет выполнять следующее:

i. Блокировать трафик определенного типа, например IRC (Internet Relay Chat), исходящий из локальной сети в Интернет.

ii. Разрешить трафик определенного типа из Интернет к конкретным хост-компьютерам локальной сети.

iii. Разрешить доступ к web-серверу всем, кроме конкурентов.

iv. Разрешить использование определенных протоколов, например Telnet, лишь полномочным пользователям локальной сети.

Эти определяемые пользователям правила работают, используя принцип проверки IP-адреса источника и IP-адреса назначения сетевого трафика, типа протокола IP, и проверки на соответствие правилам, установленным администратором.

Возможность назначения правил межсетевого экрана является очень мощным инструментом. С помощью таких правил можно отключить сетевую защиту целиком или заблокировать любой доступ в Интернет. Создание и удаление правил межсетевого экрана требует большой осторожности. После создания новых правил необходимо их проверить на правильность работы.

Ниже дается краткое техническое описание отслеживания таких соединений. Соединения могут быть определены либо с помощью протоколов верхнего уровня (например, TCP), или собственно OMNI ADSL (как "виртуальные соединения", создаваемые для UDP и ICMP).

10.5.3 Безопасность TCP

OMNI ADSL использует информацию о состоянии, включенную в пакеты TCP. В первом пакете нового соединения флаг SYN установлен, а флаг ACK снят; это пакеты-"инициаторы". Пакеты, не содержащие таких флажков, называются "последующими", так как несут данные, возникающие затем в потоке TCP.

Если из глобальной сети появляется пакет-"инициатор", это означает, что кто-то пытается подключиться к локальной сети из сети Интернет. Такие пакеты, за исключением некоторых особых случаев (см. "Протоколы верхнего уровня" приведенные далее), регистрируются и сбрасываются.

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

При получении устройством OMNI ADSL последующего пакета (из сети Интернет или из локальной сети) из него извлекается информация о соединении и сравнивается с записанной в кэше. Прохождение пакета разрешается только при условии его соответствия данному соединению (то есть, если он является ответом на запрос соединения из локальной сети).

10.5.4 Безопасность UDP/ICMP

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

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

Подобная ситуация имеет место и для ICMP, но в этом случае OMNI ADSL содержит более строгие ограничения. В частности, лишь в ответ на исходящие эхо-запросы разрешены входящие эхо-

отклики, на исходящий запрос маски подсети - входящий ответ, а входящий ответ временной метки разрешен только на исходящий запрос. Межсетевой экран не пропускает никакие другие пакеты ICMP, так как они представляют собой большую опасность и содержат слишком мало информации о маршруте. Например, прием ICMP-пакетов переадресации запрещен, так как с их помощью можно перенаправить трафик через атакующие машины.

10.5.5 Протоколы верхнего уровня

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

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

Чтобы получить доступ к файлам, OMNI ADSL инспектирует данные FTP на уровне приложений. В частности, он ищет выходную команду "PORT", и, если таковая имеется, добавляет в кэш запись об ожидаемом соединении для передачи данных. Эта операция безопасна, поскольку команда PORT содержит адрес и порт, по которым идентифицируется соединение.

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

10.6 Руководство по повышению безопасности с помощью межсетевого экрана

1. Изменить пароль, заданный по умолчанию, через системный терминал или Web-конфигуратор.
2. Тщательно продумать управление доступом *до* подключения консольного порта к сети, в том числе подсоединение модема к порту. Следует знать, что в результате сбоя в работе консольного порта неавторизованные пользователи могут получить полный доступ к сетевой защите, даже при установленном контроле доступа.
3. Ограничить круг лиц, имеющих право telnet-подключения к маршрутизатору.
4. Не подключать локальные службы (SNMP или NTP), которые не используются. Любое такое лишнее подключение может представлять потенциальную угрозу безопасности. Находчивый хакер может отыскать оригинальные способы злоупотребления подключенными услугами для получения доступа к сетевой защите и сети.

5. Подключенные локальные серверы необходимо обезопасить. Защита обеспечивается путем ограничения взаимодействия до конкретных клиентских устройств и назначением правил блокирования пакетов, поступающих через конкретный интерфейс.
6. Активизированный межсетевой экран обеспечит защиту от IP-спуфинга.
7. Межсетевой экран должен находиться в безопасном (закрытом) помещении.

10.6.1 Общая безопасность

Предусмотреть все возможные случаи нереально. Факторы, выходящие за пределы возможностей межсетевого экрана по фильтрации или трансляции сетевых адресов, могут повлечь бреши в системе защиты. Ниже приводятся некоторые общие рекомендации, выполнение которых позволит свести этот риск к минимуму.

1. Организации/компании необходимо разработать комплексный план по защите. Качественное сетевое администрирование предполагает учет возможностей хакеров и предвидение атак. Лучшей защитой от хакеров и взломщиков является информированность. Все сотрудники компании должны быть осведомлены о том, как важна безопасность и как минимизировать риск. Рекомендуется составить перечни, подобные этому.
2. Подключения с помощью DSL или кабельного модема являются соединениями типа “always-on” ("всегда включено") и особенно уязвимы, так как предоставляют хакерам возможность взлома системы. Компьютер, который в данный момент не используется, нужно выключить.
3. Никогда не сообщать пароль или другие секретные данные, отвечая на незатребованный телефонный звонок или сообщение по электронной почте.
4. Никогда не отправлять секретные сведения, такие как пароли, данные о кредитных картах и т.д. в незашифрованном виде.
5. Не сообщать секретные данные на web-страницу, если web-сайт не использует безопасные подключения. Безопасное подключение можно идентифицировать по иконке в виде ключа в нижней панели браузера (Internet Explorer 3.02 и выше или Netscape 3.0 и выше). Если Web-сайт использует безопасное подключение, предоставление информации безопасно. Безопасные web-транзакции довольно сложно взламывать.
6. Не сообщать IP-адрес и прочие системные данные по сети людям, не имеющим отношения к Вашей организации. Обращать внимание на файлы, присылаемые по электронной почте неизвестными отправителями. Общеизвестный способ получить вирус BackOrifice - принять его в составе другого файла в качестве "троянского коня".
7. Время от времени менять пароли. Использовать пароли, которые невозможно угадать. Наиболее трудно взламывать пароли, содержащие буквы нижнего и верхнего регистров, одновременно числа и символы типа % или #.

8. Регулярно обновлять программное обеспечение. Множество старых версии программ, особенно Web-браузеры, имеют недостатки в системе защиты. Обновления программ позволяют получить самые последние патчи и исправления.
9. При посещении “chat rooms” (чатов) или участвуя в IRC-сессиях необходимо тщательно следить за информацией, сообщаемой незнакомым людям.
10. При подозрительном поведении системы необходимо обратиться к своему Интернет-провайдеру. Некоторые хакеры используют средства, вызывающие с течением времени все более неустойчивую или неприемлемую работу системы.
11. Уничтожать конфиденциальную информацию, особенно о компьютере, содержащуюся в выбрасываемых документах. Некоторые хакеры могут получить необходимую им информацию, исследуя ненужные документы, выбрасываемые организацией или отдельными людьми .

10.7 Сравнение функций фильтрации пакетов и межсетевого экрана

Ниже приводится сравнение функций фильтрации маршрутизатора OMNI ADSL и его межсетевого экрана.

10.7.1 Фильтрация пакетов:

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

Когда используется фильтрация пакетов

1. Для блокирования/разрешения прохождения пакетов локальной сети по их MAC-адресам.
2. Для блокирования/разрешения пропуска особых пакетов IP, которые не являются пакетами TCP, UDP, или ICMP.
3. Для блокирования/разрешения как входящего (из WAN в LAN), так и исходящего (из LAN в WAN) трафика между конкретным внутренним хостом/сетью "A" и внешним хостом/сетью "B". Если фильтр блокирует трафик из A в B, то также блокируется и трафик из B в A. Фильтры не могут различать трафик, исходящий от внутреннего или внешнего хоста по IP-адресу.
4. Для блокирования/разрешения IP trace route.

10.7.2 Межсетевой экран

- Межсетевой экран проверяет содержание пакетов и адреса их источника и назначения. Экраны такого типа используют модуль контроля, подходящий ко всем протоколам, и распознающий данные пакета разных уровней, от сетевого уровня (заголовки IP) до уровня приложений.
- Межсетевой экран выполняет инспекцию пакетов с учетом состояния. Он учитывает состояние обрабатываемых подключений, например, легальный входящий пакет можно сопоставить с исходящим запросом на этот пакет и разрешить его вхождение. Напротив, входящий пакет, маскирующийся под ответ на несуществующий исходящий запрос, блокируется.
- Межсетевой экран выполняет фильтрацию сеансов связи, т.е. использует сложные правила, расширяющие процесс фильтрации с проверки отдельных пакетов в рамках сеанса связи до контроля всего сеанса в целом.
- Межсетевой экран, в случае поступления обычных отчетов и предупреждений, извещает о них сообщениями электронной почты.

Когда используется межсетевой экран

1. Для защиты от атак типа DoS и предотвращения проникновения в сеть хакеров.
2. При необходимости применения сложных правил защиты с назначением IP-адресов источника и назначения, а также номеров портов, использование экрана является более предпочтительным.
3. Для выборочного блокирования/разрешения входящего и исходящего трафика между внутренними и внешними хост-машинами/сетями. Напомним, что фильтры не в состоянии отличать трафик с внутреннего или внешнего хоста по IP-адресу.
4. Межсетевой экран предпочтительнее фильтрации, если необходима проверка на соответствие многим правилам.
5. Предпочтительнее пользоваться межсетевым экраном в случае необходимости получения по электронной почте плановых отчетов о системе или сообщений об атаках.
6. Межсетевой экран позволяет блокировать трафик от определенного URL, если таковой появится. Указатели URL сохраняются в базе данных списка контроля доступа.

Chapter 11
Настройка межсетевого экрана

В данной главе описывается как подключить и настроить межсетевой экран маршрутизатора OMNI ADSL. Содержание данной главы относится к моделям OMNI ADSL LAN H/HW и OMNI ADSL LAN H-E.

11.1 Дистанционное управление и межсетевой экран

При соответствующих настройках дистанционного управления, разрешающих его применение (см. главу *Дистанционное управление*), включенный межсетевой экран выполняет следующие функции:

- Блокировка дистанционного управления из глобальной сети (пока не будет задано соответствующее правило его работы).
- Разрешение дистанционного управления из LAN.

11.2 Включение межсетевого экрана

Щелкните по **Advanced Setup**, **Firewall**, а затем **Config** для вызова следующего экрана. Включите флажок **Firewall Enabled (Выключить брандмауэр)** и щелкните по **Apply** для его включения (или активации).

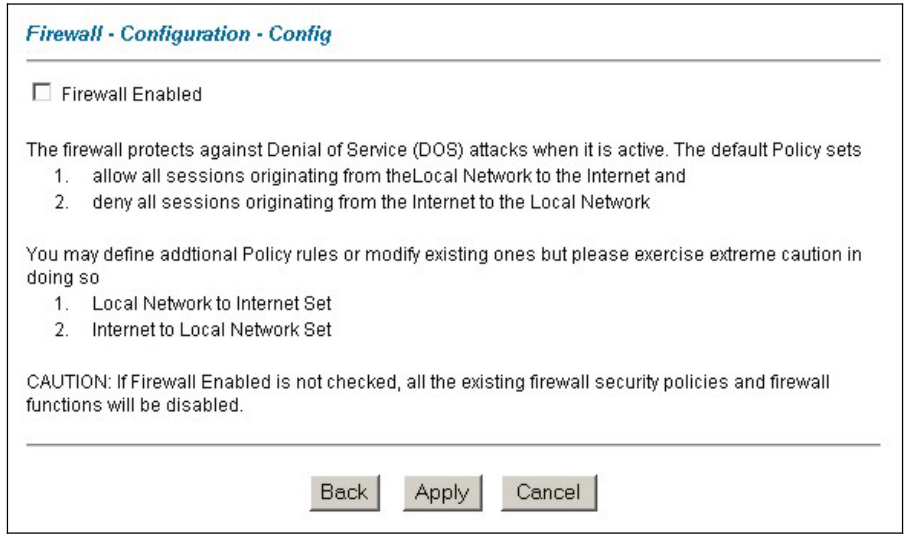


Рис.. 11-1 Активизация межсетевого экрана

11.3 Настройка предупреждений E-Mail

Для изменения настроек журнала регистрации электронной почты щелкните по **Advanced Setup**, **Firewall**, а затем **E-mail**. Появится экран приведенного ниже вида.

Экран **E-Mail** следует использовать для настройки адресования рассылки устройством OMNI ADSL регистрационных журналов, расписания их отправки, а также того, какие журналы и/или предупреждения OMNI ADSL должен отправлять. Сообщение "End of Log" (Конец журнала) появляется каждый раз, когда отправляется полностью заполненный журнал.

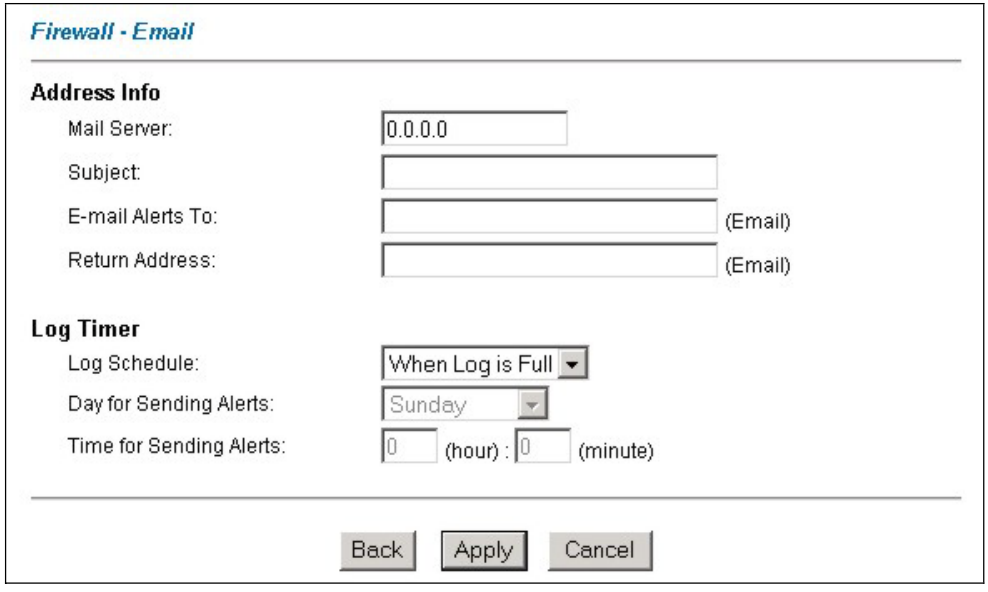


Рис. 11-2 Электронная почта

В следующей таблице приведены описания полей данного экрана.

Табл. 11-1 E-mail

ПОЛЕ	ОПИСАНИЕ
Address Info (Информация об адресе)	

Табл. 11-1 E-mail

ПОЛЕ	ОПИСАНИЕ
Mail Server (Почтовый сервер)	Введите имя сервера или IP-адрес почтового сервера для адресов электронной почты, указанных ниже. Если не заполнять это поле, журналы и предупреждающие сообщения не будут высылаться по электронной почте.
Subject (Тема)	Введите наименование заголовка, которое будет находиться в строке "Тема" сообщений журнала регистрации, отправляемых по электронной почте устройством OMNI ADSL.
E-mail Alerts To (Адрес e-mail для направления предупреждений)	Предупреждения будут отправляться по адресам электронной почты, указанным в этом поле. Если оставить это поле незаполненным, то предупреждения не будут высылаться по электронной почте.
Return address (Обратный адрес)	Введите e-mail адрес OMNI ADSL для его идентификации как отправителя e-mail сообщений, т.е. адрес return-to-sender (вернуть отправителю) в целях резервного сохранения адреса.
Таймер журнала	
Log Schedule (План журнальной регистрации)	В этом "всплывающем" меню задается частота рассылки журнальных записей по электронной почте: • **Daily** • **Weekly** • **Hourly** • **When Log is Full** • **None.** Если выбрана опция **Weekly (Еженедельно)** или **Daily (Ежедневно)**, укажите, в какое время дня следует отправить электронную почту. Если выбрана опция **Weekly (Еженедельно)**, то укажите также в какой день недели следует отправить электронную почту. Если выбрана опция **When Log is Full (После заполнения журнала регистрации)**, предупреждение будет отправлено после заполнения журнала. Если выбрана опция **None**, сообщения журнала регистрации отправляться не будут
Day for Sending Alerts (День рассылки предупреждений)	Следует воспользоваться раскрывающимся списком для выбора дня недели, когда должны быть отправлены журналы.
Time for Sending Alerts(Время рассылки предупреждений)	Введите время суток в 24-часовом формате (например, 23:00 соответствует времени 11:00 вечера), когда должны быть отправлены журналы.

Табл. 11-1 E-mail

ПОЛЕ	ОПИСАНИЕ
Back (Назад)	Щелкните по **Back (Назад)**для возвращения к предыдущему экрану.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения настроек и выхода из экрана.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отемна)** для возвращения к ранее сохраненным настройкам.

11.4 Предупреждения об атаках

Предупреждения об атаках являются сообщениями реального времени об атаках типа DoS. На экране **Attack Alert,** представленном ниже, можно назначить генерацию сообщения об ошибке при обнаружении атаки. В случае атак типа DoS в OMNI ADSL используются допустимые пределы для определения момента, когда следует прервать не полностью установленный сеанс связи. Данные допустимые пределы в общем случае относятся ко всем сессиям.

Можно использовать значения допустимых пределов по умолчанию или установить собственные в соответствии с требованиями безопасности.

11.4.1 Предупреждения

Предупреждения - это сообщения о событиях (таких как атаки), информация о которых может быть необходима пользователю сразу. Выдачу предупреждения об атаке можно задать на экране **Attack Alert** *(Рис. 11-3* - поставить флажок **Generate alert when attack detected**) или при совпадении с правилом на экране **Rule Config** (см. *Рис.12-5)*. При возникновении события, порождающего предупреждение, должно быть немедленно отправлено сообщение на учетную запись, заданную в экране **Log Settings** (см. главу о журналах).

11.4.2 Значения допустимых пределов

Если что-то не работает, а таймеры ожидания межсетевого экрана проверены, необходимо настроить данные параметры. Данные установки, принятые по умолчанию, прекрасно подходят для большинства небольших офисов. Выбор значений допустимых пределов зависит от следующих величин:

1. Максимальное число открытых сессий.
2. Минимальное число возможных незавершенных заданий на сервере локальной сети.
3. Возможности центральных процессоров серверов локальной сети.

4. Пропускная способность сети.
5. Тип трафика для отдельных серверов.

Если по причинам, зависящим от каких-то из вышеперечисленных факторов, сеть работает медленнее, чем обычно (особенно если имеются медленные серверы или серверы, обрабатывающие большое число задач и поэтому часто занятые), значения по умолчанию необходимо уменьшить. Изменения значений допустимых пределов должны выполняться до продолжения работы по настройке параметров межсетевого экрана.

11.4.3 Полуоткрытые соединения

Слишком большое число полуоткрытых соединений (выраженное конкретным числом или в виде частоты поступлений) может означать наличие атаки Denial of Service. Для TCP "полуоткрытое" соединение означает, что оно не установлено полностью, т.е. не выполнен трехсторонний TCP-обмен запросами (см. *Рис. 10-2*). Для UDP, "полуоткрытое" соединение означает, что межсетевым экраном не обнаружен ответный трафик.

OMNI ADSL определяет как общее число имеющихся в данный момент полуоткрытых соединений, так и частоту попыток установить соединение. Для обоих типов соединений, TCP и UDP, считается число полуоткрытых соединений и интенсивность поступлений запросов. Подсчеты производятся поминутно.

Когда число существующих полуоткрытых соединений превышает максимально допустимый предел (**max-incomplete high**), OMNI ADSL начинает удалять полуоткрытые соединения для размещения новых запросов. Полуоткрытые соединения будут удаляться до тех пор, пока их число не уменьшится до значения, не превышающего другого (минимального) допустимого предела (**max-incomplete low**).

Если частота новых попыток соединений превысит максимально допустимый уровень в минуту (**one-minute high**), OMNI ADSL начнет удалять полуоткрытые соединения для размещения новых запросов. Полуоткрытые соединения будут удаляться до тех пор, пока частота новых попыток соединений не снизится до значения, не превышающего другого (минимального) допустимого предела в минуту (**one-minute low**). Частота соединений - это число новых попыток, обнаруженное за последний установленный период выборки длительностью в одну минуту.

Значения TCP Maximum Incomplete и Blocking Time

Слишком большое число полуоткрытых соединений с одним и тем же адресом хоста назначения может означать атаку Denial of Service , направленную на данный хост-компьютер.

Если число полуоткрытых соединений с одним и тем же адресом назначения превышает допустимый предел (**TCP Maximum Incomplete**), Pestige начинает удалять полуоткрытые соединения одним из следующих способов:

1. Если время ожидания **Blocking Time** установлено на 0 (по умолчанию), OMNI ADSL удаляет самые старые из существующих полуоткрытых соединений для данного хоста с каждым новым запросом соединения. В этом случае число полуоткрытых соединений для данного хоста не может превысить допустимый предел.
2. Если значение **Blocking Time** больше 0, OMNI ADSL блокирует все вновь поступающие на данный хост запросы соединения, оставляя серверу время обработать текущие запросы. OMNI ADSL блокирует все вновь поступающие запросы соединения до полного истечения времени **Blocking Time**.

OMNI ADSL также посылает предупреждения о превышении значения **TCP Maximum Incomplete**. Глобальные значения допустимого предела и времени ожидания действительны для всех TCP-соединений. Щелкните по **Advanced Setup (Дополнительная настройка)**, **Firewall (Межсетевой экран)** и **Alert (Предупреждение)** для вызова следующего экрана.

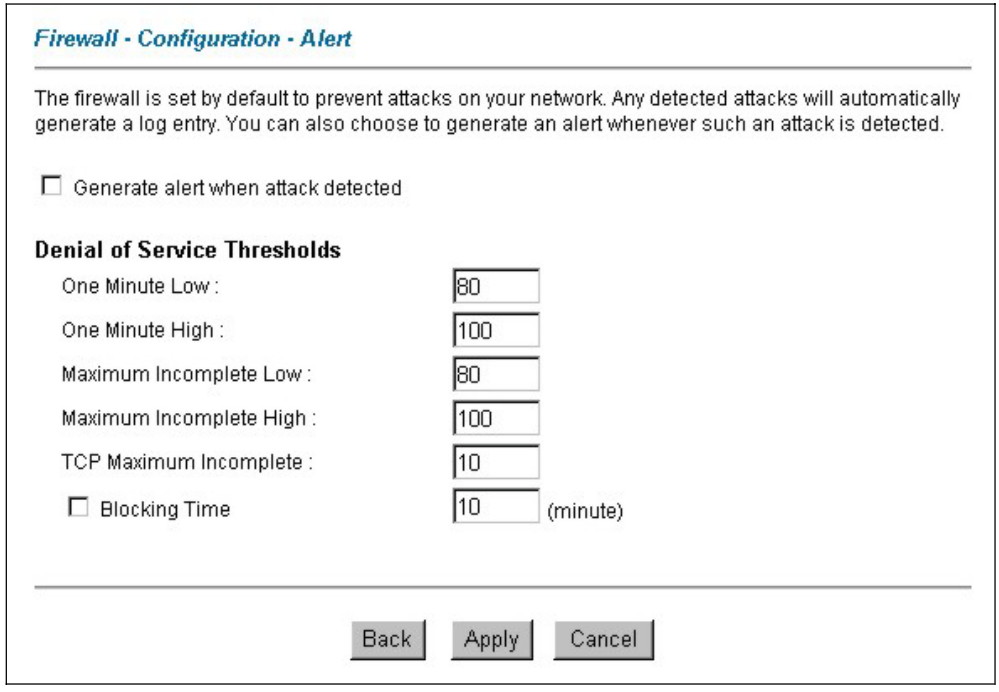


Рис. 11-3 Предупреждения об атаках

В следующей таблице приведены описания полей данного экрана.

Табл. 11-2 Предупреждения об атаках

LABEL	DESCRIPTION
Generate alert when attack detected (Генерирование предупреждения при обнаружении атаки)	Поставить метку в этом окошке для задания отправки предупреждений в случае обнаружения атак.
Denial of Services Thresholds (Отказ от обслуживания)	
One Minute Low	Частота появления новых полуоткрытых соединений, при которой межсетевой экран прекращает удалять полуоткрытые соединения. Полуоткрытые соединения будут удаляться до тех пор, пока частота новых попыток соединений не снизится до значения, не превышающего данное. По умолчанию считается равным "80".
One Minute High	Частота появления новых полуоткрытых соединений, при которой межсетевой экран начинает удалять полуоткрытые соединения. По умолчанию считается равным "100". Как только частота новых запросов соединений превышает данное значение, OMNI ADSL удаляет полуоткрытые соединения для размещения вновь поступивших запросов. OMNI ADSL прекращает удаление полуоткрытых соединений, когда их число становится меньше заданного в поле **One Minute Low.**
Maximum Incomplete Low	Число существующих полуоткрытых соединений, при котором межсетевой экран прекращает удалять полуоткрытые соединения (по умолчанию принимается равным "80"). Полуоткрытые соединения будут удаляться до тех пор, пока число существующих полуоткрытых соединений не снизится до значения, не превышающего данное.
Maximum Incomplete High	Число существующих полуоткрытых соединений, при котором межсетевой экран прекращает удалять полуоткрытые соединения (по умолчанию принимается равным "100"). Как только число существующих полуоткрытых соединений превысит данное значение, OMNI ADSL начнет удалять полуоткрытые соединения для размещения вновь поступивших запросов. OMNI ADSL прекращает удаление полуоткрытых соединений, когда их число становится меньше заданного в поле **Maximum Incomplete Low**. Нельзя устанавливать значение **Maximum Incomplete High** ниже, чем текущее значение **Maximum Incomplete Low**.

Табл. 11-2 Предупреждения об атаках

LABEL	DESCRIPTION
TCP Maximum Incomplete	Число существующих полуоткрытых соединений TCP с одним и тем же IP-адресом назначения (по умолчанию принимается равным "10"), при котором межсетевой экран начинает сбрасывать полуоткрытые соединения с адресатом по данному IP-адресу. Введите значение в интервале от **1** до **250**. Общим принципом является выбор меньшего значения для меньшей по размерам сети, медленной системы или ограниченной пропускной способности.
Blocking Time	По достижении значения **TCP Maximum Incomplete** следующее соединение можно разрешить или блокировать. Если задать значение **Blocking Time,** новые соединения будут блокироваться на период времени, указываемый **(в минутах)** в следующем поле, а все старые незавершенные соединения в течение этого времени будут удаляться. В целях повышения безопасности рекомендуется блокировать трафик на короткое время, так как серверу в этом случае дается время обработать имеющиеся запросы.
(min)	Введите значение **Blocking Time (Время блокировки)** в минутах (1-256). По умолчанию принимается равным "0".
Back (Назад)	Щелкните по **Back (Назад)**для возвращения к предыдущему экрану.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения настроек и выхода из экрана.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возвращения к ранее сохраненным настройкам.

Chapter 12
Создание собственных правил

В этой главе даются указания по созданию правил для локальной сети и Интернет. Содержание данной главы относится к моделям OMNI ADSL LAN H/HW и OMNI ADSL LAN H-E.

12.1 Общие сведения о правилах

Правила межсетевого экрана подразделяются на правила для LAN и для сети Интернет. По умолчанию функция инспекции пакетов с учетом состояния в OMNI ADSL разрешает связь с Интернет, если она исходит из локальной сети, и блокирует весь трафик, поступающий в локальную сеть из Интернет. Возможно назначение дополнительных правил или модификация существующих, однако делать это следует с большой осторожностью.

При составлении правил без необходимых навыков существует риск случайного возникновения сбоя в работе межсетевого экрана и системе защиты сети. Проверьте работоспособность правил тестированием после завершения настроек.

Например, можно назначить следующие правила:

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

Эти определяемые пользователям правила работают на основе принципа проверки IP-адреса источника и IP-адреса назначения сетевого трафика, а также типа протокола IP, на соответствие правилам, установленным администратором. Определяемые пользователем правила имеют более высокий приоритет по сравнению с правилами по умолчанию и могут замещать последние.

12.2 Логика правил

Прежде, чем назначать правила, необходимо тщательно изучить данные указания.

12.2.1 Список вопросов для составления правил

1. Сформулировать смысл данного правила. Например: "Ограничить доступ к системе IRC из локальной сети в сеть Интернет". или: "Позволить удаленному серверу Lotus Notes синхронизацию с внутренним сервером Notes через сеть Интернет."
2. Пересылать или блокировать трафик?
3. Направление соединения: из локальной сети в Интернет или из сети Интернет в локальную сеть?
4. На какие виды обслуживания IP оно повлияет?
5. На каких компьютерах локальной сети отразится выполнение этого правила?
6. На каких компьютерах в Интернете отразится выполнение этого правила? Эти сведения должны быть по возможности конкретны. Например, если разрешается пересылка трафика из Интернет в локальную сеть, лучше указать определенные серверы в Интернете, которые будут иметь доступ к локальной сети.

12.2.2 Правила межсетевого экрана

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

1. Не препятствует ли данное правило пользователям в локальной сети иметь доступ к каким-то важным ресурсам в Интернете? Например, если IRC блокируется, есть ли пользователи, которым этот вид услуги необходим?
2. Нельзя ли видоизменить правило так, чтобы оно стало более конкретным? Например, если IRC блокирован для всех пользователей, возможно, будет более целесообразным задать правило, которое блокирует этот доступ только для определенных пользователей.
3. Не является ли правило, позволяющее пользователям сети Интернет иметь доступ к ресурсам локальной сети, причиной появления слабых мест в системе защиты? Например, если соединение с локальной сетью через порт FTP (TCP 20, 21) возможно из Интернета, пользователи сети Интернет могут получить доступ к работающим FTP-серверам.
4. Нет ли конфликта между данным правилом и другими имеющимися правилами?

После получения ответов на вышеперечисленные вопросы процесс составления правил сводится лишь к правильному заполнению соответствующих полей экрана **Rules** Web-конфигуратора.

12.2.3 Правила: основные поля для заполнения

Action (Действие)

Выберите **Block** или **Forward**

"Block" (Блокировать) **означает, что пакет просто уничтожается.**

Тип обслуживания

Выберите тип обслуживания из окна списка **Service**. Если нужной услуги нет в списке, необходимо сначала ее определить. Дополнительную информацию по предварительно определенным услугам см. в *разделе 12.6*.

Адрес источника

Адрес источника соединения; может быть в локальной или глобальной сети, одиночный IP, диапазон IP или подсеть

Адрес назначения

Адрес назначения соединения; может быть в локальной или глобальной сети, одиночный IP, диапазон IP или подсеть

12.3 Направление связи

В этом разделе описан процесс назначения правил работы межсетевого экрана для подключений из LAN к WAN и из WAN к LAN.

12.3.1 Правила для соединений LAN - WAN

По умолчанию относительно трафика LAN и WAN принимается правило, согласно которому все пользователи ЛВС имеют неограниченный доступ к ресурсам глобальной сети. При выборе настроек правил Policy -> LAN to WAN -> (стратегия доступа из ЛВС в глобальную сеть), обычно, подразумевается необходимость установления ограничений для всех или нескольких пользователей на доступ к услугам глобальной сети. См. следующий рисунок.

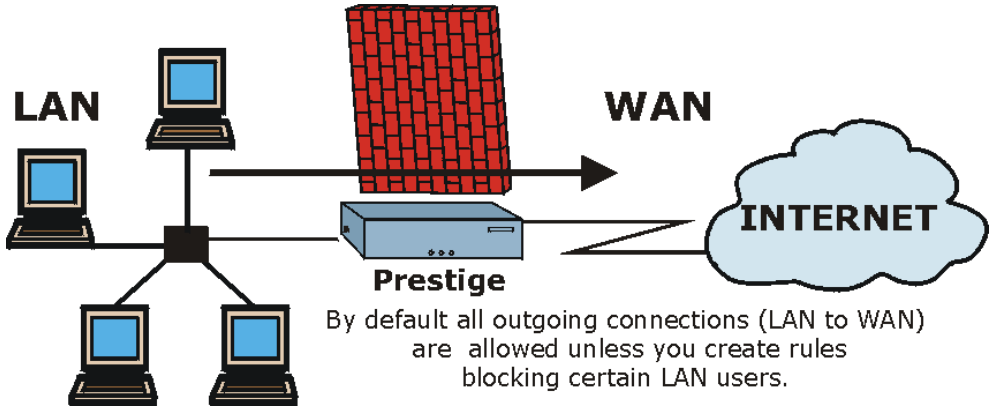


Рис. 12-1 Трафик LAN - WAN

12.3.2 Правила для соединений WAN - LAN

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

См. следующий рисунок.

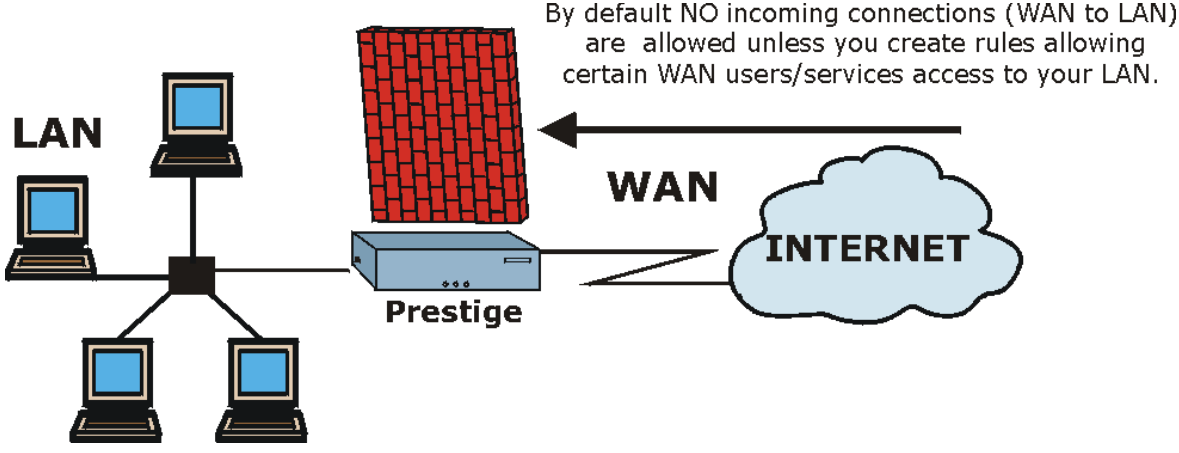


Рис.. 12-2 Трафик WAN - LAN

12.4 Журналы регистрации

Журнальная регистрация - это подробная запись, создаваемая для пакетов, которые удовлетворяют или не удовлетворяют правилу, или для тех и других, а также при создании/редактировании правил работы межсетевого экрана (см. *Рис.12-5)*. В этом экране можно отменить создание регистрации для какого-либо правила. В случае атаки журнальная запись генерируется автоматически. Журналы могут отправляться электронной почтой в адрес учетной записи или сервера системного журнала, настройки которого задаются в экране **E-mail** (см. раздел о журналах электронной почты).

Для того чтобы увидеть настройки межсетевого экрана и контент-фильтра журналов следует воспользоваться данным экраном.

Щелкните по **Advanced Setup (Дополнительные настройки)**, **Firewall (Межсетевой экран)**, а затем **Logs** для вызова экрана **Logs**.

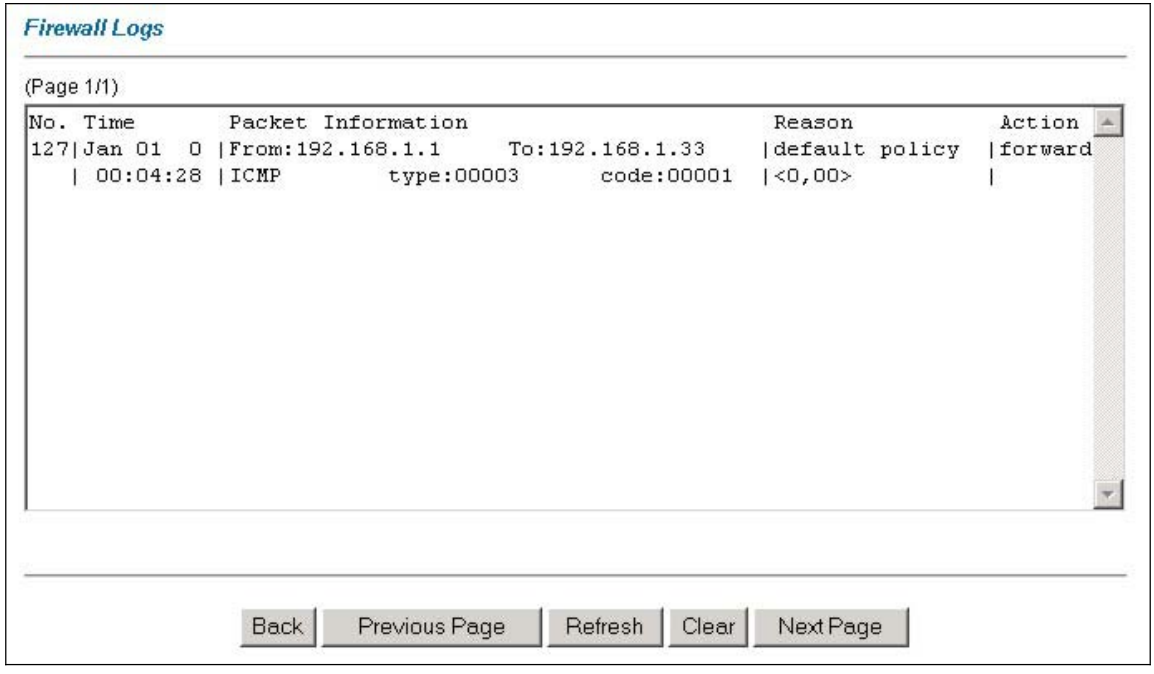


Рис. 12-3 Журналы межсетевого экрана

В следующей таблице приведены описания полей данного экрана.

Табл. 12-1 Журналы межсетевого экрана

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
No.	Порядковый номер журнальной записи. Возможен в пределах 128 записей с номерами от 0 до 127. Как только они будут использованы, заполнение журнала начинается вновь, при этом старые записи не сохраняются.	
Time (Время)	Время внесения записи в данном формате. Для правильного отображения времени следует сделать настройку меню 24.10.	dd:mm:yy (дд:мм:гг), например, Jan 01 0; hh:mm:ss (чч:мм:сс), например, 00:04:28
Packet Information (Данные о пакете)	В этом поле содержатся следующие данные о пакете: IP-адреса отправителя и получателя, протокол и номера портов.	
Reason (Причина)	В этом поле указывается причина регистрации записи; т.е., соответствие или несоответствие правилу, или атака. Координаты набора и правила (<X, Y>, где X=1,2; Y=00~10), сопровождаемые кратким объяснением. Существует два набора стратегий: набор 1 (X = 1) для правил для направления LAN - WAN и набор 2 (X = 2) для правил для направления WAN - LAN. Y означает номер правила в наборе. Можно задавать до 10 правил в любом наборе (Y = 01 до 10). Правило под номером "00" означает правило по умолчанию.	not match <1,01> dest IP Это означает, что в данном пакете IP-адрес назначения не соответствует заданному в наборе 1 правилу 1. Другими причинами этой ситуации (кроме упомянутой выше) является несоответствие src IP (IP-адреса источника), dest port (номера порта назначения), src port (номера порта источника) и протокола.
	Регистрация атаки DoS.	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop или syn flood. В *Chapter 10* содержится более подробное описание каждой из этих атак.

Табл. 12-1 Журналы межсетевого экрана

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Action	Пакет должен быть блокирован (т.е. просто удален), передан или ни то ни другое (**Block**, **Forward** или **None**). None означает, что данным правилом не предусмотрено никакое действие.	**Block**, **Forward** или **None**
Back	Щелкните по **Back (Назад)**для возвращения к предыдущему экрану.	
Previous Page	Щелкните по **Previous Page (Предыдущая страница)**, чтобы увидеть большее количество записей.	
Refresh	Щелкните по **Refresh (Обновление)** для обновления экрана отчетов. Отчет также обновляется автоматически после закрытия и повторного открытия экрана.	
Clear	Щелкните по **Clear (Очистить)**для удаления всех записей.	
Next Page	Щелкните по **Next Page (Следующая страница)**, чтобы увидеть большее количество записей.	

12.5 Краткий обзор правил

Поля экрана Rule Summary (Обзор правил) **одинаковы как для** Local Network **(Локальная сеть), так и для** Internet **(Интернет), поэтому приведенные ниже сведения относятся и к тем, и к другим.**

Щелкните по **Firewall**, а затем по **Rule Summary** для вызова следующего экрана. На экране появится краткое перечисление существующих правил. Следует обратить внимание на тот порядок, в котором они перечислены.

Порядок расположения правил имеет большое значение, так как правила выполняются по очереди.

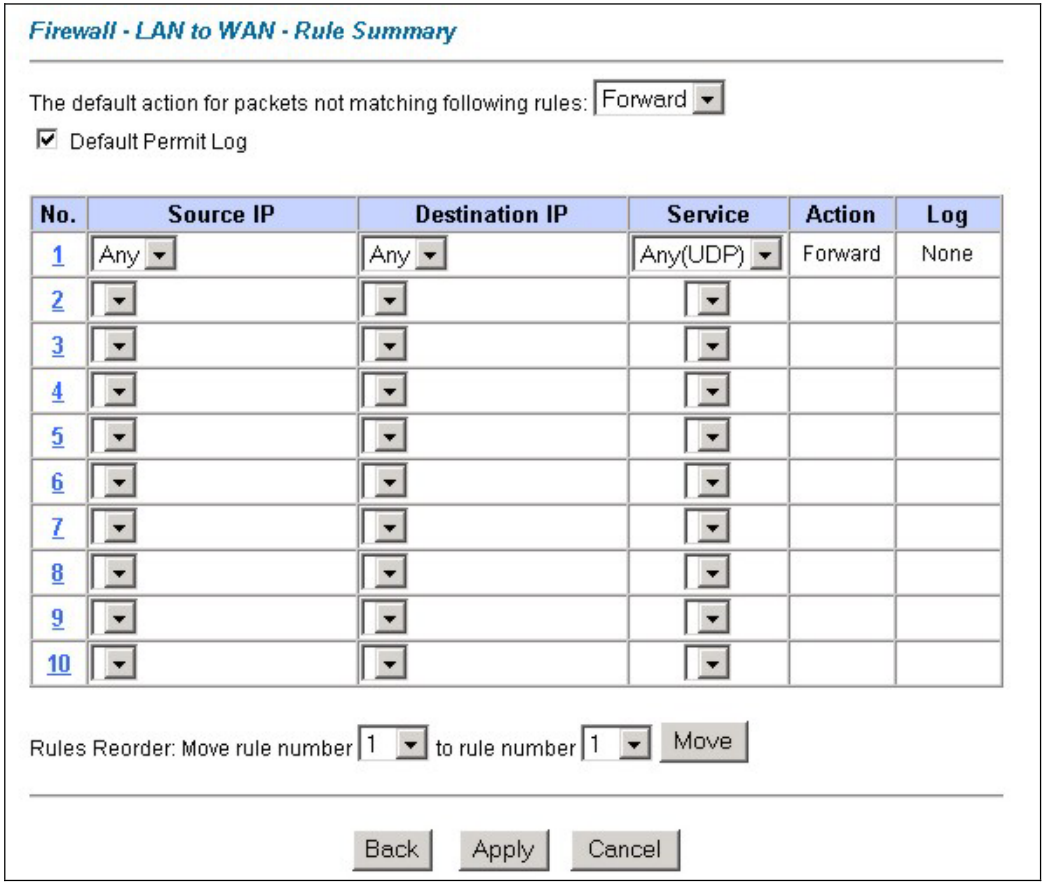


Figure 12-4 Обзор правил межсетевого экрана: Первый экран

В следующей таблице приведены описания полей данного экрана.

Табл. 12-2 Обзор правил межсетевого экрана: Первый экран

ПОЛЕ	ОПИСАНИЕ

Табл. 12-2 Обзор правил межсетевого экрана: Первый экран

The default action for packets not matching following rules	Пользуйтесь раскрывающимся списком для выбора опций **Block** (сброс без уведомления) или **Forward** (разрешение пересылки) пакетов, не отвечающих следующим правилам.
Default Permit Log	Поставьте флажок для записи всех соответствующих правил в набор ACL по умолчанию
Следующие поля относятся ко всем созданным правилам. Эти поля имеют статус "только для чтения". Выбрать закладку tab в верхней части окна, чтобы расположить поля как указано в этой закладке.	
No.	Номер правила. Порядок расположения правил имеет большое значение, так как правила выполняются по очереди. Поле **Move (Переместить)** позволяет изменить порядок следования правил. Щелкните по номеру правила для его редактирования.
Source IP	Адрес источника пакета. Следует отметить, что незаполнение полей "source" или "destination address" аналогично действию опции **Any**.
Destination IP	Адрес назначения пакета. Следует отметить, что незаполнение полей "source" или "destination address" аналогично действию опции **Any**.
Service	Услуга, которой касается применение данного правила. Подробнее см. *Табл. 12-3*.
Action	Задаваемое действие для данного правила, **Block** (Сброс) или **Forward** (Разрешение на передачу) пакетов.
Log	В поле помещается информацию о том, что в журнале создается запись для пакетов, которые: удовлетворяют правилу (**Match**), не удовлетворяют правилу (**Not Match**), не удовлетворяют обоим правилам (**Both**) или запись не создается (**None**).
Rules Reorder	С помощью данной функции можно изменить порядок правил. Для изменения нумераций правил укажите старый номер правила в раскрывающемся списке. Порядок расположения правил имеет большое значение, так как правила выполняются по очереди.
To Rule Number	Укажите новый номер правила в раскрывающемся списке.
Move	Щелкните по **Move (Переместить)** для перемещения правила.
Back	Щелкните по **Back (Назад)**для возвращения к предыдущему экрану.
Apply	Щелкните по кнопке **Apply (Применить)** для сохранения внесенных изменений.

Табл. 12-2 Обзор правил межсетевого экрана: Первый экран

Cancel	Щелкните по кнопке **Cancel (Отмена)** для возвращения к ранее сохраненным настройкам.

12.6 Предварительно определенные услуги

Окно списка **Available Services** на экране **Edit Rule** (см. *Рис.12-5*) содержит все предварительно определенные виды сервиса, поддерживаемые системой OMNI ADSL. Рядом с названием услуги помещаются два поля в скобках. В первом поле указан тип протокола IP (TCP, UDP или ICMP). Во втором - номер порта IP для данной услуги. (Следует учесть, что тип протокола IP может быть не один. В качестве примера можно привести конфигурацию по умолчанию с обозначением "(**DNS**)". Запись **(UDP/TCP:53)** означает UDP-порт 53 и TCP-порт 53. Возможно до 128 вхождений. Услуги, определяемые пользователем, можно описывать, используя упомянутую далее функцию **Custom Ports**.

Табл. 12-3 Предварительно определенные услуги

ТИП ОБСЛУЖИВАНИЯ	ОПИСАНИЕ
AIM/NEW_ICQ(TCP:5190)	Система пересылки сообщений в сети Интернет, предоставляемая корпорацией AOL, используется службой ICQ как "слушающий" порт.
AUTH(TCP:113)	Протокол аутентификации, используемый некоторыми серверами
BGP(TCP:179)	Протокол BGP (пограничный межсетевой протокол).
BOOTP_CLIENT(UDP:68)	Клиент DHCP.
BOOTP_SERVER(UDP:67)	Сервер DHCP.
CU-SEEME(TCP/UDP:7648, 24032)	Популярная программа для видеоконференций от компании White Pines Software.
DNS(UDP/TCP:53)	Сервер имен доменов, служба, сопоставляющая web-имена (например www.zyxel.com) с IP-адресами.
FINGER(TCP:79)	Finger - команда для UNIX или Интернет, используемая для проверки вхождения пользователя в сеть.
FTP(TCP:20.21)	Протокол передачи файлов, программа для быстрой передачи файлов, в том числе файлов большого размера, которые невозможно пересылать средствами электронной почты.
H.323(TCP:1720)	Протокол для Net Meeting.
HTTP(TCP:80)	Протокол передачи гипертекста - протокол уровня клиент/сервер

Табл. 12-3 Предварительно определенные услуги

ТИП ОБСЛУЖИВАНИЯ	ОПИСАНИЕ
	для WWW.
HTTPS	Протокол защищенной передачи текстов, часто используемый в Интернет-коммерции.
ICQ(UDP:4000)	Популярная система интерактивного общения в Интернет.
IPSEC_TRANSPORT/TUNNEL(AH:0)	Туннелирующий протокол IPSEC AH (аутентифицирующий заголовок).
IPSEC_TUNNEL(ESP:0)	Этим видом сервиса пользуется туннелирующий протокол IPSec ESP (протокол безопасной инкапсуляции).
IRC(TCP/UDP:6667)	Еще одна программа интерактивного общения в Интернет.
MSN Messenger(TCP:1863)	Протокол для передачи сообщений в сетях Microsoft.
MULTICAST(IGMP:0)	Широковещательный протокол взаимодействия групп в сети Интернет, используется для рассылки пакетов определенным группам хост-машин.
NEWS(TCP:144)	Протокол для групп новостей.
NFS(UDP:2049)	Сетевая файловая система - NFS, распределенная файловая система клиент/сервер, обеспечивающая прозрачное совместное использование файлов в сетевом окружении.
NNTP(TCP:119)	Сетевой протокол передачи новостей, система доставки для групп новостей USENET.
PING(ICMP:0)	Отправитель пакетов Интернет, протокол отправки запроса отклика ICMP для проверки доступности удаленного узла.
POP3(TCP:110)	Почтовый протокол версии 3, позволяет клиентскому компьютеру получать электронную почту с сервера POP3, используя временное соединение (TCP/IP или другое).
PPTP(TCP:1723)	Протокол туннелирования между узлами, обеспечивает безопасную передачу данных в общедоступных сетях. Канал управления.
PPTP_TUNNEL(GRE:0)	Протокол туннелирования между узлами, обеспечивает безопасную передачу данных в общедоступных сетях. Канал данных.
RCMD(TCP:512)	Удаленное управление командной строкой.
REAL_AUDIO(TCP:7070)	Система прямого воспроизведения звука, обеспечивает передачу аудиопотоков в Интернет в реальном времени.

Табл. 12-3 Предварительно определенные услуги

ТИП ОБСЛУЖИВАНИЯ	ОПИСАНИЕ
REXEC(TCP:514)	Демон удаленного выполнения команд.
RLOGIN(TCP:513)	Дистанционная регистрация.
RTELNET(TCP:107)	Удаленный сетевой теледоступ.
RTSP(TCP/UDP:554)	Протокол передачи мультимедийных потоков (RTSP), обеспечивает удаленное управление аудиовизуальными потоками в сети Интернет.
SFTP(TCP:115)	Простой протокол передачи файлов.
SMTP(TCP:25)	Простой протокол электронной почты, стандартный протокол обмена сообщениями в сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой.
SNMP(TCP/UDP:161)	Простой протокол сетевого управления.
SNMP-TRAPS(TCP/UDP:162)	Система регистрации событий в потоке SNMP (RFC:1215).
SQL-NET(TCP:1521)	Язык структурированных запросов, интерфейс доступа к системам баз данных различного типа, в том числе к суперЭВМ, среднепроизводительным машинам, системам UNIX и сетевым серверам.
SSDP(UDP:1900)	Протокол SSDP (упрощенной службы обнаружений) выполняет в домашней сети поиск устройств с функциями "Plug and Play" или шлюзов глобальной сети Интернет, использующих порт UDP 1900.
SSH(TCP/UDP:22)	Программа безопасной дистанционной регистрации.
STRMWORKS(UDP:1558)	Протокол передачи потоков Stream Works.
SYSLOG(UDP:514)	Системный журнал обеспечивает пересылку системных журналов на сервер UNIX.
TACACS(UDP:49)	Система управления доступом на основе контроллера доступа к терминалу.
TELNET(TCP:23)	Telnet - протокол регистрации и эмуляции терминала, общий для среды Интернета и UNIX, работающий в сетях TCP/IP. Его главная задача состоит в том, чтобы позволить пользователям регистрироваться в удаленных хост-системах.
TFTP(UDP:69)	Упрощенный протокол передачи файлов, протокол передачи файлов, подобный FTP, но использующий протокол UDP (протокол

Табл. 12-3 Предварительно определенные услуги

ТИП ОБСЛУЖИВАНИЯ	ОПИСАНИЕ
	передачи дейтаграмм пользователя), а не TCP (протокол управления передачей).
VDOLIVE(TCP:7000)	Еще одна программа для видеоконференций.

12.7 Создание и редактирование правил для межсетевого экрана

Для создания нового правила нужно щелчком по номеру (**No.**) в предыдущем экране вызвать следующий.

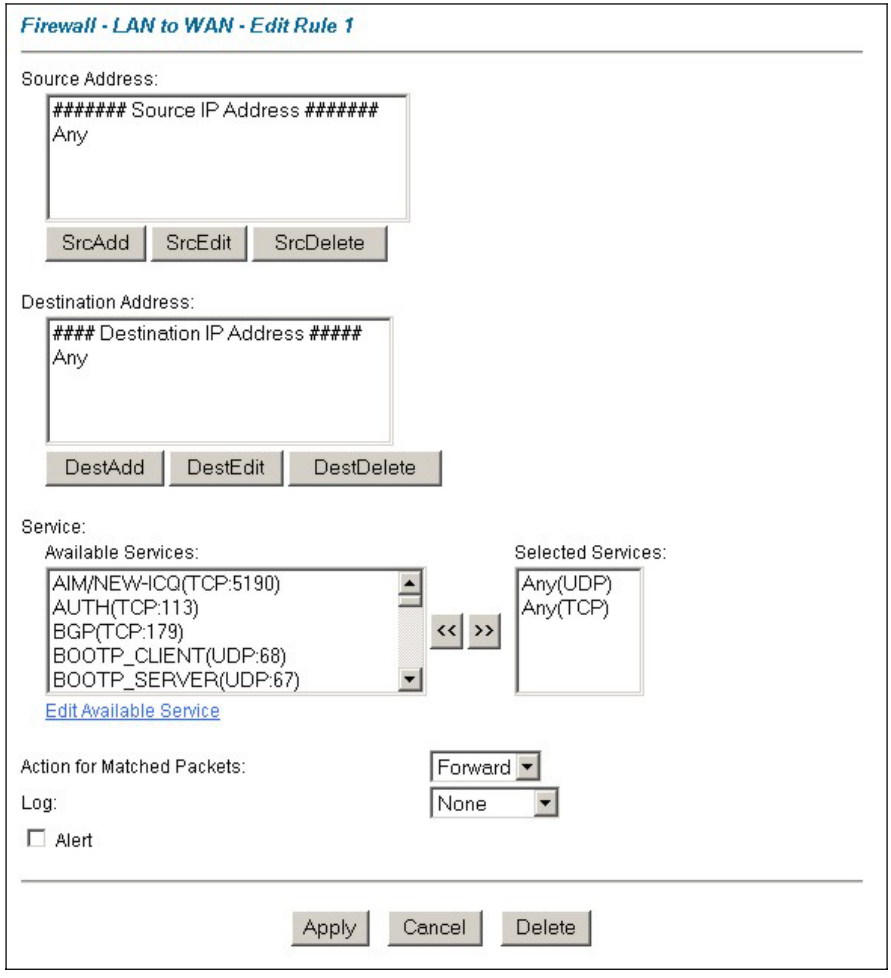


Рис.12-5 Создание и редактирование правил для межсетевого экрана

В следующей таблице приведены описания полей данного экрана.

Табл.12-4 Создание и редактирование правил для межсетевого экрана

ПОЛЕ	ОПИСАНИЕ
Source Address (Адрес источника)	Выбрать **SrcAdd** для добавления нового адреса, **SrcEdit** для изменения существующего или **SrcDelete** для удаления.

Табл.12-4 Создание и редактирование правил для межсетевого экрана

ПОЛЕ	ОПИСАНИЕ
Destination Address (Адрес назначения)	Выберите **DestAdd** для добавления нового адреса, **DestEdit** для изменения существующего или **DestDelete** для удаления.
Services (Услуги)	Выберите нужный вид сервиса в окне **Available Services** слева и пометьте его флажком, щелкнув по **>>**. Выбранные виды сервиса будут отображаться в окне **Selected Services** справа. Чтобы удалить услугу, выделите ее в списке **Selected Services** справа и щелкните по **<<**.
Edit Available Service (Редактирование доступности услуг)	Щелкните по этой кнопке для перехода к экрану "**Услуги, выбираемые пользователем"**. См. *главу 14* для получения дополнительной информации.
Action for Matched Packets (Действие для соответствующих пакетов)	Пользуйтесь раскрывающимся списком для выбора опций **Block (silently discard)** (Сброс без уведомления) или **Forward** (Разрешение пересылки) пакетов, отвечающих данному правилу.
Log (Журнал)	Информация в этом поле указывает на то, что в журнале создается запись для пакетов, которые: удовлетворяют правилу (**Match**), не удовлетворяют правилу (**Not Match**), удовлетворяют обоим правилам (**Both**) или запись не создается (**None**).
Alert (Предупреждение)	Поставьте флажок в поле **Alert (Предупреждение).** Это означает, что в случае выполнения данного правила будет отправлено предупреждение.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для выхода из экрана без сохранения настроек.
Delete (Удалить)	Щелкните по **Delete (Удалить)** для удаления текущего правила.

12.7.1 Адреса источника и назначения

Чтобы добавить новый адрес источника или назначения, необходимо выбрать в предыдущем экране соответственно **SrcAdd** или **DestAdd**. Для изменения существующего адреса источника или назначения, выбрать его из списка и щелкнуть в предыдущем экране на **SrcEdit** или **DestEdit**. Любое из этих действий приводит к появлению следующего экрана.

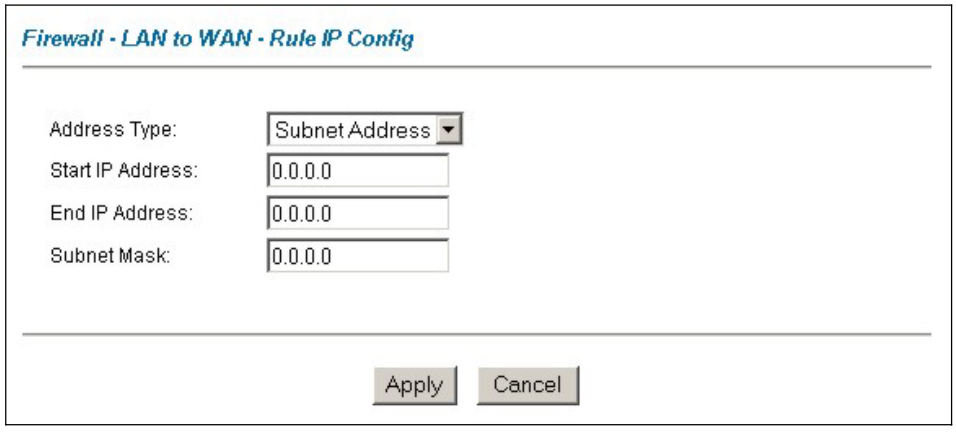


Рис. 12-6 Добавление/Редактирование адресов источника и назначения

В следующей таблице приведены описания полей данного экрана.

Табл.12-5 Добавление/Редактирование адресов источника и назначения

ПОЛЕ	ОПИСАНИЕ
Address Type (Тип адреса)	IP-адрес пакетов, удовлетворяющих данному правилу - может быть одиночный, групповой IP-адрес (например, 192.168.1.10 - 192.169.1.50), подсеть или любой IP-адрес вообще. Выберите соответствующую опцию из следующего раскрывающегося списка: **Single Address (одиночный адрес)**, **Range Address (групповой адрес)**, **Subnet Address (адрес подсети)** и **Any Address (любой адрес).**
Start IP Address(Начальный IP-адрес)	Введите одиночный IP-адрес или начальный IP-адрес в группе.
End IP Address (Конечный IP-адрес)	Введите конечный IP-адрес группы.
Subnet Mask (Маска подсети)	Если нужно, введите маску подсети.
Apply (Применить)	Щелкните по кнопке **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возвращения к ранее сохраненным настройкам.

12.8 Правила

Поля данного экрана Timeout **одинаковы для** локальной сети **и** сети Интернет, **поэтому приведенное ниже описание относится к обеим сетям.**

12.8.1 Факторы, влияющие на выбор значений времени ожидания

Факторы, влияющие на выбор значений времени ожидания те же, что и факторы, влияющие на выбор значений допустимых пределов – см. *раздел 11.4.2*. Щелкните по **Timeout** для настройки **Local Network** или **Internet**.

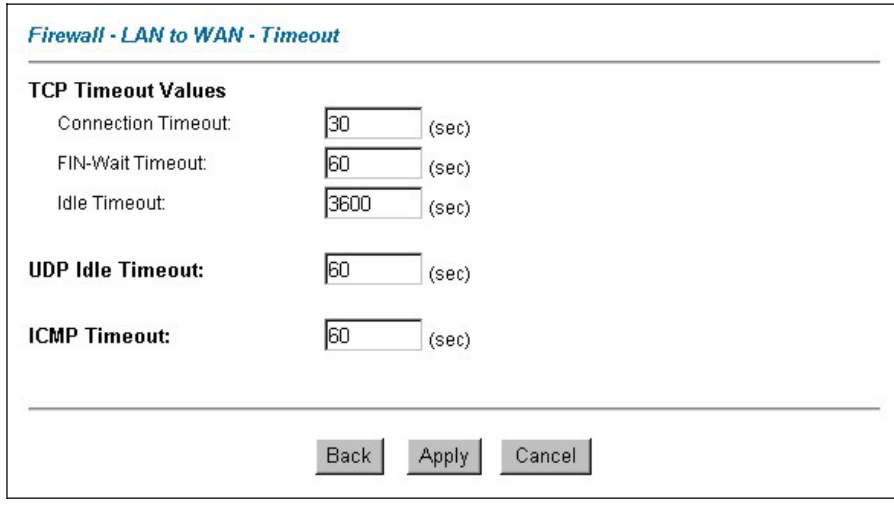


Рис. 12-7 Установка времени ожидания

В следующей таблице приведены описания полей данного экрана.

Табл. 12-6 Настройка времени ожидания

ПОЛЕ	ОПИСАНИЕ
TCP Timeout Values (Значения времени ожидания для TCP)	

Табл. 12-6 Настройка времени ожидания

ПОЛЕ	ОПИСАНИЕ
Connection Timeout (Время ожидания установки соединения)	Введите значение времени в секундах (по умолчанию принято равным 30), определяющее продолжительность времени ожидания OMNI ADSL сессии TCP перед тем как ее сбросить.
FIN-Wait Timeout (Время ожидания FIN)	Введите значение времени в секундах (по умолчанию принято равным 60), определяющее продолжительность сессии TCP после обнаружения межсетевым экраном сообщения FIN-exchange (указывающего на завершение сессии TCP).
Idle Timeout (Тайм-аут простоя)	Введите значение времени в секундах (по умолчанию принято равным 3600), определяющее время бездействия, в течение которого соединение TCP остается открытым, пока OMNI ADSL не закроет его.
UDP Idle Timeout (Тайм-аут простоя UDP)	Введите значение времени в секундах (по умолчанию принятое равным 60), определяющее время бездействия, в течение которого соединение UDP остается открытым, пока OMNI ADSL не закроет его.
ICMP-Timeout (Время ожидания ICMP)	Введите значение времени в секундах (по умолчанию принято равным 60), определяющего продолжительность ожидания отклика ICMP для сессии ICMP.
Back (Назад)	Щелкните по **Back (Назад)**для возвращения к предыдущему экрану.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения настроек и выхода из экрана.
Cancel (Отмена)	Щелкните по **Cancel (Отмена)** для возврата к предыдущей конфигурации.

Chapter 13
Дополнительные услуги

В данной главе описывается создание, просмотр и редактирование услуг по выбору пользователя. Содержание данной главы относится к моделям OMNI ADSL LAN H/HW и OMNI ADSL LAN H-E.

13.1 Введение: дополнительные услуги

Настройка дополнительных услуг и выбор номеров портов, не определенных маршрутизатором OMNI ADSL (см. *Рис.12-5)*. Полный список номеров портов и услуг можно посмотреть на сайте IANA (агентство по назначению имен и уникальных параметров протоколов сети Интернет). Дополнительную информацию по услугам см. в *разделе 12.6.* Для настройки сервиса в экране редактирования правил щелкните по **Edit Available Service (Редактирование перечня доступных услуг)** для вызова следующего экрана.

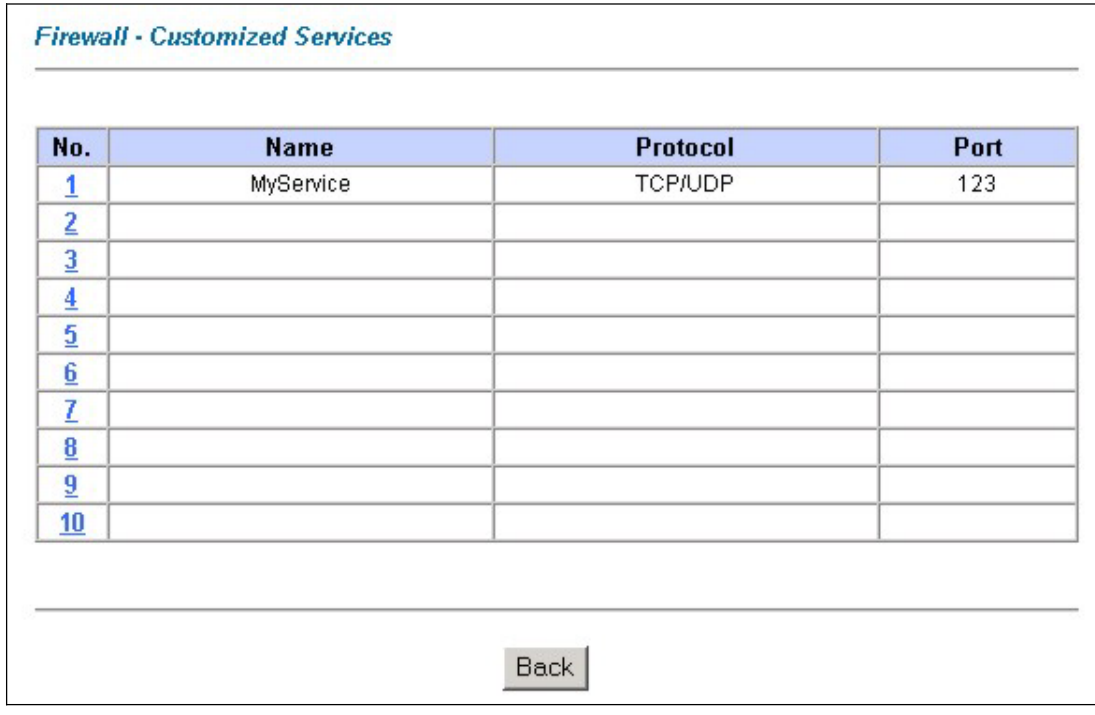


Рис. 13-1 Настройка дополнительных услуг

В следующей таблице приведены описания полей данного экрана.

Табл. 13-1 Настройка дополнительных услуг

ПОЛЕ	ОПИСАНИЕ
Customized Services Дополнительные услуги)	
No.	Номер дополнительно назначаемого порта. Щелкните по полю с порядковым номером услуги для перехода к экрану **Firewall Customized Services Config (Настройка дополнительных услуг межсетевого экрана)** для настройки и редактирования дополнительных услуг.
Name (Имя)	Имя дополнительно назначаемой услуги.
Protocol (Протокол)	Используемый протокол IP (**TCP**, **UDP** или **Both** (оба) для выбранной услуги.
Port (Порт)	Номер порта или группа номеров, соответствующих выбранной услуге.
Back (Назад)	Щелкните по кнопке **Back** для возврата к экрану **Firewall Edit Rule (Правило редактирования настроек межсетевого экрана)**.

13.2 Создание/Редактирование дополнительных услуг

Выберите щелчком номер правила в предыдущем экране для создания нового порта по Вашему выбору или редактирования существующего. Это действие приводит к появлению следующего экрана.

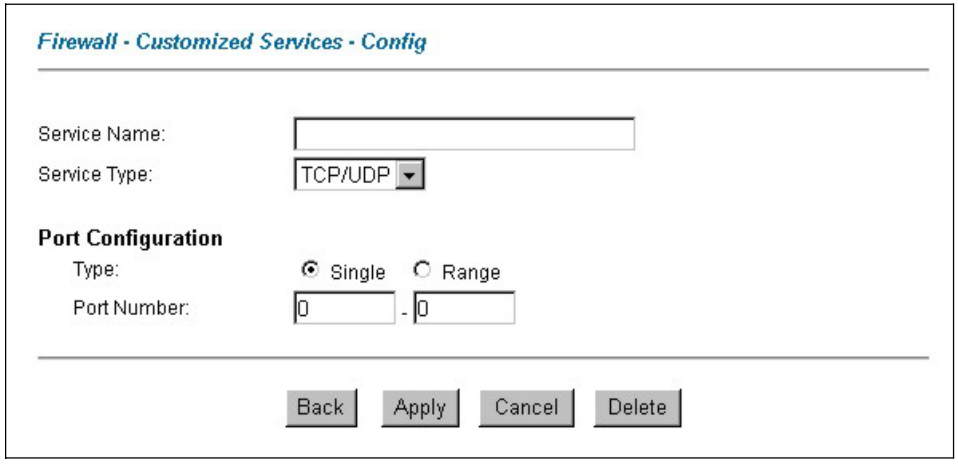


Рис. 13-2 Создание/Редактирование дополнительных услуг

В следующей таблице приведены описания полей данного экрана.

Табл. 13-2 Создание/Редактирование дополнительных услуг

ПОЛЕ	ОПИСАНИЕ
Service Name (Название услуги)	Введите уникальное имя для выбранного порта.
Service Type (Тип услуги)	Выберите из раскрывающегося списка порт IP (**TCP**, **UDP** или **TCP/UDP**) для Вашего дополнительного порта.
Port Configuration (Конфигурация порта)	
Type (Тип)	Выберите **Single** для назначения одного порта или **Range** для нескольких портов для дополнительно назначаемой услуги.
Port Number (Номер порта)	Введите одиночный номер порта или задайте диапазон номеров портов, определяющих выбранную услугу.
Back (Назад)	Щелкните по кнопке **Back (Назад)** для возврата к экрану **Firewall Customized Services**.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения настроек и выхода из экрана.
Cancel (Отмена)	Щелкните по **Cancel (Отмена)** для возврата к ранее сохраненным настройкам.
Delete (Удалить)	Щелкните по кнопке **Delete (Удалить)** для удаления текущего правила.

13.3 Пример задания правил дополнительной услуги межсетевого экрана

Приведенное ниже правило работы межсетевого экрана позволяет получить доступ к гипотетической службе “My Service” в сети Интернет.

Step 1. Щелкните по **Rule Summary (Сводка правил)** под окном **Internet to Local Network Set (настройка подключения ЛВС к сети Интернет)**.

Step 2. Выберите щелчком номер правила для вызова экрана редактирования правил.

Step 3. Отметьте флажком поле **Any** в окне **Source Address**, а затем щелкните по кнопке **ScrDelete**.

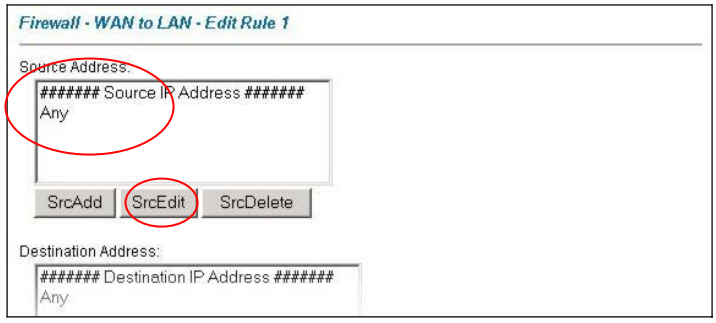


Рис. 13-3 Пример редактирования правил

Step 1. Щелкните по кнопке **ScrAdd** для вызова экрана **Rule IP Config**. Выполните настройку как показано на рисунке и щелкните по кнопке **Apply**.

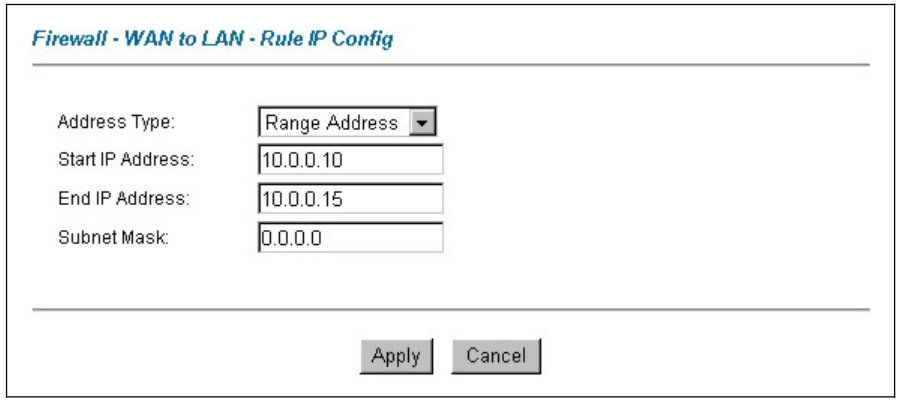


Рис. 13-4 Пример настройки источника IP

Step 5. Щелкните по **Edit Available Service** в экране **Edit rule**, а затем щелчком по номеру правила вызовите экран **Firewall Customized Services Config**. Выполните настройку следующим образом.

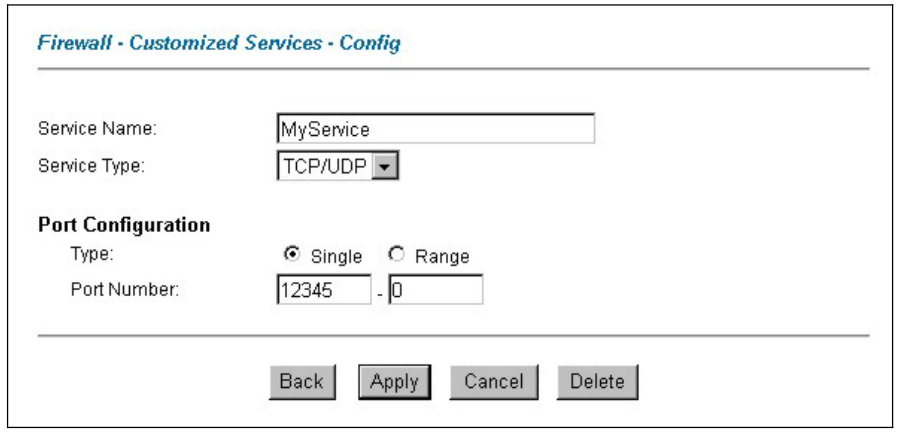


Рис. 13-5 Дополнительная услуга для примера "MyService"

Услуги, заданные пользователем, помечены символом "*" в окне списка Services **и в окне списка Rule Summary. После создания дополнительной услуги щелкните по** Apply**.**

Step 4. Для настройки правил воспользуйтесь процедурами, ранее описанными в данной главе. Выполните настройку экрана конфигурации правил, как показано ниже, для использования в работе.

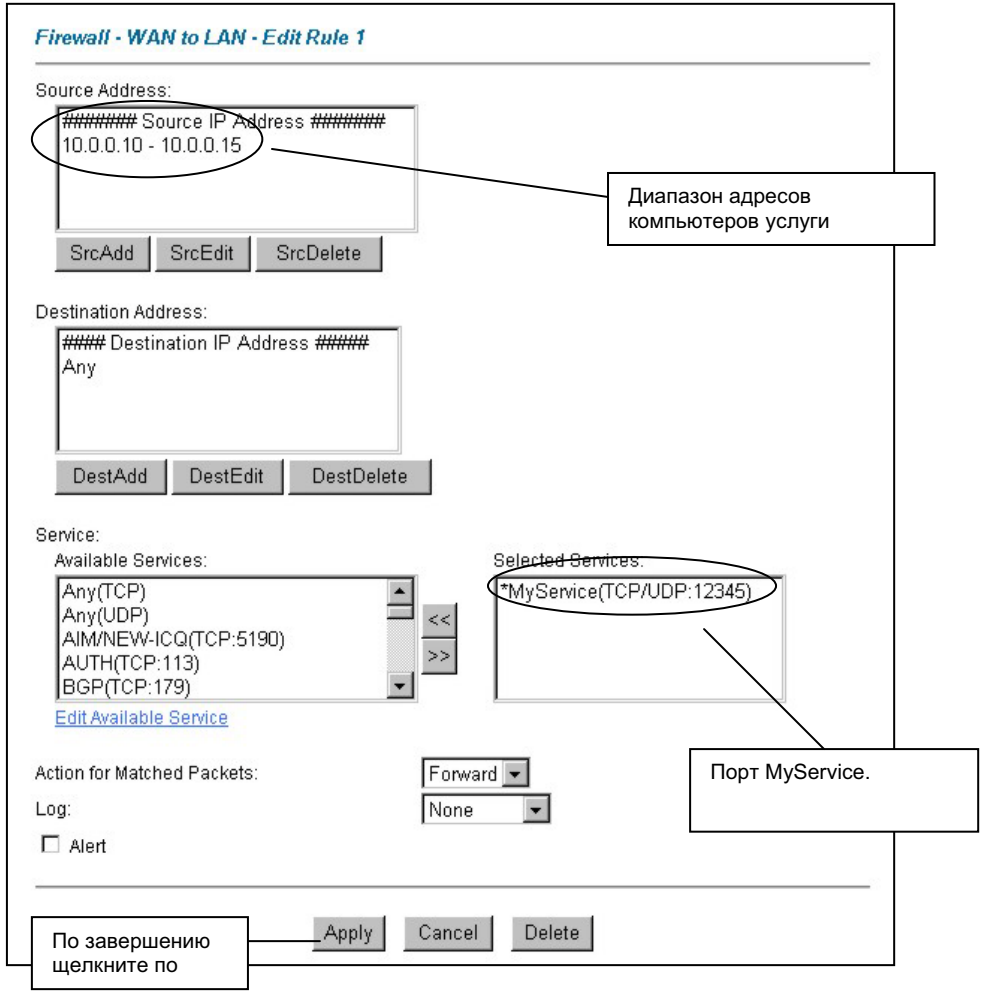


Рис. 13-6 Пример настройки правил ведения системного журнала

Step 6. По окончании процедуры конфигурации, окно **Rule Summary** для данных правил межсетевого экрана, касающихся сети Интернет, должно выглядеть следующим образом. Не забудьте щелкнуть по **Apply** по окончании работы с правилами для сохранения новых настроек в OMNI ADSL.

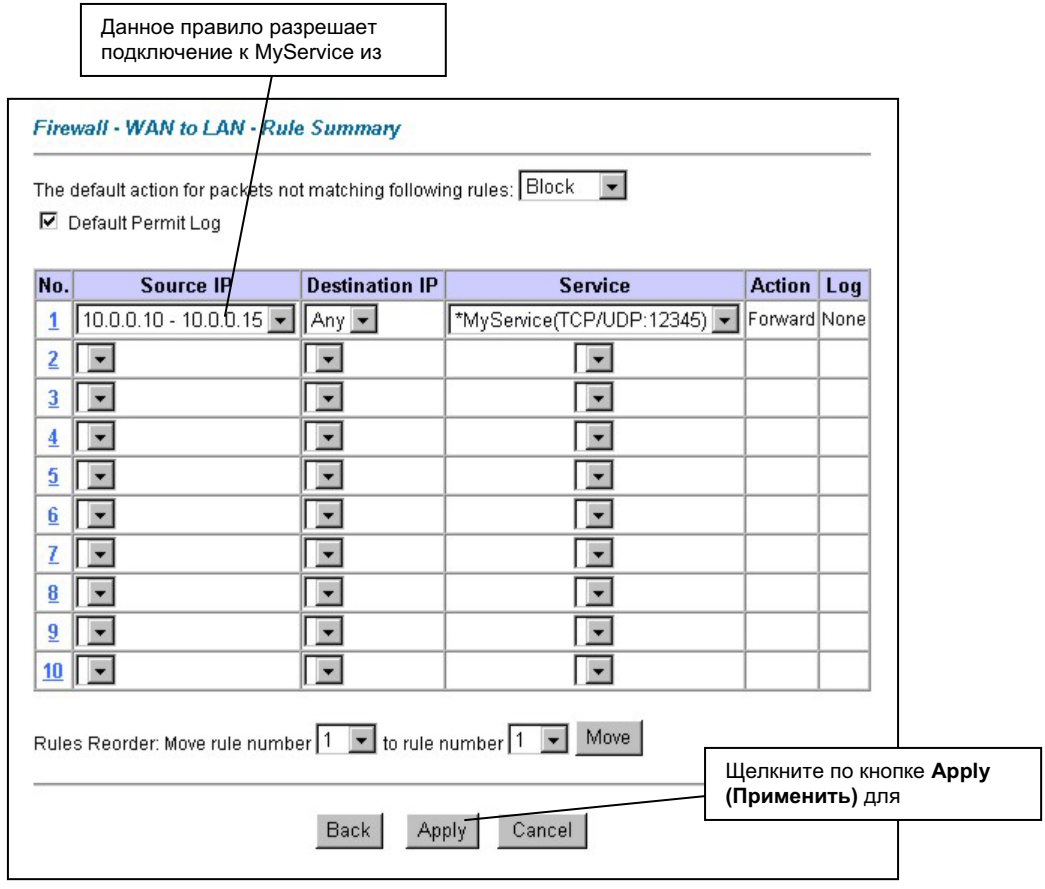


Рис. 13-7 Пример сводки правил

Chapter 14
Контент-фильтрация

В данной главе описывается настройка функций контент-фильтра. Содержание данной главы относится к моделям OMNI ADSL LAN H/HW и P650H-E.

14.1 Описание работы контент-фильтра

Функция контент-фильтрации в сети Интернет позволяет сформулировать и усилить действенность стратегий доступа к ресурсам сети Интернет в соответствии с Вашими потребностями. Функции контент-фильтрации дают возможность включения блокировки доступа к Web-сайтам заданием ключевых слов (по Вашему выбору), находящихся в их URL. Можно также установить расписание работы OMNI ADSL в режиме контент-фильтра, а также указать IP-адреса, пользующиеся доверием, на которые не распространяется действие контент-фильтра.

14.2 Настройка блокировки по ключевым словам

Для включения блокировки сайтов, в URL которых входят определенные ключевые слова, следует пользоваться данным экраном. Например, если в составе ключевых слов используется "bad", OMNI ADSL блокирует доступ ко всем сайтам, в URL которых оно содержится, включая URL http://www.website.com/bad.html, даже если этот сайт не включен в Filter List (Список фильтров).

Для включения блокировки доступа OMNI ADSL к сайтам с помощью задания ключевых слов в их URL-адресах щелкните по **Content Filter** и **Keyword**. Появится экран следующего вида.

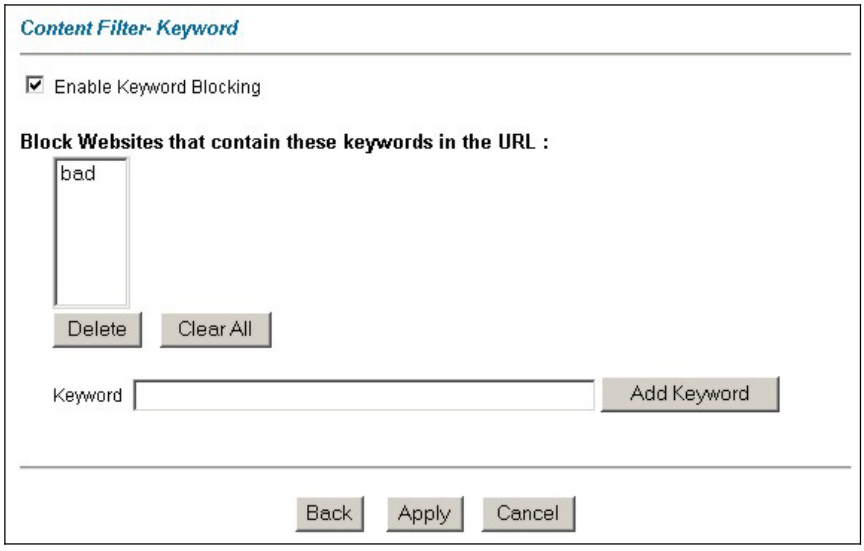


Рис. 14-1 Настройка контент-фильтра: Ключевое слово

В следующей таблице приведены описания полей данного экрана.

Табл. 14-1 Настройка контент-фильтра: Ключевое слово

ПОЛЕ	ОПИСАНИЕ
Enable Keyword Blocking (Включение блокировки по ключевым словам)	Поставьте метку в этом окне для включения данной функции.
Block Websites that contain these keywords in the URL(Блокировка Web-сайтов, имеющих в URL-адресе данные ключевые слова):	В данном окне отображается список ключевых слов для настройки блокировки OMNI ADSL.
Delete (Удалить)	Выделите ключевое слово в окне и щелкните по кнопке **Delete** для его удаления.
Clear All (Очистить все)	Щелкните по **Clear All** для удаления всех ключевых слов из списка.

Табл. 14-1 Настройка контент-фильтра: Ключевое слово

ПОЛЕ	ОПИСАНИЕ
Keyword (Ключевое слово)	Введите в это поле ключевое слово. Можно ввести до 64 любых символов. Не разрешается применение знаков подстановки.
Add Keyword (Добавить ключевое слово)	Щелкните по **Add Keyword (Добавить ключевое слово)** после его набора. Повторите эту процедуру для добавления других ключевых слов. Разрешается использование до 127 ключевых слов. При попытке доступа к сайту, в URL-адресе которого содержится данное ключевое слово, будет получено сообщение о том, что контент-фильтр заблокировал этот запрос.
Back (Назад)	Щелкните по **Back (Назад)**для возврата к предыдущему экрану.
Apply (Применить)	Щелкните по кнопке **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возврата к ранее сохраненным настройкам.

14.3 Настройка расписания

Для указания времени и дней, когда OMNI ADSL будет выполнять функции контент-фильтра, щелкните по **Content Filter** и **Schedule**. Появится экран следующего вида.

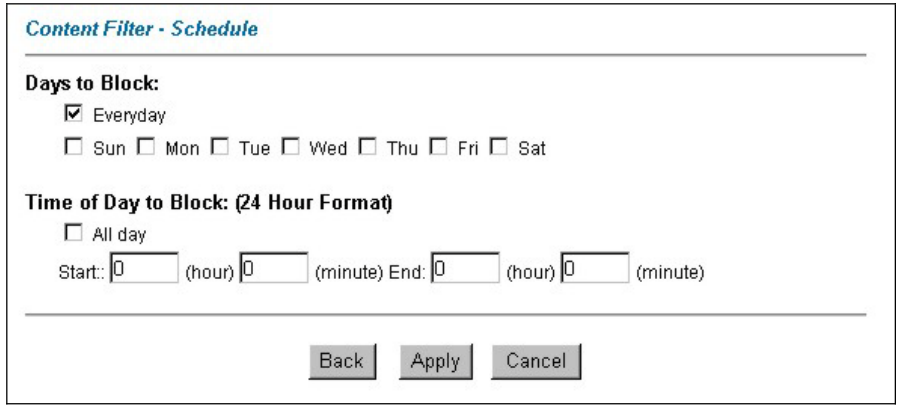


Рис. 14-2 Контент-фильтр: Расписание работы

В следующей таблице приведены описания полей данного экрана.

Табл. 14-2 Контент-фильтр: Расписание работы

ПОЛЕ	ОПИСАНИЕ
Days to Block (Дни работы блокировки):	Отметьте флажками в окне, какие дни недели (или все дни) включены в расписание работы контент-фильтра.
Time of Day to Block (время работы блокировки):	Для назначения временного интервала работы контент-фильтра пользуйтесь 24-часовым форматом (или пометьте флажком окно **All day (Круглосуточно)**).
Back (Назад)	Щелкните по **Back (Назад)**для возврата к предыдущему экрану.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения изменений настройки.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возврата к ранее сохраненным настройкам.

14.4 Настройка списка компьютеров, пользующихся доверием

Для создания списка пользователей ЛВС, на которых не распространяется действие функции контент-фильтра OMNI ADSL щелкните по **Content Filter (Контент-фильтр)** и **Trusted (Пользующийся доверием)**. Появится экран следующего вида.

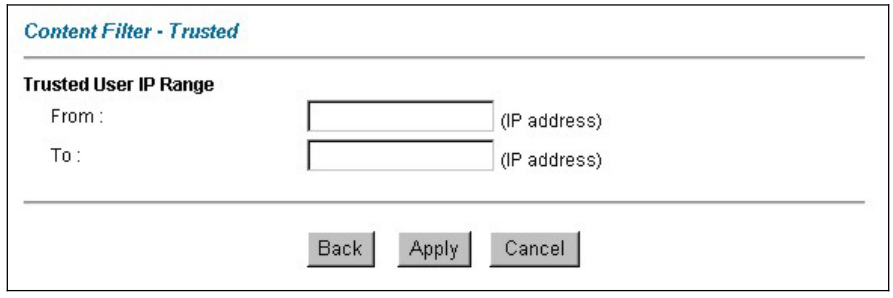


Рис. 14-3 Контент-фильтр: Создание доверительного списка

В следующей таблице приведены описания полей данного экрана.

Табл. 14-3 Контент-фильтр: Создание доверительного списка

ПОЛЕ	ОПИСАНИЕ
Trusted User IP Range (Диапазон IP-адресов доверительного списка пользователей)	
From (От)	Введите IP-адрес отдельного компьютера (или первый адрес заданного диапазона IP-адресов компьютеров) локальной сети, на которые по Вашему желанию не должно распространяться действие функции контент-фильтра.
To (До)	Введите последний адрес заданного диапазона IP-адресов пользователей локальной сети, на которые по Вашему желанию не должно распространяться действие функции контент-фильтра. Оставьте это поле незаполненным, если необходимо включить в список отдельный компьютер.
Back (Назад)	Щелкните по **Back (Назад)**для возврата к предыдущему экрану.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по **Cancel (Отмена)** для возврата к ранее сохраненным настройкам.

14.5 Настройка параметров регистрационных записей

В этом экране записаны результаты выбранных стратегий фильтрации содержания. Щелкните по **Content Filter** и **Logs**. Появится экран следующего вида.

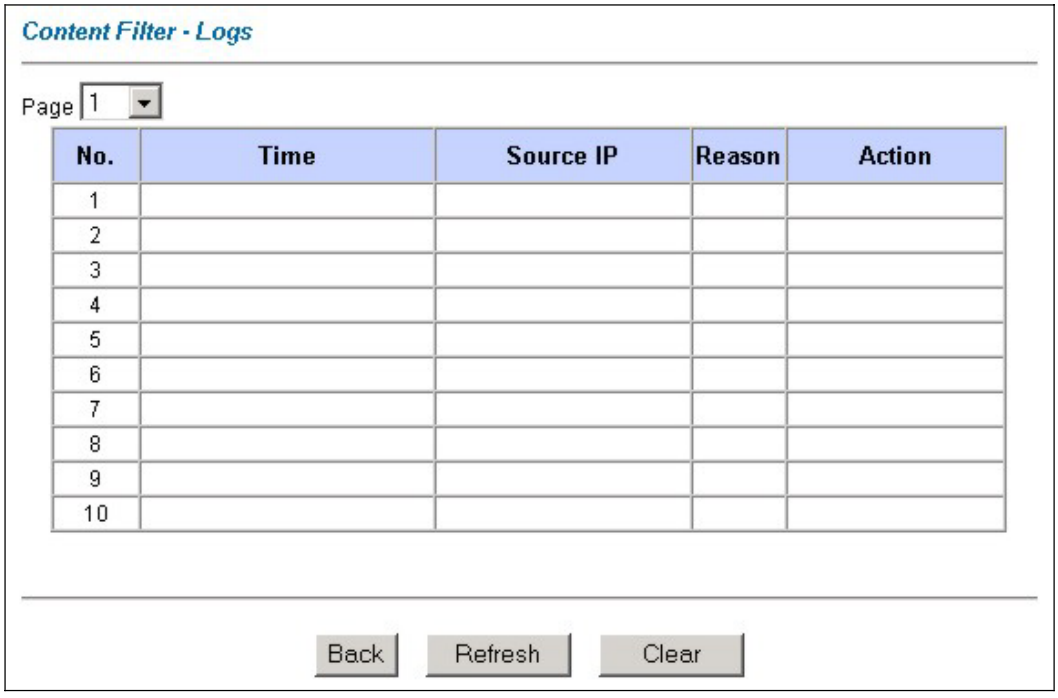


Рис. 14-4 Настройка параметров регистрационных записей контент-фильтра

В следующей таблице приведены описания полей данного экрана.

Табл. 14-4 Настройка параметров регистрационных записей контент-фильтра

ПОЛЕ	ОПИСАНИЕ
Page (Страница)	Выберите страницу регистрационных записей из раскрывающегося списка.
No.	Номер регистрационной записи контент-фильтра.
Time (Время)	В данном поле отображается время регистрации записи.
Source IP (Источник IP)	В этом поле отображается IP-адрес компьютера, обращающегося к Web-сайту.
Reason (Причина)	В данном поле отображается какой параметр настройки контент-фильтра инициировал блокировку доступа. Например: (BLOCK_EXCEPT_TRUSTED_DOMAINS), (BLOCK_UNTRUST_DOMAIN), (BLOCK_KEYWORD), (BLOCK_ACTIVEX), (BLOCK_JAVA_APPLET), (BLOCK_COOKIE), (BLOCK_PROXY), (BLOCK_CYBERNOT).

Табл. 14-4 Настройка параметров регистрационных записей контент-фильтра

ПОЛЕ	ОПИСАНИЕ
Action (Действие)	В данном поле отображается сообщение о том что доступ был разрешен - (**FORWARD**) или заблокирован - (**BLOCK**).
Back (Назад)	Щелкните по **Back (Назад)**для возврата к предыдущему экрану.
Refresh (Обновление)	Щелкните по **Refresh (Обновление)** для обновления экрана отчетов. Отчет также обновляется автоматически после закрытия и повторного открытия экрана.
Clear (Очистка)	Щелкните по **Clear** для удаления всех записей.

Part V:

VPN (Виртуальная частная сеть)/IPSec (Интернет-протокол безопасности передачи данных)

В данной части приводится описание настройки VPN/IPSec для обеспечения безопасности связи.

Chapter 15
Знакомство с IPSec

В данной главе содержатся основные сведения о работе протокола IPSec в виртуальных частных сетях. Содержание данной части относится к моделям OMNI ADSL LAN H/HW.

15.1 Описание виртуальных частных сетей (VPN)

VPN (Virtual Private Network - Виртуальная частная сеть) обеспечивает безопасную передачу данных между сайтами без затрат на выделенные линии "сайт" - "сайт". Безопасная частная виртуальная сеть представляет собой совокупность технологий/служб туннелирования, шифрования, аутентификации, управления доступом и контроля, используемых для передачи трафика через Интернет или другие небезопасные сети, использующие для коммуникаций стек протоколов TCP/IP.

15.1.1 IPSec (Интернет-протокол безопасной передачи данных)

Интернет-протокол безопасной передачи данных (IPSec) - основанная на стандартах реализация VPN, которая предлагает гибкие решения передачи данных в общедоступных сетях, таких как Интернет. IPSec сочетает в себе стандартизованные средства шифрования данных, позволяющие обеспечить конфиденциальность, целостность данных и аутентификацию на уровне IP.

15.1.2 Безопасное соединение

Security Association (SA - Соглашение по безопасности) - договор между двумя сторонами о параметрах защиты, таких как используемые алгоритмы и ключи.

15.1.3 Прочие термины

- **Шифрование**

  Шифрование - это математическая операция преобразования исходных данных, открытых для прочтения, в кодированный (зашифрованный) с помощью "ключа" набор данных. Ключ и открытый текст шифруются с помощью специальной процедуры, в результате чего данные приобретают надежную криптографическую защиту. Дешифрование - процесс, обратный шифрованию: это математическая операция преобразования зашифрованного текста в открытый. Для дешифрования также требуется ключ.

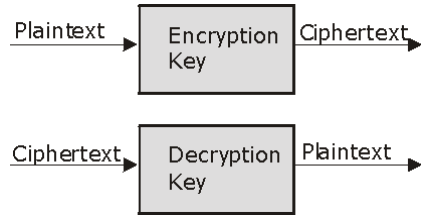


Рис. 15-1 Шифрование и дешифрование

- **Конфиденциальность данных**

  При использовании IPSec отправитель может зашифровать пакеты данных перед их передачей по сети.

- **Целостность данных**

  При использовании IPSec получатель может проверить целостность пакетов данных, переданных отправителем, чтобы убедиться в том, что данные не были изменены в процессе передачи.

- **Аутентификация источника данных**

  Получатель IPSec может сверить источники IPSec-пакетов. Данная функция зависит от целостности данных.

15.1.4 Применения VPN

OMNI ADSL поддерживает следующие приложения VPN.

- **Связь между двумя и более частными сетями**

  Локальные сети филиалов и деловых партнеров можно подключать друг к другу через Интернет, значительно сократив при этом расходы и улучшив производительность, по сравнению с использованием выделенных линий между сайтами.

- **Доступ к сетевым ресурсам с включенной функцией NAT**

  При включенной функции NAT удаленные пользователи не могут получить доступ к хост-компьютерам локальной сети, если только хост не обозначен как общедоступный сервер локальной сети для конкретного протокола. Так как туннель VPN заканчивается внутри локальной сети, удаленным пользователям будут доступны все компьютеры с частными IP-адресами в локальной сети.

- **Неподдерживаемые приложения IP**

  В случае наличия неподдерживаемых приложений IP можно создать туннель VPN.

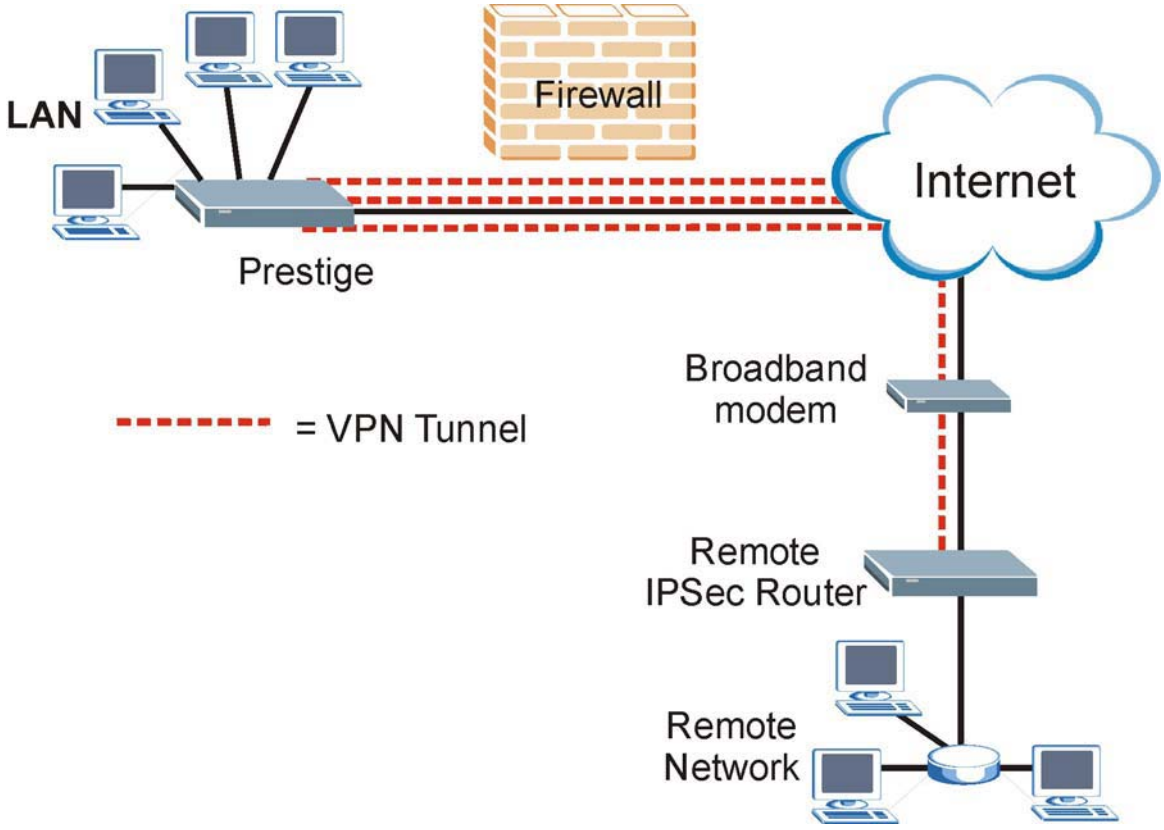


Рис. 15-2 Применение VPN

15.2 Архитектура IPSec

Полная архитектура IPSec приведена ниже.

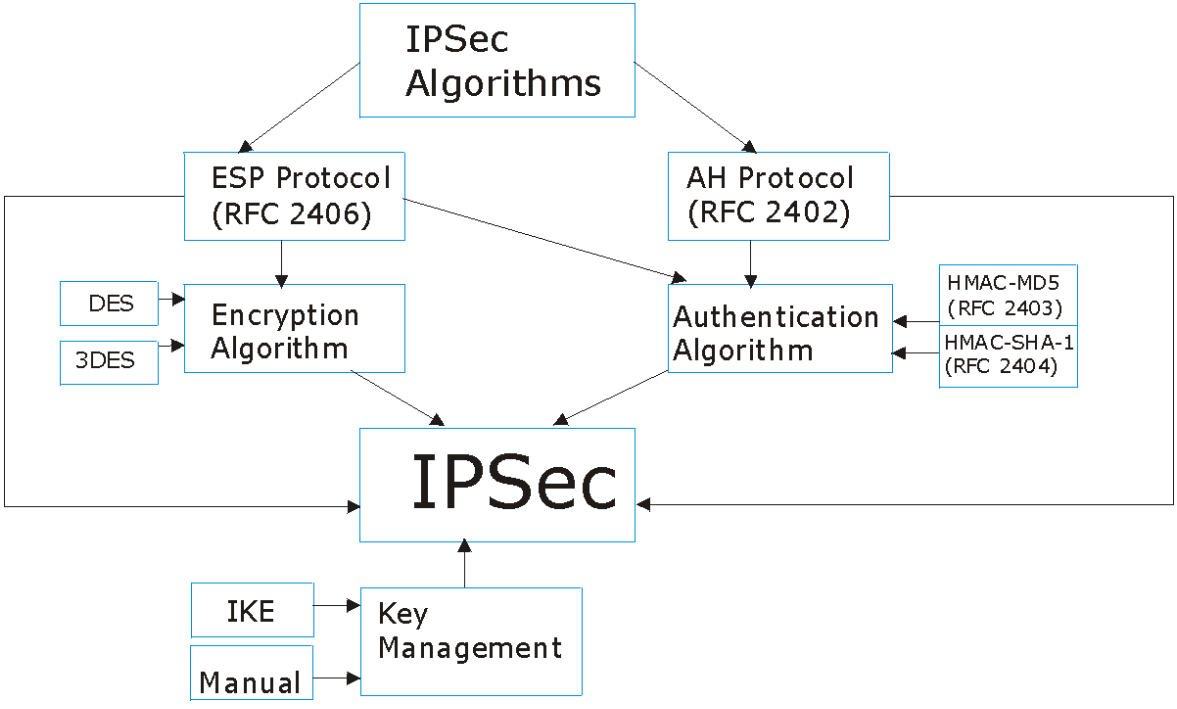


Рис. 15-3 Архитектура IPSec

15.2.1 Алгоритмы IPSec

Протокол **ESP** (Encapsulating Security Payload - Протокол инкапсуляции зашифрованных данных) (RFC 2406) и протокол **AH** (Authentication Header - Аутентифицирующий заголовок) (RFC 2402) определяют форматы пакетов и стандарты структур пакетов, заданные по умолчанию (включая алгоритмы реализации).

Алгоритм шифрования описывает применение таких процедур криптографической защиты, как DES (Data Encryption Standard - Стандарт шифрования данных) и Triple DES (Тройной DES).

Алгоритмы аутентификации HMAC-MD5 (RFC 2403) и HMAC-SHA-1 (RFC 2404) представляют собой механизм аутентификации для протоколов **AH** и **ESP**. Дополнительную информацию см. в *разделе 16.2*.

15.2.2 Управление ключами

Функция управления ключами при настройке виртуальной частной сети позволяет выбрать либо IKE (ISAKMP), либо конфигурацию ключей вручную.

15.3 Инкапсуляция

Для виртуальных частных сетей, работающих по протоколу IPSec, существует два режима работы - **Транспортный** и **Туннельный**.

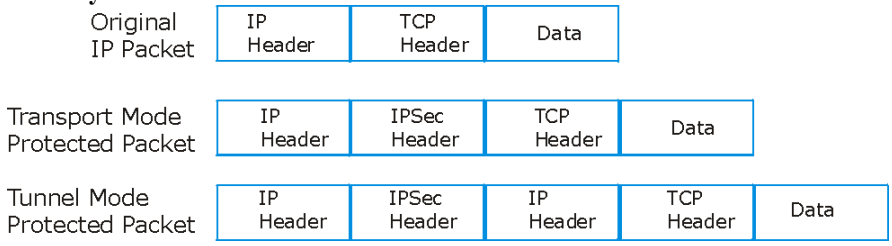


Рис. 15-4 Инкапсуляция IPSec: Транспортный и туннельный режим

15.3.1 Транспортный режим

Транспортный режим используется для защиты сообщений протоколов верхнего уровня и воздействует только на данные пакета IP. В **Транспортном** режиме пакет IP содержит сообщение протокола безопасности (**AH** или **ESP**), расположенное между собственным и дополнительными заголовками IP и следующими данными протоколов более высокого уровня, содержащимися в пакете (такими как TCP и UDP).

В случае применения **ESP** защищенными оказываются только сообщения протоколов более высокого уровня, содержащиеся в пакете. Информация о заголовке и опциях пакета IP не включается в процесс аутентификации. Таким образом, проверка целостности осуществляется только в отношении данных и исходный IP-адрес не может быть проверен.

В случае применения в качестве протокола безопасности **AH**, защита распространяется и на заголовок IP, таким образом осуществляется проверка целостности данных всего пакета путем включения частей исходного заголовка IP в процессе хэширования (добавления хэш-функции).

15.3.2 Туннельный режим

Туннельный режим инкапсулирует весь IP-пакет с целью его безопасной передачи. **Туннельный** режим применяется при использовании шлюзов для доступа к внутренним системам. **Туннельный режим** по существу объединяет функции туннелирования IP, аутентификации и шифрования. Он является самым распространенным режимом работы. **Туннельный режим** применяется для соединений типа "шлюз-шлюз" и "хост-шлюз". При работе в **туннельном** режиме существует два набора заголовков IP:

- **Внешний заголовок:** Внешний заголовок IP содержит IP-адрес назначения шлюза VPN.
- **Внутренний заголовок**: Внутренний заголовок IP содержит IP-адрес назначения конечной системы за шлюзом VPN. Сообщение протокола безопасности размещается между внешним и внутренним заголовками IP.

15.4 IPSec и NAT

Рекомендуется ознакомиться с этим разделом, если Вы пользуетесь IPSec на хост-компьютере за устройством OMNI ADSL.

NAT несовместима с протоколом **AH** как в **транспортном**, так и в **туннельном** режиме. VPN, поддерживающая IPSec и использующая протокол **AH**, добавляет в исходящий пакет (в поля данных и заголовки) значение хэш-функции. При использовании протокола **AH** содержание пакета (поля данных) не шифруется.

Устройство трансляции сетевых адресов между конечными пунктами IPSec замещает адрес либо источника, либо получателя другим адресом, выбирающимся самим устройством. Устройство VPN принимающей стороны проверяет целостность поступающего пакета, вычисляя собственное значение хэш-функции, и сообщает о несовпадении со значением в полученном пакете. Так как устройство VPN принимающей стороны "не знает" о существовании устройства NAT на пути пакета, то оно будет считать это умышленным изменением данных.

IPSec, использующий **ESP** в **туннельном** режиме, инкапсулирует весь исходный пакет (включая заголовки) в новый IP-пакет. Адрес источника в новом пакете - это адрес шлюза VPN на отправляющей стороне, а адрес назначения - адрес устройства VPN на принимающей стороне. При использовании протокола **ESP** с аутентификацией шифруется все содержимое пакета (в данном случае весь первоначальный пакет целиком). К зашифрованному содержанию (новые заголовки не шифруются) пакета добавляется значение хэш-функции.

Протокол **ESP** в **туннельном** режиме с аутентификацией совместим с NAT, так как проверка целостности осуществляется поверх комбинации "исходный заголовок плюс исходные данные", в которую устройством NAT не вносятся изменения. **Транспортный** режим **ESP** с аутентификацией несовместим с NAT.

Табл. 15-1 VPN и NAT

ПРОТОКОЛ БЕЗОПАСНОСТИ	РЕЖИМ	NAT
AH	Транспортный	N
AH	Туннельный	N
ESP	Транспортный	N
ESP	Туннельный	Y

Chapter 16
Экраны VPN

Содержание данной главы позволяет получить общее представление об экранах VPN. См. главу о журналах регистрации для получения дополнительной информации о просмотре журналов и Справочное руководство с описанием журналов IPSec. Содержание данной части относится к моделям OMNI ADSL LAN H/HW.

16.1 Описание VPN/IPSec

Пользуйтесь приведенным в данной главе описанием экранов для настройки правил VPN-соединений и управления виртуальной частной сетью.

16.2 Алгоритмы IPSec

Протоколы **ESP** и **AH** необходимы для создания безопасных соединений (SA) - основы IPSec VPN. Любое безопасное соединение начинается с аутентификации, осуществляющейся протоколами **AH** и **ESP**. Первичной функцией управления ключами является установление и поддержка соединения SA между системами. Передача данных начинается, как только установлено SA.

16.2.1 Протокол AH (Authentication Header - Аутентифицирующий заголовок)

Протокол **AH** (RFC 2402) был разработан для обеспечения целостности, аутентификации и непрерывности последовательности (защита от повторного воспроизведения), а также защиты от отказов, однако этот протокол не решает проблему конфиденциальности информации, в отличие от протокола **ESP**.
В тех приложениях, где конфиденциальность не требуется или не продиктована официально установленными ограничениями по шифрованию данных, для обеспечения целостности достаточно использовать протокол **AH**. Данная реализация не может предотвратить разглашение информации, однако учитывает возможность проверки целостности информации и аутентификации источника.

16.2.2 Протокол ESP (Encapsulating Security Payload - Инкапсуляция зашифрованных данных)

Протокол **ESP** (RFC 2406) осуществляет шифрование данных, а также реализует некоторые услуги протокола **AH**. **Возможности протокола ESP** в части аутентификации являются ограниченными по сравнению с протоколом **AH**, поскольку им не используется информация заголовка IP в ходе

процесса аутентификации. Однако использования протокола **ESP** достаточно, если только не требуется аутентификация с помощью протоколов более высокого уровня.
Дополнительным свойством протокола **ESP** является функция "заполнителя", обеспечивающая дополнительную защиту обмена данными, так как позволяет скрыть истинный размер передаваемого пакета.

Табл. 16-1 Протоколы AH и ESP

ESP	AH
DES (по умолчанию) Data Encryption Standard (Стандарт шифрования данных - DES) - это широко применяемый способ шифрования данных с помощью частного (секретного) ключа. В DES применяется 56-битовый ключ к каждому 64-битовому блоку данных.	**MD5** (по умолчанию) MD5 (Message Digest 5) порождает 128-битовый дайджест для аутентификации пакетных данных.
3DES Стандарт Triple DES (3DES) является разновидностью DES с трехкратным применением трех различных ключей (3 x 56 = 168 бит), таким образом удваивающих эффективность DES.	**SHA1** SHA1 (Secure Hash Algorithm/Алгоритм безопасного хэширования) порождает 160-битовый дайджест для аутентификации пакетных данных.
Выберите **DES**, если необходимо обеспечить минимальную защиту, и **3DES** - для максимальной. Для настройки туннеля без шифрования выберите **NULL**.	Выберите **MD5** для минимальной защиты и **SHA-1** - для максимальной.

16.3 Собственный IP-адрес

В поле **My IP Addr** укажите IP-адрес OMNI ADSL в глобальной сети. Если оставить в этом поле 0.0.0.0, то для установки туннеля VPN OMNI ADSL будет использовать текущий IP-адрес OMNI ADSL в глобальной сети (статический или динамический). Если значение в поле **My IP Addr** меняется после настройки, OMNI ADSL будет вынужден перестраивать туннель VPN.

16.4 Адрес безопасного шлюза

Secure Gateway Addr - это IP-адрес в глобальной сети или имя домена удаленного маршрутизатора IPSec (безопасного шлюза).

Если удаленный безопасный шлюз имеет статический IP-адрес в глобальной сети, укажите его в поле **Secure Gateway Address**. В качестве альтернативы можно в этом поле можно указать имя домена удаленного безопасного шлюза (если таковое имеется).

Можно также ввести значение доменного имени удаленного шлюза безопасности в поле **Secure Gateway Address (Адрес шлюза безопасности)** , если удаленный шлюз безопасности имеет динамический IP-адрес в глобальной сети и использует DDNS. OMNI ADSL должен выполнять настройку туннеля VPN всякий раз при изменении IP-адреса удаленного шлюза безопасности в глобальной сети (поэтому могут быть задержки, связанные с обновлением DDNS серверами IP-адресов удаленных шлюзов в глобальной сети).

16.4.1 Динамический адрес шлюза безопасности

Если удаленный безопасный шлюз имеет динамический IP-адрес в глобальной сети и не поддерживает DDNS, в поле Secure Gateway Addr следует ввести 0.0.0.0. В этом случае инициализацию безопасного соединения может выполнить только удаленный шлюз безопасности. Это может быть полезным для удаленных пользователей, инициирующих туннель VPN к корпоративной сети. См. *раздел 16.16*, где приведены примеры настройки.

В поле Secure Gateway IP Address можно выставить 0.0.0.0 только в случае управления ключами с помощью IKE**, а при** ручном **управлении ключами - нельзя.**

16.5 Экран VPN Summary

Приведенный ниже рисунок помогает объяснить назначение основных компонентов Web-конфигуратора.

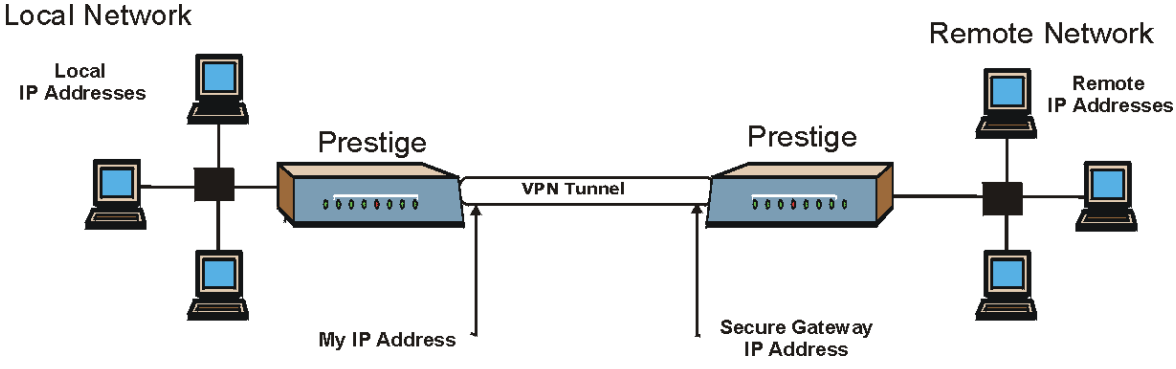


Рис. 16-1 Значения полей меню IPSec

Локальные и удаленные адреса IP должны быть статическими.

Щелкните по **VPN** и **Setup** для вызова экрана **VPN Summary**. Это информационное меню, предназначено для ознакомления (только для чтения) с правилами (туннелями) конкретного применения IPSec. Меню IPSec summary предназначено только для чтения. Отредактируйте VPN, выбрав порядковый номер и выполнив настройку связанных с ним подменю.

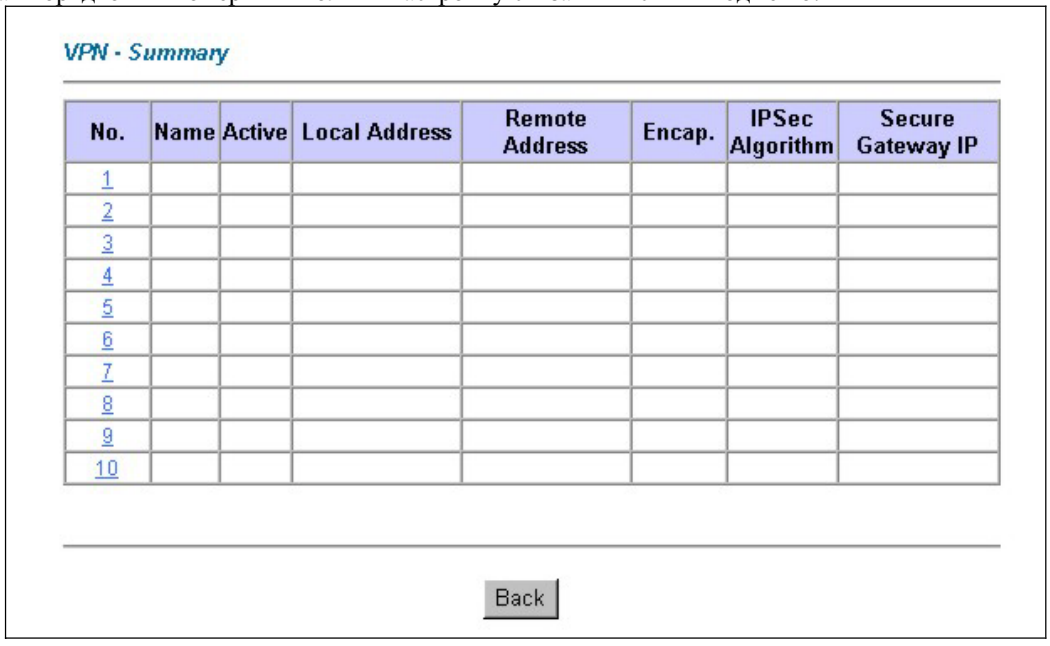


Рис. 16-2 Меню VPN Summary

В следующей таблице приведены описания полей данного меню.

Табл. 16-2 Меню VPN Summary

ПОЛЕ	ОПИСАНИЕ
No.	Индекс стратегии VPN. Для редактирования стратегий VPN щелкните по соответствующему номеру.
Name (Имя)	В этом поле указывается уникальное идентификационное имя данной стратегии VPN.
Active (Активно)	Данные поля отображаются независимо от того, является ли стратегия VPN активной или нет. Символ "Y" обозначает, что данная стратегия VPN является активной.

Табл. 16-2 Меню VPN Summary

ПОЛЕ	ОПИСАНИЕ
Local Address (Локальный адрес)	Это IP-адрес(-а) компьютеров локальной сети, находящиеся за устройством OMNI ADSL.
Remote Address (Удаленный адрес)	Это IP-адрес(-а) компьютеров удаленной сети, находящихся за удаленным маршрутизатором IPSec router.
Encap (Инкапсуляция)	В этом поле отображается признак режима **Tunnel** или **Transport**.
IPSec Algorithm (Алгоритм IPSec)	В этом поле указываются протоколы безопасности, используемые для соединения SA. Как AH, так и ESP требуют повышения производительности OMNI ADSL при обработке данных и увеличивают время установления (задержки связи).
Secure Gateway IP (IP-адрес шлюза безопасности)	Это IP-адрес удаленного маршрутизатора IPSec. Это должен быть фиксированный, общедоступный IP address для трафика, проходящего по сети Интернет.
Back (Назад)	Щелкните по **Back** для возврата к предыдущему экрану.

16.6 Функция Keep Alive (Поддержание активности)

При инициализации туннеля IPSec с включенной опцией "keep alive", OMNI ADSL автоматически восстанавливает туннель по истечении периода существования IPSec SA (см. *раздел 16.10* для получения дополнительной информации по данному вопросу). Вследствие этого после инициализации туннель IPSec становится “постоянно включенным” соединением. Для реализации данной возможности оба IPSec маршрутизатора должны иметь включенными OMNI ADSL-совместимые функции поддержания соединения ("keep alive").

Если OMNI ADSL работает одновременно с максимальным количеством туннелей IPSec с включенной функцией поддержания соединения, ни один дополнительный туннель не сможет подключиться к OMNI ADSL, поскольку устройство никогда не сбросит уже подключенные туннели. Проверьте по *Табл. 1-1 Model Specific Features (Специальные характеристики модели)* в главе 1, какое количество одновременно работающих туннелей IPSec SAs может поддерживать ваша модель OMNI ADSL.

Ситуация наличия выходного трафика при отсутствии входного вызывает автоматический сброс туннеля устройством OMNI ADSL в течение двух минут.

16.7 Тип адреса и его значение

Поддерживая активный режим согласования (см. *раздел 16.10.1*), OMNI ADSL осуществляет идентификацию входящих безопасных соединений SA по типу адреса и его значению, в случае если идентификационная информация не зашифрована. Это позволяет OMNI ADSL различать многочисленные правила для безопасных соединений, осуществляемых удаленными маршрутизаторами IPSec с динамическими IP-адресами глобальной сети. Для одновременного подключения к OMNI ADSL через маршрутизаторы IPSec с динамическими адресами (см. *раздел 16.17.2* для ознакомления с примером настройки удаленного пользователя) удаленные пользователи могут применять различные пароли .

В основном режиме (см. *раздел 16.10.1*) тип адреса и его значение зашифрованы в целях защиты конфиденциальности. В этом случае OMNI ADSL может различить только до восьми входящих SA-соединений от удаленных маршрутизаторов IPSec с динамическими IP-адресами в глобальной сети. OMNI ADSL может различать до восьми входящих SA-соединений, поскольку при настройке правил VPN можно выбрать только один из двух алгоритмов шифрования (DES или 3DES), один из двух алгоритмов аутентификации (MD5 или SHA1) и один из двух ключей групп (DH1 или DH2) (см. *раздел 16.11*). Тип адреса и его значение действуют как дополнительный уровень процедур идентификации для входящих SA-соединений.

Различным типам адресов соответствуют: имя домена, IP-адрес или E-Mail адрес, а типам значений – соответствующие значения типов адресов.

Табл. 16-3 Поля "тип адреса" и его значение

ТИП ЛОКАЛЬНОГО АДРЕСА=	ЗНАЧЕНИЕ=
IP	Введите в это поле значение типа IP-адреса Вашего компьютера или оставьте его незаполненным, для того чтобы OMNI ADSL автоматически пользовался своим собственным IP-адресом.
DNS	Введите имя домена (до 31 символа) для идентификации данного устройства OMNI ADSL.
E-mail	Введите E-Mail адрес (до 31 символа) для идентификации данного устройства OMNI ADSL.
Имя домена или E-Mail адрес, набранные в поле **Content**, используются только для идентификации и не являются фактическими.	

Табл. 16-4 Поля "тип адреса клиентского устройства" и его значение

ТИП АДРЕСА КЛИЕНТСКОГО УСТРОЙСТВА=	ЗНАЧЕНИЕ=
IP	Введите в это поле IP-адрес компьютера, с которым устанавливается соединение VPN или оставьте его незаполненным, для того чтобы OMNI ADSL автоматически пользовался адресом, указанным в поле **Secure Gateway Address**.
DNS	Введите имя домена (до 31 символа) для идентификации удаленного маршрутизатора IPSec.
E-mail	Введите E-Mail адрес (до 31 символа) для идентификации удаленного маршрутизатора IPSec.
Имя домена или E-Mail адрес, набранные в поле **Content**, используются только для идентификации и не являются фактическими. Имя домена также не должно совпадать с IP-адресом удаленного маршрутизатора или набранным ниже в поле **Secure Gateway Address**.	

16.7.1 Примеры типов адресов и их значений

Два маршрутизатора IPSec должны иметь подходящие типы адресов и их значений для настройки туннеля VPN.
Два устройства OMNI ADSL в этом примере могут выполнить согласование и установить туннель VPN.

Табл. 16-5 Примеры подходящих настроек типов адресов и их значений

OMNI ADSL A	OMNI ADSL B
Local ID type (Тип локального адреса): E-mail	Local ID type (Тип локального адреса): IP
Local ID content (Значение локального адреса): tom@yourcompany.com	Local ID content (Значение локального адреса): 1.1.1.2
Peer ID type (Тип адреса клиентского устройства): IP	Peer ID type (Тип адреса клиентского устройства): E-mail
Peer ID content (Значение адреса клиентского устройства): 1.1.1.2	Peer ID content (Значение адреса клиентского устройства): tom@yourcompany.com

Два устройства OMNI ADSLs в этом примере не могут завершить согласование, поскольку локальным типом адреса устройства OMNI ADSL B **Local ID type** является **IP**, а типа адреса устройства OMNI ADSL A **Peer ID type** установлен как **E-mail**. В журнале IPSEC LOG появится сообщение “ID mismatched” ("несоответствие адреса").

Табл. 16-6 Пример случая несоответствия настроек типов адресов и их содержания

OMNI ADSL A	OMNI ADSL B
Local ID type (Тип локального адреса): IP	**Local ID type (Тип локального адреса):IP**
Local ID content (Значение локального адреса): 1.1.1.10	Local ID content (Значение локального адреса): 1.1.1.10
Peer ID type (Тип адреса клиентского устройства):E-mail	Peer ID type (Тип адреса клиентского устройства): IP
Peer ID content (Значение адреса клиентского устройства): aa@yahoo.com	Peer ID content (Значение адреса клиентского устройства): N/A

16.8 Pre-Shared Key (Предварительно согласованный ключ)

Предварительно согласованный ключ служит для идентификации участника во время 1-й фазы согласования по обмену ключами (IKE) (см. *раздел 16.10* для получения дополнительной информации о фазах IKE). Ключ называется “предварительно согласованным”, так как его необходимо сообщить партнеру до установления связи через безопасное соединение.

16.9 Редактирование стратегий VPN

Щелкните по номеру (**No.**) в экране **Summary** для редактирования стратегий VPN.

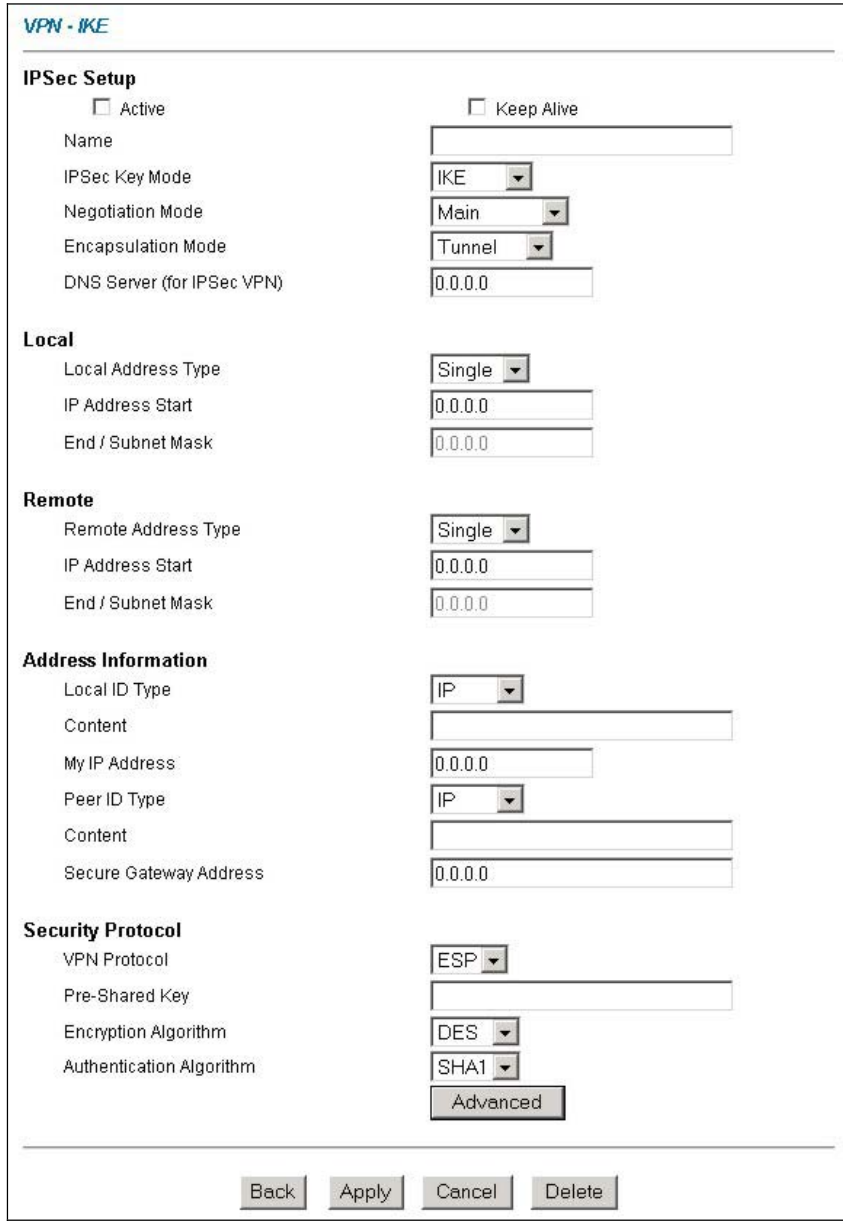


Рис. 16-3 Согласование обмена ключами VPN

В следующей таблице приведены описания полей данного меню.

Табл. 16-7 Согласование обмена ключами VPN

ПОЛЕ	ОПИСАНИЕ
IPSec Setup	
Active (Активно)	Поставьте метку в этом окне, чтобы активировать данную стратегию VPN.
Keep Alive (Поддержание активности)	Выберите **Yes** или **No** из раскрывающегося списка. Выберите опцию **Yes** для автоматической повторной инициализации устройством OMNI ADSL SA-соединения по истечению времени жизни, даже при отсутствии трафика. Удаленный маршрутизатор IPSec также должен иметь включенной функцию поддержания соединения для ее выполнения.
Name (Имя)	Введите до 32 символов для идентификации вашей стратегии VPN. Для этого можно пользоваться любыми символами, включая пробелы, однако OMNI ADSL удаляет пробелы в конце строки.
IPSec Key Mode (Режим ключ IPSec)	Выберите **IKE** или **Manual** из раскрывающегося списка. **Ручное** управление ключами является полезной опцией для поиска и устранения неисправностей в случае, если возникают какие-либо проблемы при использовании **IKE**.
Negotiation Mode (Режим согласования)	Выберите **Main** или **Aggressive** из раскрывающегося списка. Для нескольких SA-соединений через безопасный шлюз должен быть установлен один и тот же режим согласования.
Encapsulation Mode (Режим инкапсуляции)	Выберите из раскрывающегося списка режим **Tunnel** или режим **Transport** .
DNS Server (for IPSec VPN) (Сервер DNS (для IPSec VPN))	Если имеется частный сервер DNS, обслуживающий VPN, введите здесь его IP-адрес. OMNI ADSL назначает этот дополнительный сервер DNS клиентам DHCP устройства OMNI ADSL, имеющим IP-адреса в диапазоне, установленном правилом IPSec, или локальные адреса. Сервер DNS помогает клиентам VPN отыскать другие компьютеры и серверы VPN по их (частным) доменным именам.

Табл. 16-7 Согласование обмена ключами VPN

ПОЛЕ	ОПИСАНИЕ
Local (Местный адрес)	Удаленные IP-адреса должны быть статическими и соответствовать заданным локальным IP-адресам удаленного маршрутизатора IPSec. Два активных SA-соединения не могут иметь один и тот же локальный и удаленный IP-адрес (адреса) одновременно. Два активных SA-соединения могут иметь один и тот же локальный или удаленный IP-адрес, но не оба сразу. Можно сконфигурировать несколько SA-соединений между одинаковыми локальными и удаленными IP-адресами, но при этом активным в любой момент времени может быть только одно из них.
Local Address Type (Типы локальных адресов)	Следует воспользоваться выпадающим меню для выбора опций **Single (Единичный)**, **Range (Диапазон)** или **Subnet (Подсеть)**. Выберите **Single** для единичного IP-адреса. Для нескольких адресов подряд выберите **RANGE**. Чтобы указать в качестве IP-адресов в сети значение их маски подсети, выберите **SUBNET**.
Start IP Address (Начальный IP-адрес)	Если в поле Local **Address Type** указано **Single**, введите в данное поле IP-адрес (статический) локальной сети, расположенной за устройством OMNI ADSL . Если в поле Local **Address Type** указано **Range**, введите в данное поле первый из диапазона IP-адрес (статический) компьютеров локальной сети, расположенной за устройством OMNI ADSL. Если в поле Local **Address Type** указано **Subnet**, введите в данное поле IP-адрес (статический) локальной сети, расположенной за устройством OMNI ADSL. .
End / Subnet Mask (Последний адрес/Маска подсети)	Если в поле **Local Address Type** указано **Single**, повторите здесь IP-адрес из поля **IP Address Start**. Если в поле Local **Address Type** указано **Range**, введите в данное поле последний статический адрес из диапазона IP-адресов компьютеров в локальной сети, расположенной за устройством OMNI ADSL. Если в поле **Local Address Type** указано **SUBNET**, то в данном поле отображается маска подсети для локальной сети, расположенной за OMNI ADSL.

Табл. 16-7 Согласование обмена ключами VPN

ПОЛЕ	ОПИСАНИЕ
Remote (Удаленный)	Удаленные IP-адреса должны быть статическими и соответствовать заданным локальным IP-адресам удаленного маршрутизатора IPSec. Содержимое этих полей не имеет значения, если в поле **Secure Gateway Address** введен код 0.0.0.0. В этом случае только удаленный маршрутизатор IPSec может инициализировать VPN. Два активных соединения SA не могут пользоваться одним и тем же локальным и удаленным IP-адресом (или адресами) одновременно. Два активных соединения SA могут пользоваться одним и тем же локальным или удаленным IP-адресом, но не обоими сразу. Можно сконфигурировать несколько соединений SA между одинаковыми локальным и удаленным IP-адресами, но при этом активным в любой момент времени может быть только одно из них.
Remote Address Type (Тип удаленного адреса)	Следует воспользоваться выпадающим меню для выбора опций **Single (Единичный)**, **Range (Диапазон)** или **Subnet (Подсеть)**. Для единичного IP-адреса выберите **SINGLE**. Для нескольких адресов подряд выберите **RANGE**. Чтобы указать в качестве IP-адресов в сети значение маски подсети, выберите **SUBNET**.
Start IP Address (Начальный IP-адрес)	Если в поле **Remote Address Type** указано **Single**, введите в данное поле IP-адрес (статический) в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Remote Address Type** указано **Range**, введите в данное поле первый из диапазона IP-адрес (статический) компьютеров в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Remote Address Type** указано **Subnet**, введите в данное поле IP-адрес (статический) в сети, расположенной за удаленным маршрутизатором IPSec.
End / Subnet Mask (Последний адрес/Маска подсети)	Если в поле **Remote Address Type** указано **Single**, повторите здесь IP-адрес из поля **IP Address Start**. Если в поле **Remote Address Type** указано **Range**, введите в данное поле значение последнего из диапазона IP-адреса (статического) компьютеров в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Remote Address Type** указано **SUBNET**, введите в данное поле значение маски подсети в сети, расположенной за удаленным маршрутизатором IPSec.
Address Information (Адресная информация)	

Табл. 16-7 Согласование обмена ключами VPN

ПОЛЕ	ОПИСАНИЕ
Local ID Type (Тип локального адреса)	Выберите опцию **IP** для идентификации данного маршрутизатора OMNI ADSL по его IP-адресу. Выберите опцию **DNS** для идентификации данного маршрутизатора OMNI ADSL по его доменному имени. Выберите опцию **E-mail** для идентификации данного маршрутизатора OMNI ADSL по его E-Mail адресу.
Content (Значение)	Если в поле **Local ID Type** выбрана опция **IP**, введите IP-адрес Вашего компьютера или оставьте это поле незаполненным для того, чтобы маршрутизатор OMNI ADSL мог автоматически использовать свой собственный IP-адрес. Если в поле **Local ID Type** выбрана опция **DNS**, введите значение доменного имени (до 31 символа) для идентификации данного устройства OMNI ADSL. Если в поле **Local ID Type** выбрана опция **E-mail**, введите любой E-Mail адрес (до 31 символа) для идентификации данного устройства OMNI ADSL. Имя домена или E-Mail адрес, набранные в поле **Content**, используются только для идентификации и не являются фактическими.
My IP Address (Собственный IP-адрес)	Введите IP-адрес OMNI ADSL в глобальной сети. Если в этом поле оставить значение 0.0.0.0, то при открытии туннеля VPN OMNI ADSL будет использовать свой текущий IP-адрес в глобальной сети (статический или динамический). При изменении IP-адреса туннель VPN должен быть перестроить.
Peer ID Type (Тип адреса клиентского устройства)	Выберите опцию **IP** для идентификации удаленного маршрутизатора IPSec по его IP-адресу. Выберите опцию **DNS** для идентификации удаленного маршрутизатора IPSec по его доменному имени. Выберите опцию **E-mail** для идентификации удаленного маршрутизатора по его E-Mail адресу.

Табл. 16-7 Согласование обмена ключами VPN

ПОЛЕ	ОПИСАНИЕ
Content (Значение)	При выборе опции **IP** в поле **Peer ID Type**, введите тип IP-адреса компьютера, с которым будет устанавливаться соединение VPN, или оставьте его незаполненным, для того чтобы OMNI ADSL автоматически пользовался адресом из поля **Secure Gateway Address**. Если в поле **Peer ID Type** выбрана опция **DNS**, введите значение доменного имени (до 31 символа) для идентификации удаленного маршрутизатора IPSec. . Если в поле **Peer ID Type** выбрана опция **E-mail**, введите любой E-Mail адрес (до 31 символа) для идентификации маршрутизатора IPSec. Имя домена или E-Mail адрес, набранные в поле **Content**, используются только для идентификации и не являются фактическими. Имя домена также не должно совпадать с IP-адресом удаленного маршрутизатора или набранным ниже в поле **Secure Gateway Address**.
Secure Gateway Address (Адрес безопасного шлюза)	В этом поле указывается IP-адрес в глобальной сети или URL (до 31 символа) маршрутизатора IPSec, с которым устанавливается VPN-соединение. Если удаленный маршрутизатор IPSec имеет динамический IP-адрес в глобальной сети, в данном поле необходимо выставить **0.0.0.0** (в поле **Key Mode** должно быть указано **IKE**).
Security Protocol (Протокол обеспечения безопасности)	
VPN Protocol (Протокол VPN)	Выберите опцию **ESP** , если хотите воспользоваться протоколом ESP (Enacapsulation Security Payload - инкапсулирующей защиты содержимого). Протокол ESP (RFC 2406) поддерживает шифрование, а также некоторые услуги протокола **AH**. Если на данном этапе выбрана опция **ESP**, следует назначить опции в полях **VPN Setup** и **Authentication Algorithm** (описанных ниже).
Pre-Shared Key (Предварительно согласованный ключ)	Введите в этом поле тип Вашего предварительно согласованного ключа . Предварительно согласованный ключ идентифицирует участника в первой фазе согласования по обмену ключами. Ключ называется "предварительно согласованным", так как его необходимо сообщить партнеру до установления связи через безопасное соединение. Для нескольких SA- соединений через безопасный шлюз должен использоваться один и тот же предварительно согласованный ключ.

Табл. 16-7 Согласование обмена ключами VPN

ПОЛЕ	ОПИСАНИЕ
Encryption Algorithm (Алгоритм шифрования)	Выберите из раскрывающегося списка опцию **DES**, **3DES** или **NULL**. При использовании стандарта **DES** как отправляющая, так и принимающая сторона должны знать один и тот же секретный ключ, с помощью которого осуществляется шифрование и дешифрование сообщений, а также генерация и проверка аутентификационного кода сообщений. В OMNI ADSL алгоритмом шифрования DES используется 56-битовый ключ. Алгоритм Triple DES (**3DES**) - это разновидность DES, использующего 168-битовый ключ. Как следствие, алгоритм 3DES надежнее протокола DES. Однако он требует большей производительности системы, что отражается в увеличении времени ожидания и в уменьшении пропускной способности. Для настройки туннеля без шифрования выбрать **NULL**. При выборе **NULL** шифровальные ключи не указываются.
Authentication ALgorithm (Алгоритм аутентификации)	Выберите из раскрывающегося списка опцию **SHA1** или **MD5**. Для аутентификации пакетных данных используются алгоритмы хэширования **MD5** (Message Digest 5 - Дайджест сообщения 5) и **SHA1** (Secure Hash Algorithm - Алгоритм безопасного хэширования). Алгоритм SHA1 в целом более надежен, чем **MD5**, но несколько медленнее. Выберите **MD5** для минимальной защиты и **SHA-1** - для максимальной.
Advanced (Дополнительные настройки)	Щелкните по **Advanced (Дополнительные настройки)** для установки дополнительных настроек управления ключом IKE.
Back (Назад)	Щелкните по **Back (Назад)**для возврата к предыдущему экрану.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по **Cancel (Удалить)** для повторной настройки данного экрана.
Удалить	Щелкните по кнопке **Delete** для удаления текущего правила.

16.10 Фазы IKE

Существуют две фазы согласования по протоколу IKE (Internet Key Exchange - Обмен ключами в Интернет) – фаза 1 (аутентификация) и фаза 2 (обмен ключами). В первой фазе устанавливается SA-соединение для обмена ключами IKE, во второй фазе это соединение SA используется для согласования по установлению SA-соединений для IPSec.

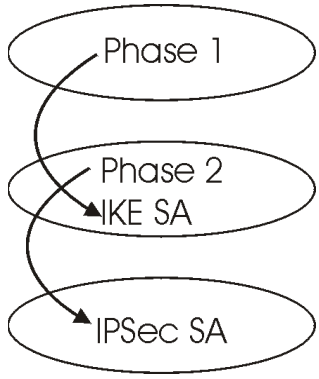


Рис. 16-4 Две фазы создания соединения/соглашения по безопасности SA по IPSec

В первой фазе необходимо выполнить следующие действия:

- Выбрать режим согласования.
- Аутентифицировать соединение с помощью предварительно согласованного совместно используемого ключа.
- Выбрать алгоритм шифрования.
- Выбрать алгоритм аутентификации.
- Выбрать группу ключей по методу шифрования Диффи-Хеллмана с помощью открытого ключа (**DH1** или **DH2**).
- Установить время существования соединения SA для обмена ключами по протоколу IKE. В данном поле указывается продолжительность соединения SA для IKE, по истечении которого оно прерывается. Соединение SA для IKE автоматически отключается в случае превышения установленной продолжительности его существования. Если происходит отключение SA для IKE при уже установленном соединении SA для IPSec, последнее остается подключенным.

Во второй фазе необходимо выполнить следующие действия:

- Выбрать протокол, который будет использоваться для обмена ключами (**ESP** или **AH**).
- Выбрать алгоритм шифрования.
- Выбрать алгоритм аутентификации
- Выбрать поддержку "идеальной прямой безопасности" (Perfect Forward Secrecy, PFS) путем применения метода шифрования Диффи-Хеллмана с открытым ключом – см. *раздел 16.10.3*. Для отключения функции PFS - выбрать **None** (заданную по умолчанию).
- Выбрать режим **Tunnel** (туннельный) или **Transport** (транспортный) .
- Установить время существования соединения SA для обмена ключами по протоколу IPSec. В данном поле указывается продолжительность соединения SA для IPSec, по истечении которого оно прерывается. OMNI ADSL автоматически повторяет согласование SA для IPSec при наличии трафика в случае превышения периода существования SA для IPSec. OMNI ADSL также автоматически повторяет согласование SA для IPSec, в случае включения функции поддержания соединений на обоих

маршрутизаторах даже при отсутствии трафика. При отключении SA для IPSec маршрутизатор IPSec должен произвести повторное согласование SA, когда кто-либо попытается отправить трафик.

16.10.1 Режим согласования

Выбор **Negotiation Mode** (Режим согласования) определяет порядок создания Security Association (SA - Соглашение по безопасности) для каждого соединения по договору об обмене ключами (IKE).

- **Main Mode** (Основной режим) устанавливает высший уровень безопасности в процессе аутентификации сторон (фаза 1). В этом режиме используется 6 сообщений во время трех сеансов обмена данными, включая: согласование SA, обмен по методу Диффи-Хеллмана и обмен случайно выбранным числом. Этот режим обеспечивает защиту конфиденциальности сторон (информация об участниках в процессе согласования не раскрывается).
- **Aggressive Mode** (Активный режим) обеспечивает более высокую скорость по сравнению с **Main Mode** так как пропускает некоторые шаги в процессе аутентификации сторон (фаза 1). Однако по причине более высокой скорости, в данном режиме ограничены возможности согласования и не обеспечивается защита конфиденциальности сторон. Этот режим полезен в случае удаленного доступа, когда адрес инициирующей стороны неизвестен отвечающей стороне, и оба участника желают использовать аутентификацию с помощью предварительно согласованного ключа.

16.10.2 Группы ключей Диффи-Хеллмана (Diffie-Hellman, DH)

Метод Диффи-Хеллмана (DH) - это протокол шифрования с открытым ключом, позволяющий двум участникам получить разделяемый секретный ключ по незащищенному каналу связи. Метод Диффи-Хеллмана используется в соединении SA для обмена ключами IKE с целью определить сеансовые ключи. Поддерживаются группы ключей Диффи-Хеллмана длиной 768 бит (группа 1 - **DH1**) и 1024 бит (группа 2 – **DH2**). После завершения обмена по Диффи-Хеллману оба участника получают одинаковый секретный ключ, однако аутентификация сторон соединения SA для IKE не выполнена. Для аутентификации следует использовать предварительно согласованные ключи.

16.10.3 Идеальная прямая безопасность (PFS)

Включение функции PFS означает, что ключ предназначен для временного использования. Каждый раз при создании нового соединения SA для IPSec вычисляется новый ключ с помощью обмена по методу Диффи-Хеллмана. При включенной функции PFS, в случае, если один ключ становится известным третьей стороне, предыдущий и последующие ключи не могут быть раскрыты, так как последующие ключи не являются производными предыдущих. "Платой" за дополнительную безопасность является довольно долгий по времени обмен по методу Диффи-Хеллмана.
Эта функция может быть необязательна для данных, не требующих высокой степени защиты, поэтому в OMNI ADSL функция PFS по умолчанию отключена (**None**). Отключение функции PFS означает, что новые ключи аутентификации и шифрования будут вычисляться из одного и того же

исходного секретного ключа (что со временем может отразиться на безопасности связи), однако установка соединения SA при этом происходит быстрее (за счет того, что не выполняется обмен ключами по методу Диффи-Хеллмана).

16.11 Установка дополнительных настроек IKE

Щелкните по **Advanced** в экране **VPN IKE**. Им является экран **VPN IKE- Advanced**, показанный ниже.

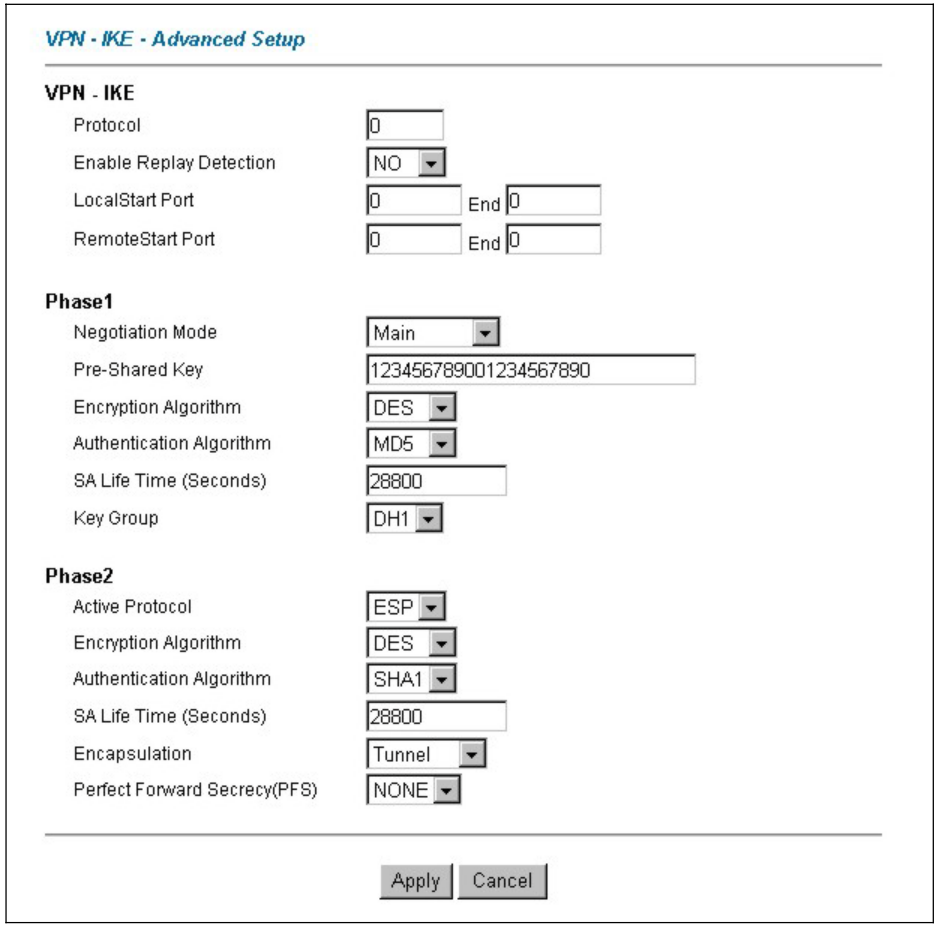


Рис. 16-5 Согласование обмена ключами VPN: дополнительная настройка

В следующей таблице приведены описания полей данного меню.

Табл. 16-8 Согласование обмена ключами VPN: дополнительная настройка

ПОЛЕ	ОПИСАНИЕ
VPN - IKE	
Protocol (Протокол)	Ввести "1" для ICMP, "6" для TCP, "17" для UDP, и т.д.. "0" - установлен по умолчанию и означает "любой протокол".
Enable Replay Protection (Включение защиты от атак при повторной передаче)	Поскольку создание VPN ведет к увеличению интенсивности обработки, система уязвима для атак "Отказ от обслуживания" (DoS). Получатель пакета, использующий протокол IPSec, может обнаружить, что такой пакет уже передавался, и отказаться от приема дублирующего пакета, обеспечивая тем самым защиту от атак, пользующихся механизмом повторной передачи. Выберите опцию **YES** из выпадающего меню для включения защиты от атак при повторной передаче или выберите **NO** для ее отключения.
Local Start Port (Местный начальный порт)	"0" устанавливается по умолчанию и означает любой порт. Введите значение номера порта в диапазоне от 0 до 65535. Наиболее типичными IP-портами являются следующие: 21 - FTP; 53 - DNS; 23 - Telnet; 80 - HTTP; 25 - SMTP; 110 - POP3.
End (Конечный)	Указать в данном поле номер порта, замыкающий диапазон портов. Это значение должно быть больше заданного в предыдущем поле. Если в поле **Local Start Port** останется значение 0, то в поле **End** также сохранится 0.
Remote Start Port (Удаленный начальный порт)	"0" устанавливается по умолчанию и означает любой порт. Введите значение номера порта в диапазоне от 0 до 65535. Наиболее типичными IP-портами являются следующие: 21 - FTP; 53 - DNS; 23 - Telnet; 80 - HTTP; 25 - SMTP; 110 - POP3.
End (Конечный)	Указать в данном поле номер порта, замыкающий диапазон портов. Это значение должно быть больше заданного в предыдущем поле. Если в поле **Remote Start Port** останется значение 0, то в поле **End** также сохранится 0.
Phase 1 (Фаза 1)	
Negotiation Mode (Режим согласования)	Выберите **Main** или **Aggressive** из раскрывающегося списка. Для нескольких соединений SA через безопасный шлюз должен быть установлен один и тот же режим согласования.

Табл. 16-8 Согласование обмена ключами VPN: дополнительная настройка

ПОЛЕ	ОПИСАНИЕ
Pre-Shared Key (Предварительно согласованный ключ)	Введите в этом поле тип Вашего предварительно согласованного ключа . Предварительно согласованный ключ идентифицирует участника в первой фазе согласования по обмену ключами. Ключ называется "предварительно согласованным", так как его необходимо сообщить партнеру до установления связи через безопасное соединение. Введите от 8 до 31 символа ASCII с учетом регистра или от 16 до 62 шестнадцатеричных символов ("0-9", "A-F"). В состав шестнадцатеричного ключа обязательно должны быть включены (на первых позициях) символы "0x" ("нуль" и "x"), которые не считаются относящимися к набору (от 16 до 32) символов ключа. Например, в коде "0x0123456789ABCDEF" символы “0x” указывают на то, что этот ключ является шестнадцатеричным и символы “0123456789ABCDEF” являются его собственным значением. Обоими конечными устройствами туннеля VPN должен использоваться один и тот же предварительно согласованный ключ. Если таковой не используется, вы получите пакет “PYLD_MALFORMED” (уведомление о наличии искажения).
Encryption Algorithm (Алгоритм шифрования)	Выберите из раскрывающегося списка опцию **DES** или **3DES**. При использовании стандарта DES как отправляющая, так и принимающая сторона должны знать один и тот же секретный ключ, с помощью которого осуществляется шифрование и дешифрование сообщений, а также генерация и проверка аутентификационного кода сообщений. В OMNI ADSL алгоритм шифрования DES использует 56-битовый ключ. Алгоритм Triple DES (**3DES**) - это разновидность DES, использующая 168-битовый ключ. Как следствие, алгоритм **3DES** надежнее протокола **DES**. Однако он требует большей производительности системы, что отражается в увеличении времени ожидания и в уменьшении ее пропускной способности.
Authentication ALgorithm (Алгоритм аутентификации)	Выберите из раскрывающегося списка опцию **SHA1** или **MD5** . Для аутентификации пакетных данных используются алгоритмы хэширования MD5 (Message Digest 5/Дайджест сообщения 5) и SHA1 (Secure Hash Algorithm - Алгоритм безопасного хэширования). Алгоритм SHA1 в целом более надежен, чем MD5, но несколько медленнее. Выберите MD5 для минимальной защиты и SHA-1 - для максимальной.

Табл. 16-8 Согласование обмена ключами VPN: дополнительная настройка

ПОЛЕ	ОПИСАНИЕ
SA Life Time (Seconds) (Продолжительность SA (в секундах))	В этом поле необходимо указать время, которое должно пройти до того, как автоматически начнется согласование нового SA-соединения для IKE. Ему может быть присвоено значение в пределах от 60 до 3000000 секунд (почти 35 дней). Малое время SA Life Time повышает безопасность, так как шлюзам VPN приходится чаще обновлять шифрующие и аутентифицирующие ключи. Однако при обновлении согласования по созданию туннеля VPN все пользователи, имеющие в этот момент доступ к удаленным ресурсам, будут временно отключены.
Key Group (Группа ключей)	Необходимо выбрать группу ключей для первой фазы обмена ключами. **DH1** (по умолчанию) означает группу Диффи-Хеллмана 1: 768-битное случайное число. **DH2** означает группу Диффи-Хеллмана 2: 1024-битное случайное число.
Phase 2 (Фаза 2)	
Active Protocol (Действующий протокол)	Воспользуйтесь раскрывающимся списком для выбора **ESP** или **AH**.
Encryption Algorithm (Алгоритм шифрования)	Выберите из раскрывающегося списка опцию **DES**, **3DES** или **NULL**. При использовании стандарта DES как отправляющая, так и принимающая сторона должны знать один и тот же секретный ключ, с помощью которого осуществляется шифрование и дешифрование сообщений, а также генерация и проверка аутентификационного кода сообщений. В OMNI ADSL алгоритм шифрования DES использует 56-битовый ключ. Алгоритм Triple DES (**3DES**) - это разновидность DES, использующая 168-битовый ключ. Как следствие, алгоритм 3DES надежнее протокола DES. Однако он требует большей производительности системы, что отражается в увеличении времени ожидания и в уменьшении пропускной способности. Для настройки туннеля без шифрования выбрать NULL. При выборе NULL шифровальные ключи не указываются.
Authentication ALgorithm (Алгоритм аутентификации)	Выберите из раскрывающегося списка опцию **SHA1** или **MD5**. Для аутентификации пакетных данных используются алгоритмы хэширования MD5 (Message Digest 5 - Дайджест сообщения 5) и SHA1 (Secure Hash Algorithm - Алгоритм безопасного хэширования). Алгоритм SHA1 в целом более надежен, чем MD5, но несколько медленнее. Выберите **MD5** для минимальной защиты и **SHA-1** - для максимальной.

Табл. 16-8 Согласование обмена ключами VPN: дополнительная настройка

ПОЛЕ	ОПИСАНИЕ
SA Life Time (Seconds) (Продолжительность SA (в секундах))	В этом поле необходимо указать время, которое должно пройти до того, как автоматически начнется согласование нового SA-соединения для IKE. Ему может быть присвоено значение в пределах от 60 до 3000000 секунд (почти 35 дней). Малое время SA Life Time повышает безопасность, так как шлюзам VPN приходится чаще обновлять шифрующие и аутентифицирующие ключи. Однако при обновлении согласования по созданию туннеля VPN все пользователи, имеющие в этот момент доступ к удаленным ресурсам, будут временно отключены.
Encapsulation (Инкапсуляция)	Выберите из раскрывающегося списка режим **Tunnel** или режим **Transport**.
Perfect Forward Secrecy (PFS)(Идеальная прямая безопасность)	Во второй фазе создания SA-соединения для IPSec функция Perfect Forward Secrecy (PFS) по умолчанию отключена (**None**). Это позволяет увеличить скорость создания IPSec, однако снижает безопасность. Выберите **DH1** или **DH2** из раскрывающегося списка для включения протокола PFS. **DH1** означает группу Диффи-Хеллмана 1: 768-битовое случайное число. **DH2** означает группу Диффи-Хеллмана 2: 1024-битное (1 Кб) случайное число (более безопасно, но работает медленнее).
Apply (Применить)	Щелкните по **Apply (Применить)**для сохранения изменений в настройке OMNI ADSL и возврата к экрану **VPN IKE**.
Cancel (Отмена)	Щелкните по **Cancel (Отмена)** для возврата к экрану **VPN IKE** без сохранения изменений настройки.

16.12 Ручная настройка ключей

Ручное управление ключами может быть полезно в случае, если возникают какие-либо проблемы при использовании управления **IKE**.

16.12.1 Индекс параметра безопасности (Security Parameter Index, SPI)

SPI используется для того, чтобы различать соединения SA с одним и тем же адресатом и использующие один и тот же протокол IPSec. Этот параметр допускает объединение нескольких соединений SA в одном шлюзе. Значение **SPI** (Security Parameter Index) вместе с IP-адресом назначения уникальным образом идентифицирует конкретное соединение в рамках соглашения по безопасности (Security Association, SA). Значение **SPI** передается от удаленного шлюза VPN

локальному шлюзу VPN. Затем, для создания туннеля локальный шлюз VPN использует значения параметров сети, шифрования и ключей, ассоциированные администратором с данным значением SPI.

Реализация ZyXEL на данный момент допускает идентичные значения исходящего и входящего SPI.

16.13 Ручная настройка ключей

Настройку **VPN Manual Key (Ручная настройка ключа VPN)**можно произвести при выборе опции **Manual** в поле **Key Management (Управление ключом)** на экране **VPN IKE**. Им является экран **VPN Manual Key,** показанный ниже.

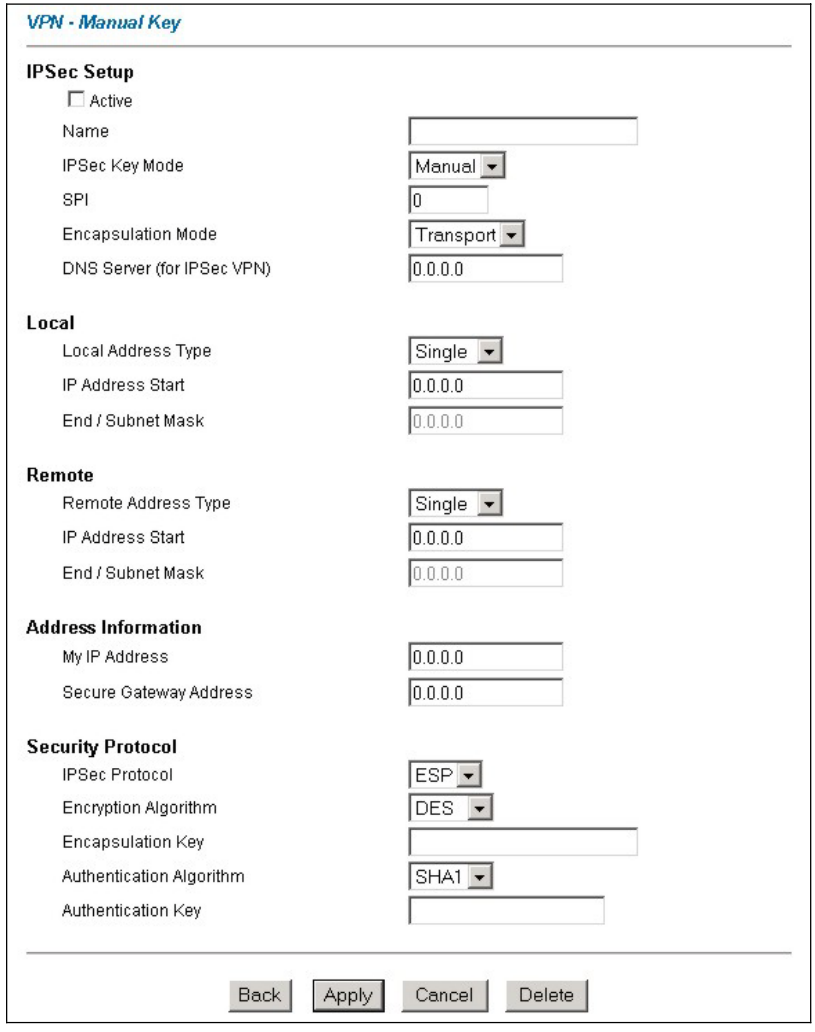


Рис. 16-6 Ручная настройка ключа VPN

В следующей таблице приведены описания полей данного меню.

Табл. 16-9 Ручная настройка ключа VPN

ПОЛЕ	ОПИСАНИЕ

Табл. 16-9 Ручная настройка ключа VPN

ПОЛЕ	ОПИСАНИЕ
IPSec Setup (Настройка IPSec)	
Active (Активно)	Поставьте метку в этом окне, чтобы активировать данную стратегию VPN.
Name (Имя)	Введите до 32 символов для идентификации стратегии VPN. Для этого можно воспользоваться любыми символами, включая пробелы, однако пробелы в конце строки OMNI ADSL удаляет.
IPSec Key Mode (Режим ключа IPSec)	Выберите из раскрывающегося списка **IKE** или **Manual**. **Ручное** управление ключами является полезной опцией для поиска и устранения неисправностей в случае, если возникают какие-либо проблемы при использовании **IKE**.
SPI (Индекс параметров безопасности)	Введите значение десятичного числа в диапазоне от 1 до 999999 для задания SPI (индекса параметров безопасности).
Encapsulation Mode (Режим инкапсуляции)	Выберите режим **Tunnel** или режим **Transport** из раскрывающегося списка.
DNS Server (for IPSec VPN) (Сервер DNS (для IPSec VPN))	Если имеется частный сервер DNS, обслуживающий VPN, введите здесь его IP-адрес. OMNI ADSL назначает этот дополнительный сервер DNS клиентам DHCP устройства OMNI ADSL, имеющим IP-адреса в диапазоне, установленном правилом IPSec, или локальные адреса. Сервер DNS помогает клиентам VPN отыскать другие компьютеры и серверы VPN по их (частным) доменным именам.
Local (Местный адрес)	Удаленные IP-адреса должны быть статическими и соответствовать заданным локальным IP-адресам удаленного маршрутизатора IPSec. Два активных соединения SA не могут иметь один и тот же локальный и удаленный IP-адрес (адреса) одновременно. Два активных соединения SA могут иметь один и тот же локальный или удаленный IP-адрес, но не оба сразу. Можно сконфигурировать несколько соединений SA между одинаковыми локальным и удаленным IP-адресами, но при этом активным в любой момент времени может быть только одно из них.

Табл. 16-9 Ручная настройка ключа VPN

ПОЛЕ	ОПИСАНИЕ
Local Address Type (Типы локальных адресов)	Следует воспользоваться выпадающим меню для выбора опций **Single (Единичный)**, **Range (Диапазон)** или **Subnet (Подсеть)**. Выберите **Single** для единичного IP-адреса. Для нескольких адресов подряд выберите **RANGE**. Чтобы указать в качестве IP-адресов в сети значение маски подсети, выбрать **SUBNET**.
IP Address Start (Начальный IP-адрес)	Если в поле **Local Address Type** указано **Single**, введите в данное поле IP-адрес (статический) локальной сети, расположенной за устройством OMNI ADSL . Если в поле **Local Address Type** указано **Range**, введите в данное поле первый из диапазона IP-адрес (статический) компьютеров локальной сети, расположенной за устройством OMNI ADSL. Если в поле **Local Address Type** указано **Subnet**, введите в данное поле IP-адрес (статический) локальной сети, расположенной за устройством OMNI ADSL .
End / Subnet Mask (Последний адрес/Маска подсети)	Если в поле **Local Address Type** указано **Single**, повторите здесь IP-адрес введенный в поле **IP Address Start**. Если в поле **Local Address Type** указано **Range**, введите в данное поле последний IP-адрес (статический) из диапазона адресов компьютеров в локальной сети, расположенной за устройством OMNI ADSL. Если в поле **Local Address Type** указано **SUBNET**, то в данном поле отображается маска подсети для локальной сети, расположенной за OMNI ADSL.
Remote (Удаленный адрес)	Удаленные IP-адреса должны быть статическими и соответствовать заданным локальным IP-адресам удаленного маршрутизатора IPSec. Содержимое этих полей не имеет значения, если в поле **Secure Gateway Address** введен код 0.0.0.0. В этом случае только удаленный маршрутизатор IPSec может инициализировать VPN. Два активных соединения SA не могут пользоваться одним и тем же локальным и удаленным IP-адресом (или адресами) одновременно. Два активных соединения SA могут пользоваться одним и тем же локальным или удаленным IP-адресом, но не обоими сразу. Можно сконфигурировать несколько соединений SA между одинаковыми локальными и удаленными IP-адресами, но при этом активным в любой момент времени может быть только одно из них.

Табл. 16-9 Ручная настройка ключа VPN

ПОЛЕ	ОПИСАНИЕ
Remote Address Type (Тип удаленного адреса)	Следует воспользоваться выпадающим меню для выбора опций **Single (Единичный)**, **Range (Диапазон)** или **Subnet (Подсеть)**. Для единичного IP-адреса выберите **SINGLE**. Для нескольких адресов подряд выберите **RANGE**. Чтобы указать в качестве IP-адресов в сети значение маски подсети, выберите **SUBNET**.
Start IP Address (Начальный IP-адрес)	Если в поле **Remote Address Type** указано Single, введите в данное поле IP-адрес (статический) в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Remote Address Type** указано **Range**, введите в данное поле первый из диапазона IP-адрес (статический) компьютеров в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Remote Address Type** указано **Subnet**, введите в данное поле IP-адрес (статический) в сети, расположенной за удаленным маршрутизатором IPSec.
End / Subnet Mask (Последний адрес/Маска подсети)	Если в поле **Remote Address Type** указано **Single**, повторите здесь IP-адрес, введенный в поле **IP Address Start** . Если в поле **Remote Address Type** указано **Range**, введите в данное поле значение последнего статического IP-адреса из диапазона адресов компьютеров в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Remote Address Type** указано **SUBNET**, введите в данное поле значение маски подсети в сети, расположенной за удаленным маршрутизатором IPSec.
My IP Address (Собственный IP-адрес)	Введите IP-адрес OMNI ADSL в глобальной сети. Если в этом поле оставить значение **0.0.0.0**, то при открытии туннеля VPN OMNI ADSL будет использовать свой текущий IP-адрес в глобальной сети (статический или динамический). При изменении IP-адреса туннель VPN должен быть перестроить.
Secure Gateway Address (Адрес безопасного шлюза)	В этом поле указывается IP-адрес в глобальной сети или URL (до 31 символа) маршрутизатора IPSec, с которым устанавливается VPN-соединение. Если удаленный маршрутизатор IPSec имеет динамический IP-адрес в глобальной сети, в данном поле необходимо выставить **0.0.0.0** (в поле **Key Mode** должно быть указано **IKE**).
Security Protocol (Протокол безопасности)	

Табл. 16-9 Ручная настройка ключа VPN

ПОЛЕ	ОПИСАНИЕ
Протокол IPSec	Если хотите воспользоваться протоколом ESP (Encapsulation Security Payload - инкапсулирующей защиты содержимого), выберите опцию **ESP**. Протокол ESP (RFC 2406) поддерживает шифрование, а также некоторые услуги протокола **AH**. Если на данном этапе выбрана опция **ESP**, то следует выбрать соответствующие опции в поле **Authentication Algorithm** (описанном ниже).
Encryption Algorithm (Алгоритм шифрования)	Выберите из раскрывающегося списка опцию **DES**, **3DES** или **NULL**. При использовании стандарта DES как отправляющая, так и принимающая сторона должны знать один и тот же секретный ключ, с помощью которого осуществляется шифрование и дешифрование сообщений, а также генерация и проверка аутентификационного кода сообщений. В OMNI ADSL алгоритмом шифрования DES используется 56-битовый ключ. Алгоритм Triple DES (**3DES**) - это разновидность DES, использующего 168-битовый ключ. Как следствие, алгоритм 3DES надежнее протокола DES. Однако он требует большей производительности системы, что отражается в увеличении времени ожидания и в уменьшении пропускной способности. Для настройки туннеля без шифрования выбрать **NULL**. При выборе **NULL** шифровальные ключи не указываются.
Encapsulation Key (only with ESP) (Ключ инкапсуляции (только с протоколом ESP)	При использовании алгоритма **DES**, введите уникальное значение ключа длиной 8 символов. При использовании алгоритма **3DES**, введите уникальное значение ключа длиной 24 символа. Допускается использование любых символов, включая пробелы, однако пробелы в конце строки удаляются.
Authentication ALgorithm (Алгоритм аутентификации)	Выберите из раскрывающегося списка опцию **SHA1** или **MD5**. Для аутентификации пакетных данных используются алгоритмы хэширования MD5 (Message Digest 5 - Дайджест сообщения 5) и SHA1 (Secure Hash Algorithm - Алгоритм безопасного хэширования). Алгоритм SHA1 в целом более надежен, чем MD5, но несколько медленнее. Выберите **MD5** для минимальной защиты и **SHA-1** - для максимальной.
Authentication Key (Ключ аутентификации)	Введите уникальное значение ключа аутентификации для использования протоколом IPSec, если он применяется. Введите значение из 16 символов, если для аутентификации применяется алгоритм MD5 или 20 символов - для алгоритма SHA-1. Допускается использование любых символов, включая пробелы, однако пробелы в конце строки удаляются.
Back (Назад)	Щелкните по **Back** для возврата к предыдущему экрану.

Табл. 16-9 Ручная настройка ключа VPN

ПОЛЕ	ОПИСАНИЕ
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по **Cancel (Отмена)** для повторной настройки данного экрана.
Удалить	Щелкните по кнопке **Delete (Удалить)** для удаления текущего правила.

16.14 Отображение монитора SA

Щелкните по **VPN** и **Monitor** для вызова данного экрана **SA Monitor**. Данным экраном следует пользоваться для отображения и управления активными соединениями VPN.
Security Association (SA - Соглашение по безопасности) - это набор настроек по защите для конкретного туннеля VPN. На этом экране показываются активные соединения VPN. Для отображения активных соединений VPN пользуйтесь опцией **Refresh** . Данная экранная форма предназначена только для чтения. Следующая таблица описывает поля данного меню.

При наличии исходящего трафика и отсутствии входящего, SA-соединение автоматически прекращается через две минуты. При отсутствии входящего или исходящего трафика туннель находится в состоянии "ожидания" и не отключается до истечения установленного периода существования соединения SA. См. *раздел 16.6* о работе функции поддержания соединения для того чтобы OMNI ADSL выполнил повторное согласование соединения SA для IPSec по истечении установленного периода существования соединения SA, даже при отсутствии трафика.

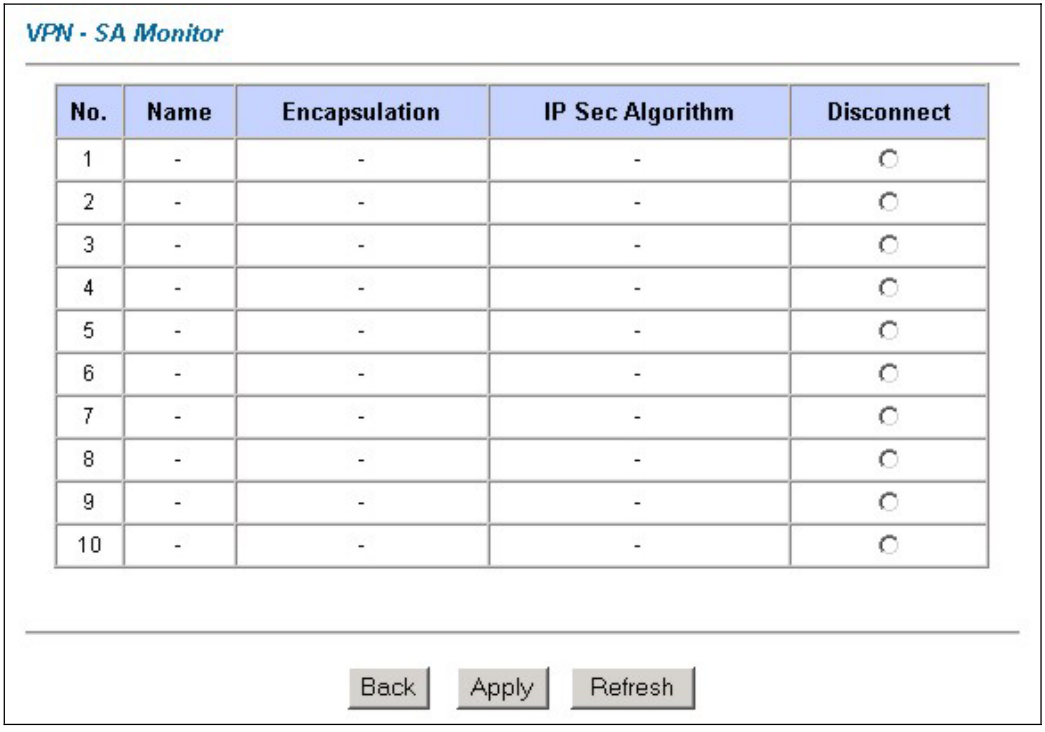


Рис. 16-7 Монитор SA

В следующей таблице приведены описания полей данного меню.

Табл. 16-10 Монитор SA

ПОЛЕ	ОПИСАНИЕ
No	Номер безопасного соединения.
Name (Имя)	В этом поле указывается уникальное идентификационное имя данной стратегии VPN.
Encapsulation (Инкапсуляция)	В этом поле отображается признак режима: Tunnel или Transport.
IPSec Algorithm (Алгоритм IPSec)	В этом поле отображаются признаки протоколов безопасности, использующихся для соединения SA. Применение обоих протоколов (AH и ESP) связано с повышением требований к производительности OMNI ADSL и понижает оперативность (увеличивает время ожидания).

Табл. 16-10 Монитор SA

ПОЛЕ	ОПИСАНИЕ
Disconnect (Отключение)	Выберите опцию **Disconnect (Отключение)** рядом с безопасным SA-соединением и щелкните по **Apply (Применить)**для его отключения.
Back (Назад)	Щелкните по **Back (Назад)**для возврата к предыдущему экрану.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Refresh (Обновить)	Щелкните по **Refresh (Обновить)** для отображения текущего активного соединения (соединений) VPN.

16.15 Конфигурирование общих настроек

Для изменения общих настроек маршрутизатора OMNI ADSL щелкните по **VPN**, а затем по **Global Setting**. Появится экранное меню следующего вида.

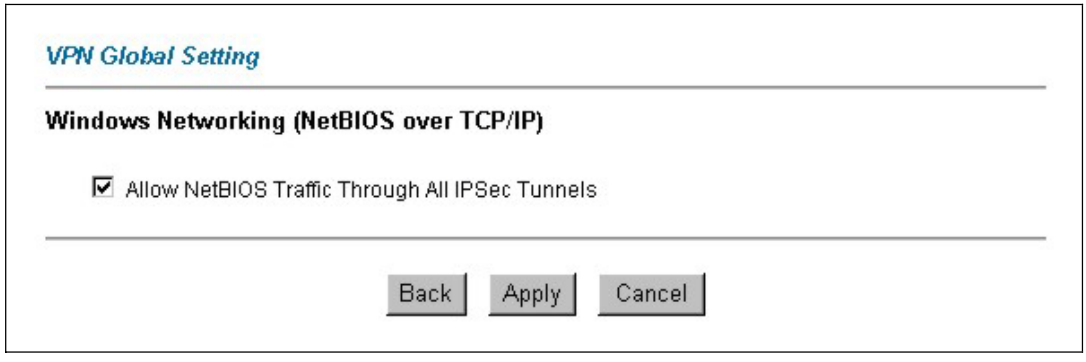


Рис. 16-8 Общие настройки

В следующей таблице приведены описания полей данного меню.

Табл. 16-11 Общие настройки

ПОЛЕ	ОПИСАНИЕ
Windows Networking (NetBIOS over TCP/IP) (Сетевое подключение в ОС Windows (NetBIOS через TCP/IP))	NetBIOS (сетевая базовая система ввода/вывода) использует широковещательные пакеты TCP или UDP, позволяющие одному компьютеру отыскать другие. Иногда необходимо разрешить прохождение пакетов NetBIOS через туннели VPN для того, чтобы разрешить локальным компьютерам отыскать компьютеры в удаленной сети и наоборот.

Табл. 16-11 Общие настройки

ПОЛЕ	ОПИСАНИЕ
Allow NetBIOS Traffic Through All IP/Sec Tunnels (Разрешение трафика NetBIOS через все туннели IP/Sec)	Поставьте метку в этом окошке для отправки пакетов NetBIOS через соединение VPN.
Back (Назад)	Щелкните по **Back (Назад)**для возврата к предыдущему экрану.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по **Cancel (Отмена)** для повторной настройки данного экрана.

16.16 Настройка журналов IPSec

Для отображения журналов IPSec на этом экране щелкните по **Advanced Setup**, **VPN**, а затем - **Logs** для вызова показанного ниже экрана.

Рис. 16-9 Журналы VPN

В следующей таблице приведены описания полей данного меню.

Табл. 16-12 Журналы VPN

ПОЛЕ	ОПИСАНИЕ
Back (Назад)	Щелкните по **Back (Назад)**для возврата к предыдущему экрану.
Previous Page (Предыдущая страница)	Щелкните по **Previous Page (Предыдущая страница)**, чтобы увидеть предыдущие записи.
Refresh (Обновить)	Щелкните по **Refresh (Обновить)** для обновления экрана отчетов. Отчет также обновляется автоматически после закрытия и повторного открытия экранного меню.
Clear (Очистить)	Щелкните по **Clear (Clear)** для удаления всех записей.
Next Page (Следующая страница)	Щелкните по **Next Page (Следующая страница)**, чтобы увидеть последующие записи.

Этот экран полезен для поиска и устранения неисправностей. Журнал отображает порядковый номер, дату и время создания записи и ее содержание.

Два восклицательных знака (!!) означают сообщение об ошибке или предупреждение.

В следующей таблице приведены образцы сообщений журнала, генерируемых во время обмена ключами (IKE).

Табл. 16-13 Образцы сообщений на этапе обмена ключами

СООБЩЕНИЕ	ОПИСАНИЕ
`Cannot find outbound SA for rule <#d>`	Пакет удовлетворяет правилу номер (#d), однако фаза 1 или фаза 2 согласования для исходящего (от инициатора VPN) трафика не завершена.
`Send Main Mode request to <IP>` `Send Aggressive Mode request to <IP>`	OMNI ADSL начал процесс согласования с клиентским устройством.
`Recv Main Mode request from <IP>` `Recv Aggressive Mode request from <IP>`	OMNI ADSL получил запрос на начало согласования по обмену ключами от клиентского устройства.
`Send:<Symbol><Symbol>` `Recv:<Symbol><Symbol>`	IKE использует протокол ISAKMP (см. RFC2408 – ISAKMP) для передачи данных. Каждый пакет ISAKMP содержит данные различных типов, информация о которых заносится в журнал - см. *Табл. 16-15*.

Табл. 16-13 Образцы сообщений на этапе обмена ключами

СООБЩЕНИЕ	ОПИСАНИЕ
`Phase 1 IKE SA process done`	Фаза согласования 1 завершена.
`Start Phase 2: Quick Mode`	Фаза согласования 2 начинается в режиме Quick Mode (быстрый режим).
`!! IKE Negotiation is in process`	OMNI ADSL начал согласование по установлению соединения с клиентским устройством, но обмен ключами (IKE) не завершен.
`!! Duplicate requests with the same cookie`	OMNI ADSL получил некоторое количество запросов от клиентского устройства, но все еще обрабатывает первый пакет IKE от него.
`!! No proposal chosen`	Параметры, установленные для фазы согласования 1 или 2, не совпадают. Рекомендуется проверить соответствующие настройки и протоколы. Например, возможно одна сторона использует стандарт шифрования 3DES, а другая DES, в результате соединение установить невозможно.
`!! Verifying Local ID failed` `!! Verifying Remote ID failed`	Во время согласования по IKE в фазе 2 обе стороны обмениваются данными стратегии, включая диапазоны локальных и удаленных IP-адресов. Если они различаются, соединение не может быть установлено.
`!! Local / remote IPs of incoming request conflict with rule <#d>`	Если адрес безопасного шлюза “0.0.0.0”, OMNI ADSL использует в качестве удаленного адреса локальный адрес клиентского устройства. Если данный IP (диапазон) не соответствует ранее установленному правилу, соединение не разрешается.
`!! Invalid IP <IP start>/<IP end>`	Неправильный диапазон локальных IP-адресов абонента.
`!! Remote IP <IP start> / <IP end> conflicts`	Если адрес безопасного шлюза “0.0.0.0”, OMNI ADSL использует в качестве удаленного адреса локальный адрес клиентского устройства. Если диапазон локальных адресов клиентского устройства конфликтует с другими соединениями, OMNI ADSL запрещает запросы VPN-соединения от него.

Табл. 16-13 Образцы сообщений на этапе обмена ключами

СООБЩЕНИЕ	ОПИСАНИЕ
`!! Active connection allowed exceeded`	OMNI ADSL ограничивает количество одновременных согласований соединений SA в Фазе 2. При превышении данного лимита процесс обмена ключами прерывается.
`!! IKE Packet Retransmit`	OMNI ADSL не получил ответа от клиентского устройства и повторно отсылает последний отправленный пакет.
`!! Failed to send IKE Packet`	OMNI ADSL не может посылать пакеты IKE из-за ошибки в сети.
`!! Too many errors! Deleting SA`	При возникновении слишком большого количества ошибок OMNI ADSL удаляет соединение SA .

В следующей таблице приведены образцы сообщений журнала, генерируемых во время передачи пакетов.

Табл. 16-14 Образцы сообщений журнала регистраций IPSec на этапе передачи пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
`!! WAN IP changed to <IP>`	Если изменяется IP-адрес OMNI ADSL в глобальной сети, адреса, указанные в поле “My IP Addr”, устанавливаются на “0.0.0.0”.. Если оставить в этом поле 0.0.0.0, то для установки туннеля VPN OMNI ADSL будет использовать текущий IP-адрес OMNI ADSL в глобальной сети (статический или динамический).
`!! Cannot find Phase 2 SA`	OMNI ADSL не может обнаружить соединение SA в Фазе 2, соответствующее параметру SPI прибывшего пакета (от клиентского устройства); пакет сбрасывается.
`!! Discard REPLAY packet`	OMNI ADSL сбрасывает полученный пакет с неправильным порядковым номером.
`!! Inbound packet authentication failed`	Настройки аутентификации некорректны. Необходимо их проверить.
`!! Inbound packet decryption failed`	Настройки дешифрования некорректны. Необходимо их проверить.

Табл. 16-14 Образцы сообщений журнала регистраций IPSec на этапе передачи пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
`Rule <#d> idle time out, disconnect`	Если в рамках соединения SA за время, установленное с помощью интерпретируемой команды, не были переданы никакие пакеты, OMNI ADSL сбрасывает данное соединение.

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. 16-15 Типы данных сообщений протокола ISAKMP согласно RFC-2408

ОБОЗНАЧЕНИЕ В ЖУРНАЛЕ	ТИП ДАННЫХ
SA	Безопасное соединение
PROP	Предложение
TRANS	Преобразование
KE	Обмен ключами
ID	Идентификация
CER	Сертификат
CER_REQ	Запрос сертификата
HASH	Хэш
SIG	Подпись
NONCE	Случайное число
NOTFY	Уведомление
DEL	Удалить
VID	Идентификационный номер продавца

16.17 Примеры удаленных компьютеров VPN/IPSec

Следующие примеры показывают, как группа удаленных компьютеров может установить соединения VPN с одним устройством OMNI ADSL в головном офисе через удаленный маршрутизатор IPSec, использующий динамический IP-адрес в глобальной сети.

16.17.1 Пример: удаленные компьютеры, пользующиеся одним правилом VPN

Группа удаленных пользователей может пользоваться одним правилом VPN для одновременного доступа к устройству OMNI ADSL, расположенному в головном офисе. Они должны иметь одинаковые параметры IPSec (включая предварительно согласованный ключ), но их локальные IP-адреса (или их диапазоны) не должны совпадать. В качестве примера см. следующую табл. и рис.

Групповое использование одного предварительно согласованного ключа делает сеть уязвимой. Если ключ окажется скомпрометированным, то все соединения VPN, пользующиеся этим правилом, окажутся в опасности. Рекомендованной альтернативой этому является использование различных правил VPN каждым удаленным пользователем с идентификацией их по уникальному идентификатору (см. *раздел 16.17.2* в качестве примера)

Табл. 16-16 Пример конфигурации для установления связи дистанционного пользователя с головным офисом

	УДАЛЕННЫЙ КОМПЬЮТЕР	ГОЛОВНОЙ ОФИС
My IP address:	0.0.0.0 (динамический IP-адрес, назначенный Интернет-провайдером)	Общеизвестный статический IP-адрес
Secure Gateway IP Address:	Общеизвестный статический IP-адрес или имя домена.	0.0.0.0 При таком IP-адресе инициировать туннель IPSec может только удаленный пользователь.

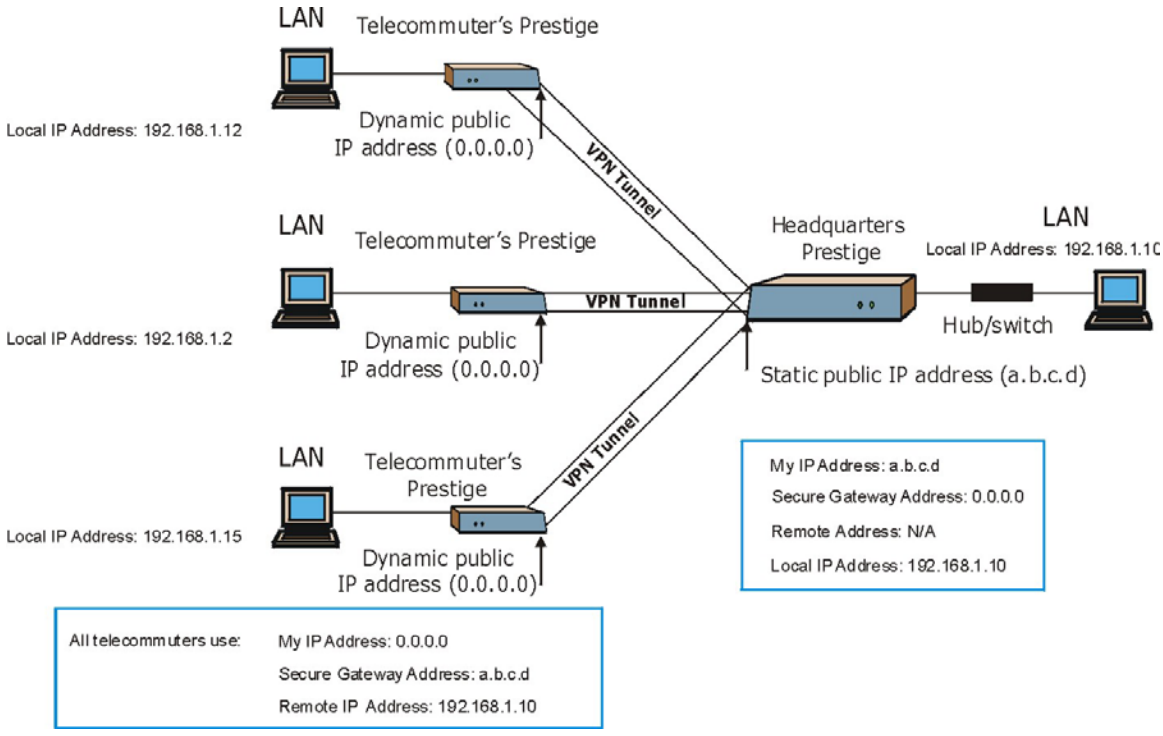


Рис. 16-10 Удаленные компьютеры, пользующиеся одним правилом VPN

16.17.2 Удаленные компьютеры, пользующиеся уникальными правилами VPN

В режиме активного согласования (см. *раздел 16.10.1*) устройство OMNI ADSL может использовать признаки типов адресов и содержания для установления различий между правилами VPN. Удаленные компьютеры могут пользоваться каждый отдельным правилом VPN для одновременного доступа к устройству OMNI ADSL, расположенному в головном офисе. Они могут пользоваться различными параметрами IPSec (включая предварительно согласованный ключ), а их локальные IP-адреса (или диапазоны адресов) могут совпадать.

См. в качестве примера следующую диаграмму, на которой представлена ситуация, когда три удаленных компьютера пользуются различными правилами VPN для инициализации соединений VPN с устройством OMNI ADSL, расположенным в головном офисе. Устройство OMNI ADSL в головном офисе идентифицирует каждого из них по значению адреса шлюза безопасности (динамическое доменное имя) и пользуется соответствующим правилом VPN для установления соединения VPN.

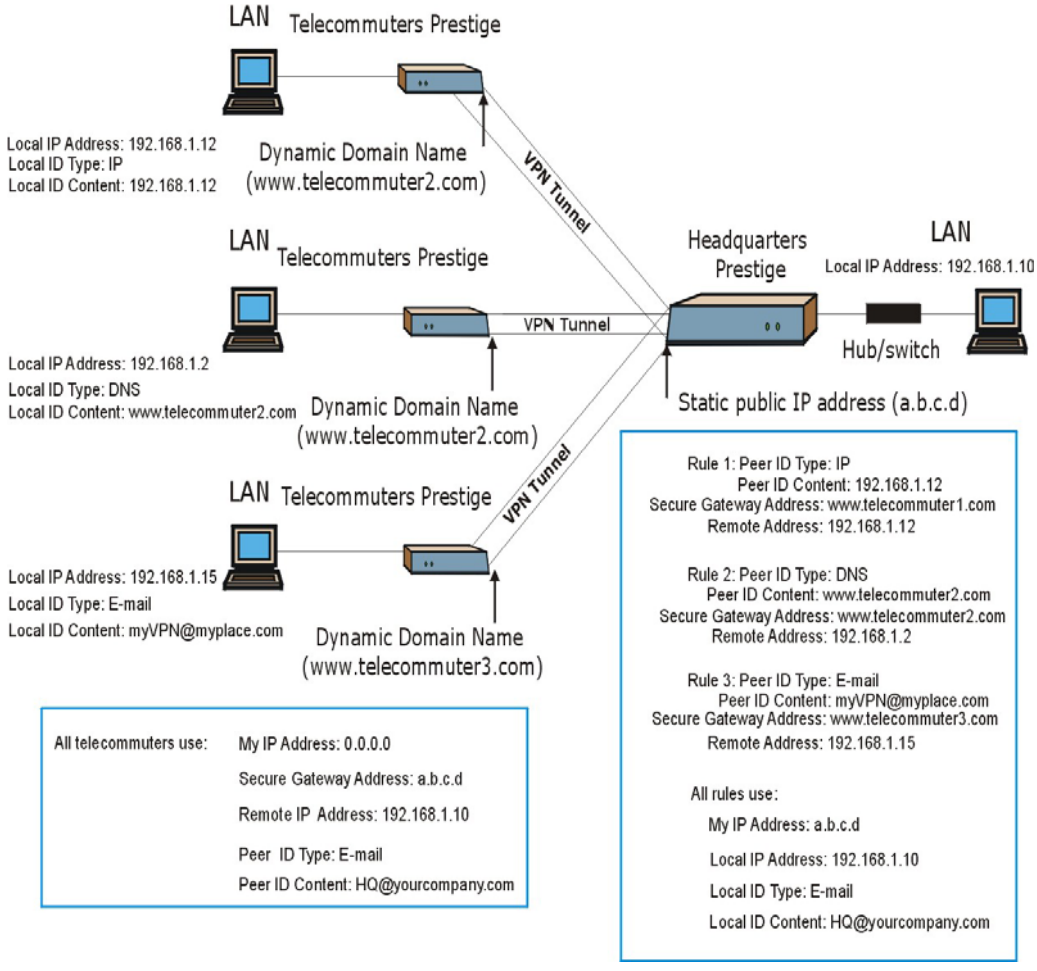


Рис. 16-11 Пример работы удаленных компьютеров, пользующихся уникальными правилами VPN

16.18 Виртуальная частная сеть и дистанционное управление

Если туннель VPN используется портом услуг дистанционного управления (Telnet, FTP, WWW) и заканчивается портом LAN или WAN устройства OMNI ADSL, для доступа к возможностям удаленного управления следует выполнить его настройку.

Если туннель VPN заканчивается IP-адресом LAN устройства OMNI ADSL, выполните настройку дистанционного управления для доступа сервера к **LAN** , или **WAN,** или **LAN & WAN** , или **LAN & WAN**).
Если туннель VPN заканчивается IP-адресом WAN устройства OMNI ADSL, выполните настройку дистанционного управления для доступа сервера к **WAN** (или **LAN & WAN,** или **LAN & WAN**).

Part VI:

Дистанционное управление, универсальный интерфейс Plug&Play и журналы

В этой части содержится информация о том, как осуществить настройку дистанционного управления OMNI ADSL, настройку универсального интерфейса Plug and Play (UPnP) и журналов.

Chapter 17
Настройка дистанционного управления

В данной главе содержится информация о настройке дистанционного управления. Функция дистанционного управления доступна не для всех моделей

17.1 Описание функции дистанционного управления

Функция дистанционного управления позволяет определить порядок доступа к ресурсам сети: с какого компьютера, к каким услугам/протоколам и через какой интерфейс (если их несколько) устройства OMNI ADSL.

Возможны следующие режимы дистанционного управления OMNI ADSL:

- Интернет (только глобальная сеть)
- Только локальная сеть
- Все (локальная и глобальная сети)
- Нет (Отключить)

Для отключения дистанционного управления сервисом, выберите **Disable (Отключить)** в соответствующем поле **Service Access (Доступ к сервису)**.

17.1.1 Ограничения дистанционного управления

Дистанционное управление через локальную или глобальную сеть невозможно в следующих случаях:

1. При активации фильтра в меню 3.1 SMT (LAN) или в меню 11.5 (WAN), применяющегося для блокировки доступа к услугам Telnet, FTP или Web.
2. При отключении доступа к данному виду сервиса с помощью одного из экранов дистанционного управления.
3. Если IP-адрес в поле **Secured Client IP** не совпадает с IP-адресом клиента. В этом случае OMNI ADSL немедленно прекращает сеанс связи Telnet.
4. Во время сеанса связи с системным терминалом.
5. При совпадении сеансов дистанционного управления одного типа (Web, FTP или Telnet). Одновременно нельзя проводить более одного сеанса дистанционного управления одного типа.

6. При совпадении сеанса дистанционного управления web с сеансом Telnet. При установлении web-соединения сеанс связи Telnet сбрасывается; Telnet-соединение при наличии Web-соединения не устанавливается.

17.1.2 Дистанционное управление и трансляция сетевых адресов

Когда функция NAT включена:

- при управлении из глобальной сети следует использовать IP-адрес устройства OMNI ADSL в глобальной сети;
- при управлении из локальной сети следует использовать IP-адрес OMNI ADSL в локальной сети.

17.1.3 Время ожидания системы

Время ожидания устанавливается продолжительностью пять минут (триста секунд) как для консольного порта, так и для соединений telnet/web/FTP. Если в течение времени ожидания не будут выполняться какие-либо действия, за исключением непрерывного обновления статуса в меню 24.1 или изменения `sys stdio` в командной строке, OMNI ADSL осуществит автоматическую выгрузку пользователя,.

17.2 Telnet

Для удаленного доступа к услугам Telnet следует выполнить настройку устройства OMNI ADSL как показано ниже.

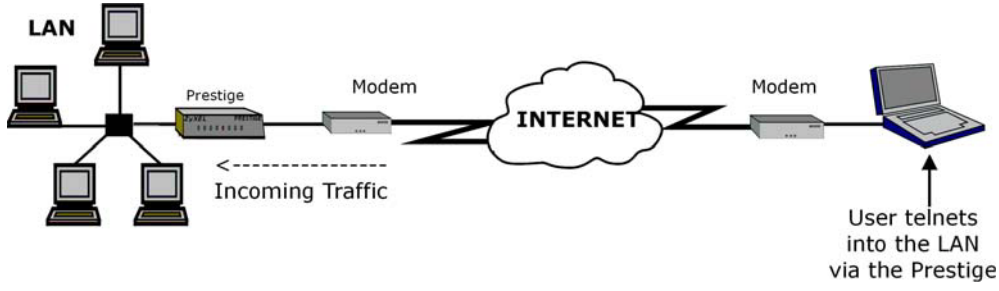


Рис. 17-1 Настройка доступа к услугам Telnet в сети TCP/IP

17.3 FTP

Загрузку и выгрузку микропрограммного обеспечения OMNI ADSL и файлов конфигурации можно осуществлять с использованием протокола FTP. Для использования такой возможности компьютер должен иметь доступ к какому-либо FTP-клиенту.

17.4 Web

Для настройки и управления файлами можно пользоваться встроенным Web-конфигуратором OMNI ADSL . Для получения дополнительной информации обращайтесь к справочной системе online .

17.5 Настройка дистанционного управления

Щелкните по опции **Remote Management (Дистанционное управление)** для вызова следующего экрана.

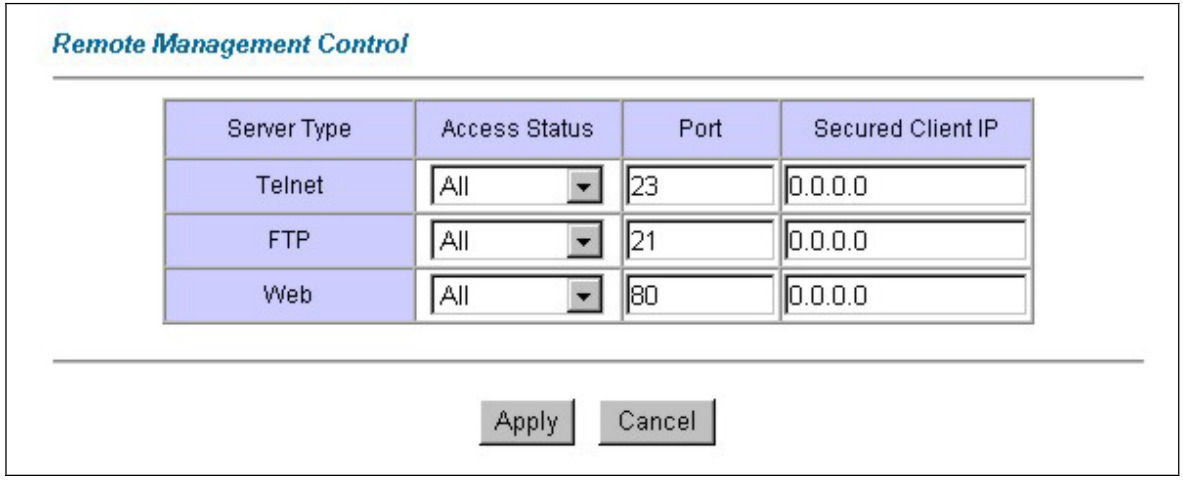


Рис. 17-2 Дистанционное управление

В следующей таблице приведены описания полей данного меню.

Табл. 17-1 Дистанционное управление

ПОЛЕ	ОПИСАНИЕ

Табл. 17-1 Дистанционное управление

ПОЛЕ	ОПИСАНИЕ
Server Type (Тип сервера)	Каждая из этих надписей указывает вид сервиса, позволяющий дистанционно управлять устройством OMNI ADSL.
Access Status (Статус доступа)	Выберите интерфейс доступа. Можно выбрать следующие опции: **All (Все)**, **LAN Only (Только LAN)**, **WAN Only (Только WAN)** и **Disable (Отключено)**.
Port (Порт)	В данном поле отображается номер порта для доступа к сервису дистанционного управления. Можно изменить номер порта для доступа к этому сервису, но необходимо пользоваться тем же самым номером порта для доступа к данному виду сервиса дистанционного управления.
Secured Client IP (Защищенный клиентский IP-адрес)	Заданное по умолчанию значение 0.0.0.0 позволяет любому клиенту пользоваться этим сервисом для дистанционного управления устройством OMNI ADSL. Введите какой-либо IP-адрес для разрешения доступа только клиенту, имеющему IP-адрес, совпадающий с указанным.
Apply (Применить)	Щелкните по**Apply (Применить)** для сохранения настроек.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для повторной настройки данного экрана.

Chapter 18
Универсальный интерфейс Plug&Play (UPnP)

В этой главе приводится описание функций интерфейса UPnP в Web-конфигураторе.

18.1 Описание универсального интерфейса Plug&Play

Универсальный интерфейс Plug&Play (UPnP) является распространенным стандартом открытых сетей, в которых применяется протокол TCP/IP простой одноранговой сети (без иерархии и выделенных серверов) для связи между устройствами. Устройство с функцией UPnP может динамически подключиться к сети, получить IP-адрес, открыть доступ к своим возможностям и получить необходимые сведения о других устройствах сети. В свою очередь, устройство может автоматически и без осложнений быть исключено из состава сети, когда оно перестает использоваться.

18.1.1 Как узнать: используется ли функция UPnP?

Аппаратура с функциями UPnP идентифицируется с помощью иконки в папке Network Connections (Сетевые соединения) операционной системы Windows XP. Каждое устройство с функциями UPnP, установленное в Вашей сети, будет отображаться в виде отдельной иконки. Выбрав иконку соответствующего устройства, Вы получите доступ к его ресурсам и необходимой информации.

18.1.2 Отслеживание устройства NAT

Отслеживание устройства NAT с функциями UPnP позволяет автоматизировать процесс получения приложением разрешения на работу через NAT. Сетевые устройства UPnP могут автоматически осуществлять настройку адресования сети, объявлять о своем присутствии в сети другим устройствам UPnP и делать возможным обмен простыми ресурсами и описаниями сервиса. Отслеживание устройств NAT позволяет выполнить следующие функции:

- Динамическое распределение портов
- Определение общедоступных IP-адресов
- Назначение разрешенного числа распределений

Программа Windows Messenger является примером приложения, поддерживающего функцию отслеживания устройств NAT и UPnP.

Для получения дополнительной информации о NAT см. главу *Трансляция сетевых адресов (NAT)* .

18.1.3 Предупреждения относительно UPnP

Автоматизация функций отслеживания NAT приложений, устанавливающих свои собственные виды сервиса, может затронуть вопросы безопасности сети. Конфигурация сети и данные о ней могут быть также получены и модифицированы пользователями из других сетей.

Все устройства с функциями UPnP могут свободно связываться друг с другом без дополнительной настройки. Отключите функцию UPnP, если в этом нет необходимости.

18.2 Универсальный интерфейс Plug&Play и ZyXEL

Компания ZyXEL получила сертификат UPnP, выданный Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). Реализация интерфейса UPnP компании ZyXEL поддерживает шлюзовое устройство IGD 1.0 (Internet Gateway Device). На момент написания руководства реализация интерфейса UPnP компании ZyXEL поддерживает также Windows Messenger 4.6 и 4.7, в то время как испытания работоспособности интерфейса с Windows Messenger 5.0 и Xbox - продолжаются.

Объявлялось, что устройства UPnP могут использоваться только в локальных сетях.

См. следующие разделы для ознакомления с примерами установки устройств UPnP в среде Windows XP и Windows Me, а также с примерами их использования в Windows.

18.2.1 Настройка устройств UPnP

Выберите **Site Map** в главном меню и щелкните по **UPnP** под **Advanced Setup** для вызова представленного ниже экрана.

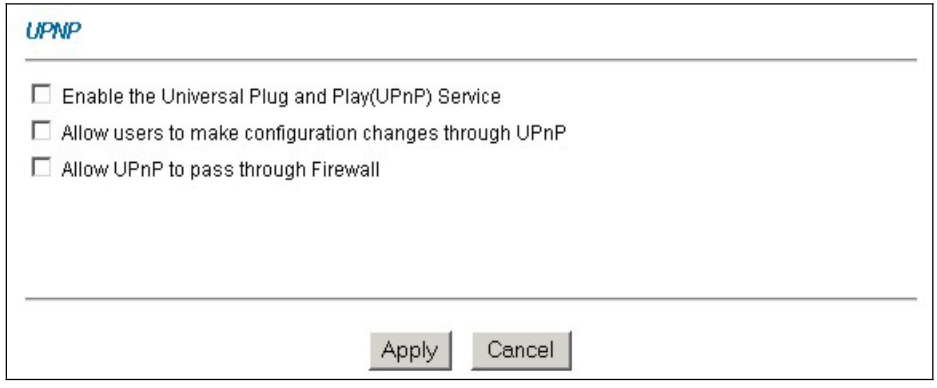


Рис. 18-1 Настройка UPnP

В следующей таблице приведены описания полей данного меню.

Рис. 18-1 Настройка UPnP

ПОЛЕ	ОПИСАНИЕ
Enable the Universal Plug and Play (UPnP) Service (Отключение функции Plug&Play (UPnP))	Поставьте флажок в этом окне для включения функции UPnP. Убедитесь в том, что никто не может воспользоваться приложением UPnP для открытия окна регистрации Web-конфигуратора без ввода IP-адреса устройства OMNI ADSL (хотя по-прежнему можно пользоваться паролем для доступа к Web-конфигуратору).
Allow users to make configuration changes through UPnP (Позволяет пользователям изменить конфигурацию с помощью интерфейса UPnP)	Поставьте флажок в этом окне для разрешения UPnP-приложениям автоматически осуществлять конфигурацию устройства OMNI ADSL, так чтобы они могли обмениваться данными через устройство OMNI ADSL, например, пользуясь функцией отслеживания NAT, UPnP-приложения автоматически резервируют порт переадресации NAT для того чтобы связаться с другим подключенным устройством UPnP, что иллюстрирует необходимость ручной настройки порта переадресации для подключенного UPnP-приложения.
Allow UPnP to pass through Firewall (Разрешает устройству UPnP доступ через межсетевой экран)	Это поле имеется не во всех моделях. Поставьте метку в этом окошке для разрешения прохождения трафика от подключенных UPnP-приложений через межсетевой фильтр. Оставьте это окошко пустым для блокировки межсетевым экраном всех пакетов UPnP-приложений (например, пакетов MSN).
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения настроек устройства OMNI ADSL.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возврата к ранее сохраненным настройкам.

18.3 Пример установки устройства UPnP в Windows

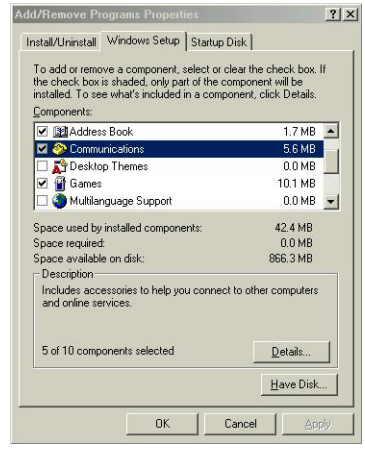
В этом разделе рассказывается, как выполнить установку устройства UPnP в Windows Me и Windows XP.

18.3.1 Установка UPnP в Windows Me

Для установки устройства UPnP в Windows Me выполните следующие действия.

Step 1. Щелкните **Start (Пуск)** и **Control Panel (Панель управления)**. Дважды щелкните по **Add/Remove Programs (Добавить/Удалить программы)**.

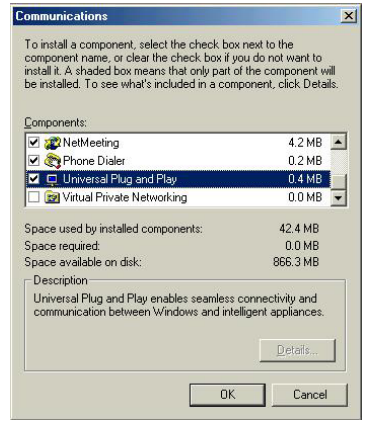
Step 2. Щелкните по закладке **Windows Setup (Настройка Windows)** и отметьте флажком опцию **Communication (Связь)** в окошке **Components (Компоненты)**. Щелкните по **Details**.



Step 3. В окне **Communications (Средства связи)** отметьте флажком **Universal Plug and Play** в окошке **Components**.

Step 4. Щелкните **OK** для возврата к окну **Add/Remove Programs Properties** и щелкните по **Next (Далее)**.

Step 5. После появления соответствующего сообщения перезапустите компьютер.



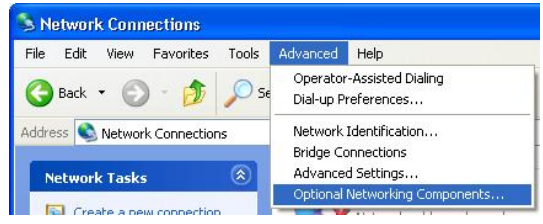
18.3.2 Пример установки устройства UPnP в Windows XP

Для установки устройства UPnP в Windows XP выполните следующие действия.

Step 1. Щелкните **Start (Пуск)** и **Control Panel (Панель управления)**.

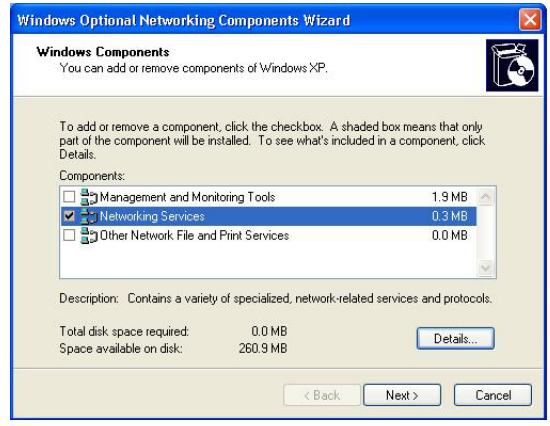
Step 2. Дважды щелкните по **Network Connections (Сетевые соединения)**.

Step 3. В окне **Network Connections (Сетевые соединения)** щелкните по **Advanced (Дополнительные настройки)** в главном меню и выберите **Optional**



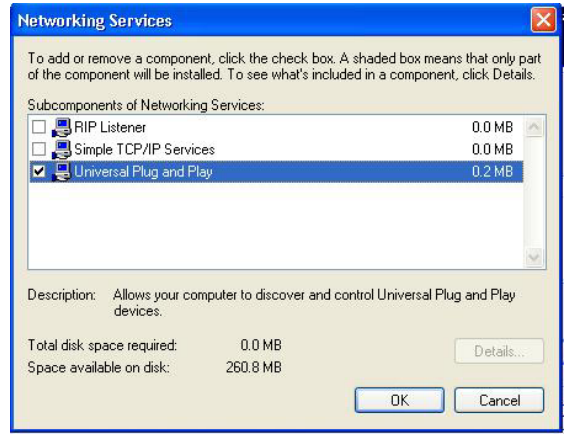
Networking Components (Дополнительные сетевые компоненты)….
В окне появится экран **Windows Optional Networking Components Wizard (Мастер-программы установки дополнительных сетевых компонентов Windows)**.

Step 4. Пометьте флажком **Networking Service (Сетевой сервис)** в окне **Components (Компоненты)** и щелкните по **Details**.



Step 5. В окне **Networking Services (Сетевой сервис)** отметьте флажком **Universal Plug and Play (Универсальный интерфейс Plug&Play)**.

Step 6. Щелкните **OK** для возврата в окно мастер-программы**Windows Optional Networking Component Wizard** и щелкните по **Next**.



18.4 Пример использования устройства UPnP в среде Windows XP

В этом разделе описывается, как можно пользоваться функцией UPnP в среде Windows XP. Для этого у Вас уже должна быть выполнена установка UPnP в Windows XP, а функция UPnP - активирована в устройстве OMNI ADSL.

Убедитесь в том, что компьютер подключен к порту ЛВС устройства OMNI ADSL. Включите компьютер и устройство OMNI ADSL.

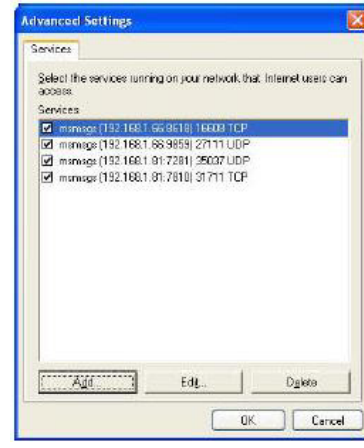
18.4.1 Автоматическое обнаружение подключенного сетевого устройства UPnP

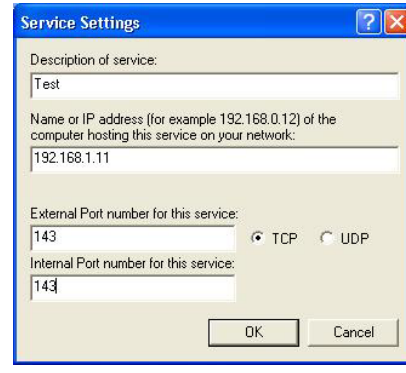
Step 1. Щелкните **Start (Пуск)** и **Control Panel (Панель управления)**. Дважды щелкните по **Network Connections (Сетевые соединения)**. Под надписью Internet Gateway (Шлюз в Интернет) отображается следующая иконка.

Step 2. Щелкните правой кнопкой мыши по иконке и выберите **Properties (Свойства)**.

Step 3. В окне **Internet Connection Properties (Свойства соединения Интернет)** щелкните по **Settings (Настройки)** для того чтобы увидеть результаты автоматически выполненного распределения портов.

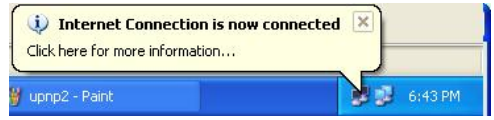
Step 4. Можно отредактировать или удалить эти назначения, или щелкните по **Add (Добавить)** для распределения портов вручную.



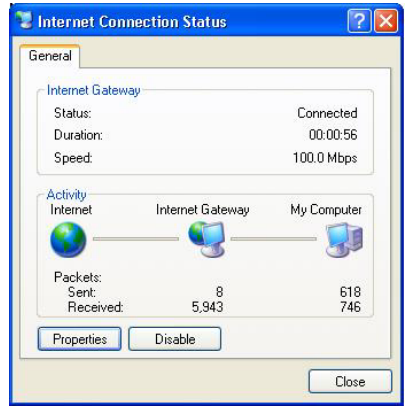


При отключении устройства UPnP от Вашего компьютера все распределения портов будут автоматически удалены.

Step 5. Выберите опцию **Show icon in notification area when connected (Отобразить иконку в строке состояния)** и щелкните **OK**. В системной области отобразится следующая иконка.



Step 6. Дважды щелкните по иконке для отображения текущего состояния соединения с сетью Интернет.



18.4.2 Простой доступ к Web-конфигуратору

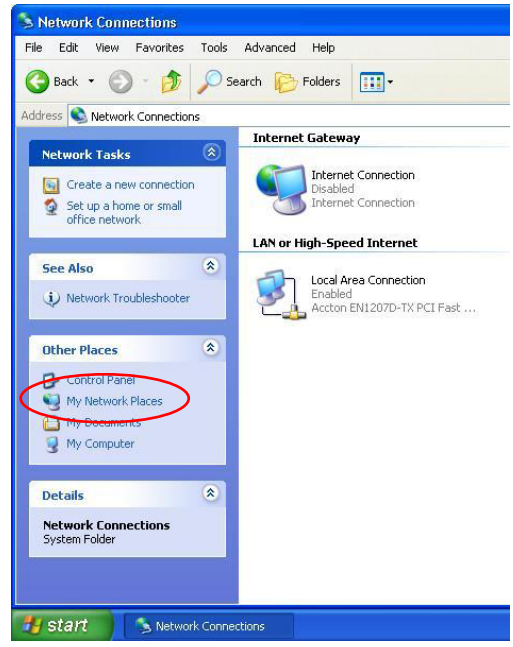
Функция UPnP позволяет обращаться непосредственно к Web-конфигуратору OMNI ADSL без необходимости предварительного поиска IP-адреса устройства . Это выглядит весьма полезным, если IP-адрес устройства OMNI ADSL неизвестен.

Для доступа к Web-конфигуратору выполните следующие действия.

Step 1. Щелкните **Start (Пуск)** и **Control Panel (Панель управления)**.

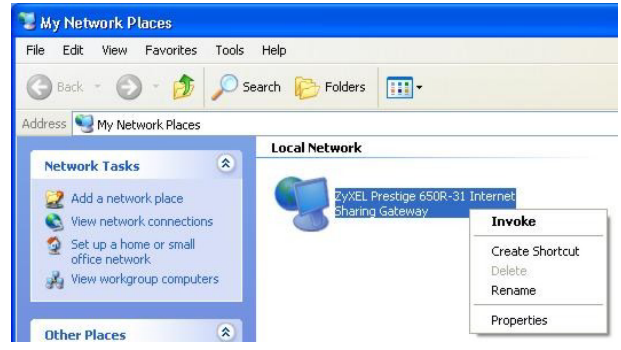
Step 2. Дважды щелкните по **Network Connections (Сетевые соединения)**.

Step 3. Выберите **My Network Places** под **Other Places**.



Step 4. Следующая иконка с описанием каждого подключенного устройства UPnP появится под надписью **Local Network (Локальная сеть)**.

Step 5. Щелкните правой кнопкой мыши по иконке, относящейся к Вашему устройству OMNI ADSL, и выберите **Invoke (Инициализировать)**. Появится экран регистрации Web-конфигуратора.



Step 6. Щелкните правой кнопкой мыши по иконке, относящейся к Вашему устройству OMNI ADSL, и выберите **Properties (Свойства)**. Появится окно свойств с основной информацией об устройстве OMNI ADSL.

Chapter 19
Журнальные экраны

В этой главе содержится информация о конфигурировании общих настроек журнала устройства OMNI ADSL и отображении их содержания. Данная глава относится к модели P650H-E. См. приложения для ознакомления с примерами пояснений к записям в журнале.

19.1 Описание журналов

Web-конфигуратор позволяет сделать выбор категорий событий и/или предупреждений, которые будут отображаться и храниться в журнале OMNI ADSL, или которые будут отправляться устройством OMNI ADSL какому-либо администратору (как E-Mail сообщения), или на сервер системного журнала.

19.1.1 Предупреждения и журналы

Под предупреждением понимается тип записи, требующей более серьезного внимания. К ним относятся сообщения: о системных ошибках, атаках (в части управления доступом) и попытках доступа к защищенным Web-сайтам. В состав некоторых категорий, таких как **System Errors (Системные ошибки),** входят как записи, так и предупреждения. Они отличаются по выделению цветом на экране **View Log (Просмотр журнала)**. Предупреждения выделяются красным цветом, а шрифт записей - черный.

19.2 Конфигурирование настроек журнала

Для настройки адресования рассылки системой OMNI ADSL регистрационных журналов, расписания их отправки, а также того, какие журналы и/или предупреждения должны регистрироваться устройством OMNI ADSL, следует использовать экраны **Log Settings**.

Для изменения настроек журнала OMNI ADSL щелкните **Logs (Журналы)**, а затем **Log Settings (Настройки журнала)**. Появится экран следующего вида.

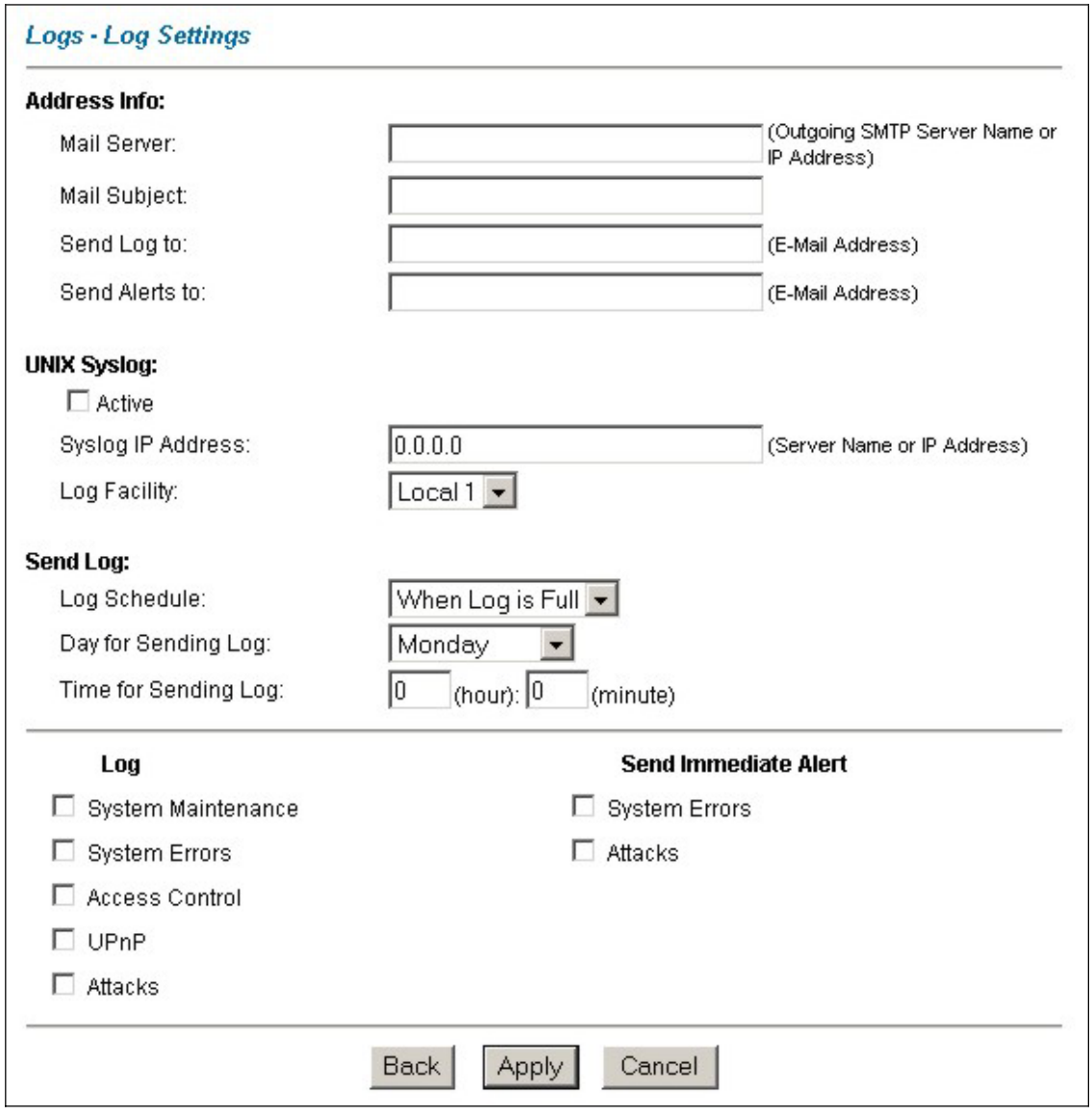


Рис. 19-1 Настройки журнала

В следующей таблице приведены описания полей данного экрана.

Табл. 19-1 Настройки журнала

ПОЛЕ	ОПИСАНИЕ
Address Info (Информация об адресе)	
Mail Server (Почтовый сервер)	Введите имя или IP-адрес почтового сервера для адресов электронной почты, указанных ниже. Если не заполнять это поле, журналы и предупреждения не будут высылаться по электронной почте.
Mail Subject (Тема сообщения)	Введите наименование заголовка, которое будет находиться в строке "Тема" сообщений журнала регистрации, отправляемых по электронной почте системой OMNI ADSL.
Send log to (Куда отправить журнал)	Журналы будут отправляться по E-mail адресам, указанным в этом поле. Если оставить это поле незаполненным, то журналы не будут высылаться по электронной почте.
Send alerts to (Куда отправить предупреждения)	Предупреждения будут отправляться по адресам электронной почты, указанным в этом поле. Если оставить это поле незаполненным, то предупреждения не будут высылаться по электронной почте.
UNIX Syslog (Системный журнал UNIX)	Системный журнал UNIX отправляет журнал на внешний сервер UNIX, использующийся для хранения журналов.
Active (Активно)	Щелкните по **Active (Активно)** для подключения системного журнала UNIX.
Syslog IP Address (IP-адрес системного журнала)	Введите имя или IP-адрес сервера системного журнала, где будут регистрироваться выбранные категории записей.
Log Facility (Функция журнальной регистрации)	Из раскрывающегося списка выберите местоположение. Журнальная утилита дает возможность регистрировать сообщения в различных файлах на сервере системного журнала. Подробные сведения см. в руководстве по системе UNIX.
Send Log (Отправить журнал)	

Табл. 19-1 Настройки журнала

ПОЛЕ	ОПИСАНИЕ
Log Schedule (План журнальной регистрации)	В этом "всплывающем" меню задается частота рассылки журнальных записей по электронной почте: • **Daily** • **Weekly** • **Hourly** • **When Log is Full** • **None** Если выбрана опция **Weekly (Еженедельно)** или **Daily (Ежедневно)**, укажите, в какое время дня следует отправлять электронную почту. Если выбрана опция **Weekly (Еженедельно)**, то укажите также в какой день недели следует отправлять электронную почту. Если выбрана опция **When Log is Full (После заполнения журнала регистрации)**, предупреждение будет отправлено после заполнения журнала. Если выбрана опция **None (Никогда)**, сообщения журнала регистрации отправляться не будут.
Day for Sending Log (День отправки журнала)	Используйте раскрывающийся список для выбора дня недели, когда должны отправляться журналы.
Time for Sending Log (Время отправки журнала)	Введите время суток в 24-часовом формате (например, 23:00 соответствует времени 11:00 вечера), когда должны быть отправлены журналы.
Log (Журнал)	Выберите категории записей, необходимые для регистрации. В состав записей входят предупреждения.
Send Immediate Alert (Отправить срочное предупреждение)	По своему усмотрению выберите категории предупреждений для регулярной отправки маршрутизатором OMNI ADSL электронной почтой предупреждений по адресам, указанным в поле **Send Alerts To (Куда отправлять предупреждения)**.
Back (Назад)	Щелкните по **Back (Назад)** для возврата к предыдущему экрану.
Apply (Применить)	Щелкните **Apply** (Применить) для сохранения настроек и выхода из меню.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для возврата к ранее сохраненным настройкам.

19.3 Отображение записей

Щелкните по **Logs (Записи)**, а затем по **View Logs (Отображение записей)** для вызова экрана **View Logs (Отображение записей)**. Экраном **View Logs (Отображение записей)** следует пользоваться для

просмотра записей согласно категориям, заданным с использованием экрана **Log Settings (Настройки журнала)** (см. *раздел 19.2*).

Записи в журнале, сделанные красным цветом, указывают предупреждения. После заполнения журнал закрывается и старые записи удаляются. Щелкните по заголовку столбца для сортировки записей. Треугольник служит для указания порядка сортировки (по убыванию или возрастанию).

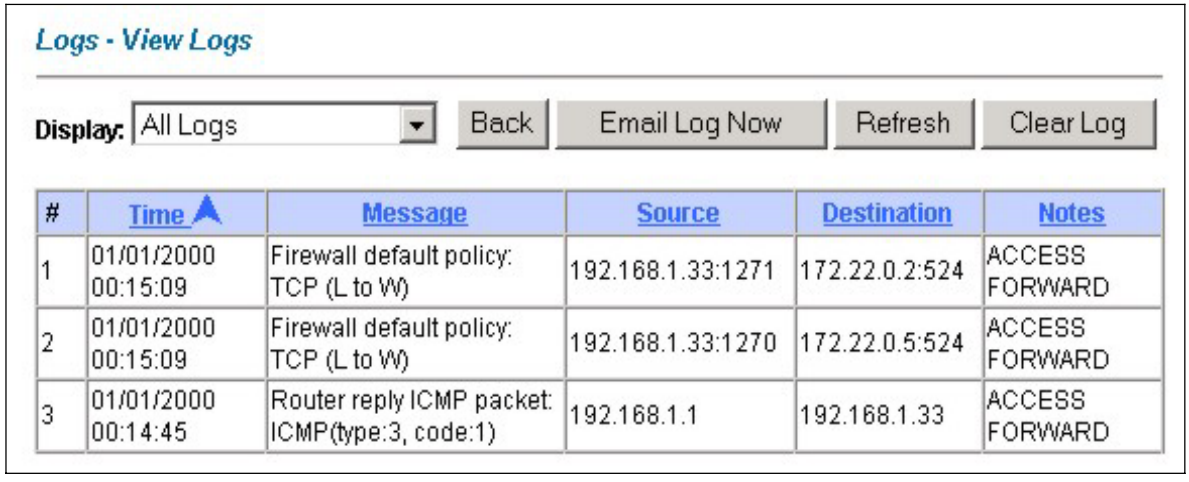


Рис. 19-2 Отображение записей

В следующей таблице приведены описания полей данного экрана.

Табл. 19-2 Отображение записей

ПОЛЕ	ОПИСАНИЕ
Display (Отобразить)	Категории записей, выбранные с использованием экрана **Log Settings** (см. *раздел 19.2*) отображаются в раскрывающемся списке. Выберите категорию записей для отображения. Выберите опцию **All Logs (Все записи)** для отображения записей всех категорий, указанных на странице **Log Settings (Настройка журналов)**.
Time (Время)	В этом поле отображается время, когда была сделана данная запись. См. главу об обслуживании системы и информации для установки времени и даты в устройстве OMNI ADSL.
Message (Сообщение)	В этом поле указывается причина регистрации записи;

Табл. 19-2 Отображение записей

ПОЛЕ	ОПИСАНИЕ
Source (Источник)	В этом поле указывается IP-адрес источника и номер порта входящего пакета.
Destination (Назначение)	В этом поле указывается IP-адрес назначения и номер порта входящего пакета.
Notes (Примечания)	В этом поле отображается дополнительная информация о записи в журнале.
Back (Назад)	Щелкните по **Back (Назад)** для возврата к предыдущему экрану.
Email Log Now (Отправить запись по электронной почте)	Щелкните **Email Log Now (Отправить запись по электронной почте)** для немедленной отправки экрана записи по E-Mail адресу, указанному на странице **Log Settings (Настройки журнала)** (убедитесь в том, что поля **Address Info (Информация об адресе)** в **Log Settings (Настройки журнала)** уже заполнены, см. *раздел 19.2*).
Refresh (Обновить)	Щелкните по **Refresh (Обновить)** для обновления информации на экране записи.
Clear Log (Удаление записей в журнале регистрации)	Щелкните по **Clear Log** для удаления всех записей.

19.4 Сообщения об ошибках SMTP

При возникновении каких-либо трудностей при отправке электронной почты появляются следующие сообщения об ошибках. О других видах сообщений об ошибках см. в разделе *Служебная информация* на входящем в комплект компакт-диске.

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

Табл. 19-3 Сообщения об ошибках SMTP

-1 означает, что устройство OMNI ADSL выключено из сети
-2 означает ошибку tcp SYN fail
-3 означает ошибку smtp server OK fail

Табл. 19-3 Сообщения об ошибках SMTP

-4 означает ошибку HELO fail
-5 означает ошибку MAIL FROM fail
-6 означает ошибку RCPT TO fail
-7 означает ошибку DATA fail
-8 означает ошибку mail data send fail

19.4.1 Образец заполнения журнала, отправленного электронной почтой

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

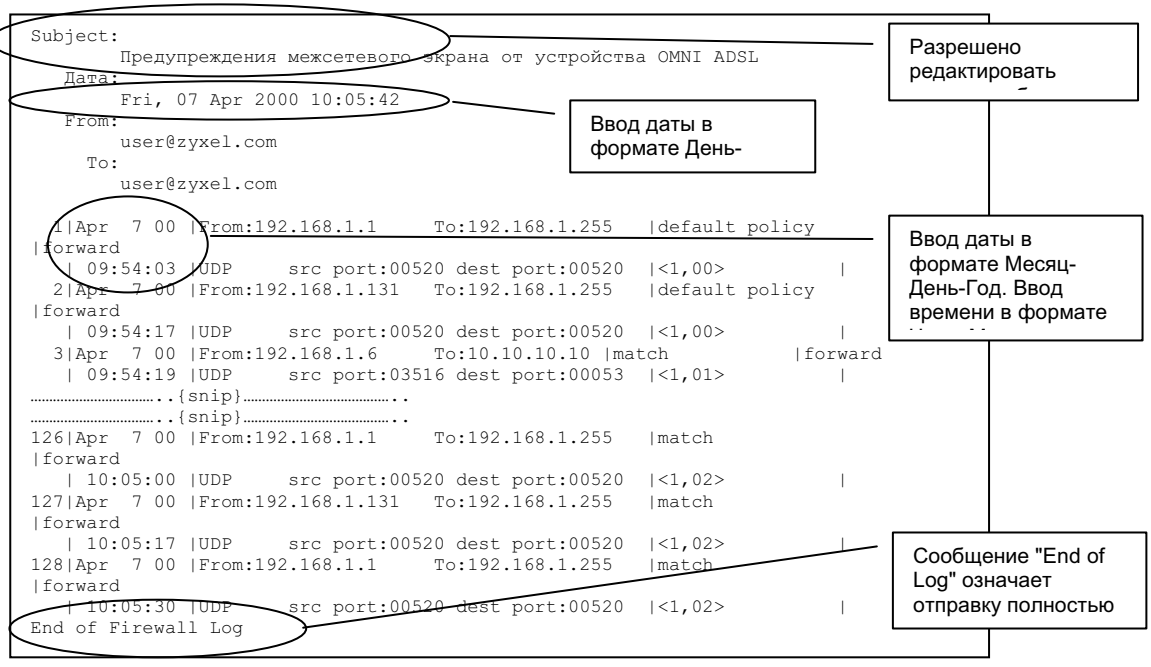


Рис. 19-3 Образец заполнения журнала, присланного по электронной почте

Part VII:

Управление пропускной способностью

В этой части руководства содержится информация о функциях и конфигурации управления пропускной способностью.

Chapter 20
Управление пропускной способностью

В этой главе описываются функции и конфигурация управления пропускной способностью. Содержание данной части относится только к моделям OMNI ADSL H/HW.

20.1 Описание процесса управления пропускной способностью

Управление пропускной способностью позволяет ввести ограничения пропускной способности интерфейса для определенных видов исходящего трафика. Это помогает убедиться в том, что OMNI ADSL пересылает определенные виды трафика (особенно приложения реального времени) с минимальной задержкой. С увеличением объема приложений реального времени, таких как передача речи по протоколу IP (VoIP), требования к управлению пропускной способностью также возрастают.

Управление пропускной способностью выдвигает такие вопросы как:

- Кто и на каких условиях получает право доступа к определенным приложениям?
- Как определить приоритетность каждого вида трафика?
- Какой трафик должен иметь гарантированную доставку?
- Какие ресурсы пропускной способности должны быть выделены для трафика с гарантированной доставкой?

Управление пропускной способностью позволяет также выполнить конфигурацию выходного интерфейса в целях определения какими ресурсами может оперировать сеть, что помогает уменьшить задержки трафика и количество сброшенных пакетов на ближайшем устройстве маршрутизации. Например, можно установить скорость передачи данных для интерфейса WAN равной 1000 кбит/с, если соединение ADSL имеет скорость исходящего потока 1000 кбит/с. На всех экранах настройки скорость трафика представляется в кбит/с (килобит в секунду), но в данном *Руководстве пользователя* используются для краткости также значения Мбит/с (мегабит в секунду).

20.2 Классы потребителей пропускной способности и фильтры

Понятие классов и дочерних классов потребителей пропускной способности позволяет решать задачи распределения пропускной способности заданной величины (бюджет пропускной способности). Конфигурирование фильтра пропускной способности для выделения класса (или дочернего класса)

потребителей пропускной способности основано на специфике приложений и/или подсетей. Следует воспользоваться таблицей **Class Configuration (Настройка класса)** (см. *раздел 20.9.1*) для назначения имен классам пропускной способности, распределения ресурсов пропускной способности и задания фильтров пропускной способности.. Можно выполнить настройку фильтра для одного класса потребителей пропускной способности. Можно также сделать настройку классов без фильтров. Тем не менее, рекомендуется, выполнение настройки дочерних классов с использованием фильтров пропускной способности для любого класса потребителей, настройка которого была выполнена без применения фильтров. OMNI ADSL оставляет определенный ресурс пропускной способности зарезервированным и недоступным для использования классами потребителей не имеющих своих фильтров или дочерними классами с фильтрами. Вы можете увидеть настройку классов и дочерних классов потребителей пропускной способности в таблице **Class Setup (Настройка классов)** (см. *раздел 20.9* для получения дополнительной информации).

Общие запасы ресурсов пропускной способности, выделенные при настройке дочерним классам потребителей, не могут превышать запасы ресурсов родительских классов.

20.3 Пропорциональное распределение ресурсов пропускной способности

Управление пропускной способностью позволяет установить какие ресурсы достаются каждому классу потребителей, однако в действительности значения ресурсов, выделяемых каждому классу, увеличиваются или уменьшаются пропорционально фактическому значению доступных ресурсов.

20.4 Примеры управления пропускной способностью

Эти примеры демонстрируют назначения программы управления пропускной способностью для интерфейса WAN, настроенного на скорость передачи данных 640 кбит/с.

20.4.1 Пример управления пропускной способностью для приложений

В приведенном ниже примере определение классов потребителей дается исключительно для приложений. Каждому классу потребителей ресурсов пропускной способности (VoIP, Web, FTP, E-mail и Video) выделено 128 кбит/с.

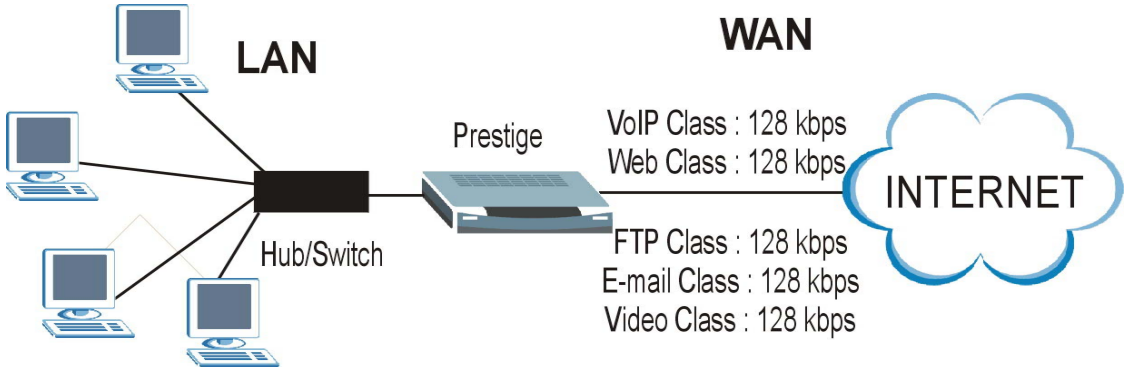


Рис. 20-1 Пример управления пропускной способностью для приложений

20.4.2 Пример управления пропускной способностью для подсетей

В приведенном ниже примере определение классов ресурсов дается исключительно для подсетей ЛВС. Каждому классу потребителей (Subnet A и Subnet B) выделено по 320 кбит/с.

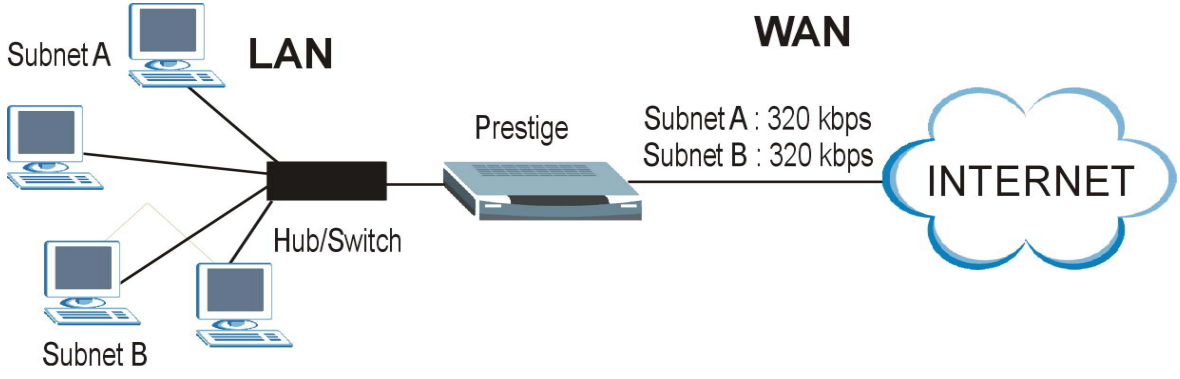


Рис. 20-2 Пример управления пропускной способностью для подсетей

20.4.3 Пример управления пропускной способностью для приложений и подсетей

В приведенном ниже примере определение классов потребителей дается для подсетей ЛВС и приложений (определенным приложениям в каждой подсети выделено определенное количество ресурсов пропускной способности).

Табл. 20-1 Пример управления пропускной способностью для приложений и подсетей

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

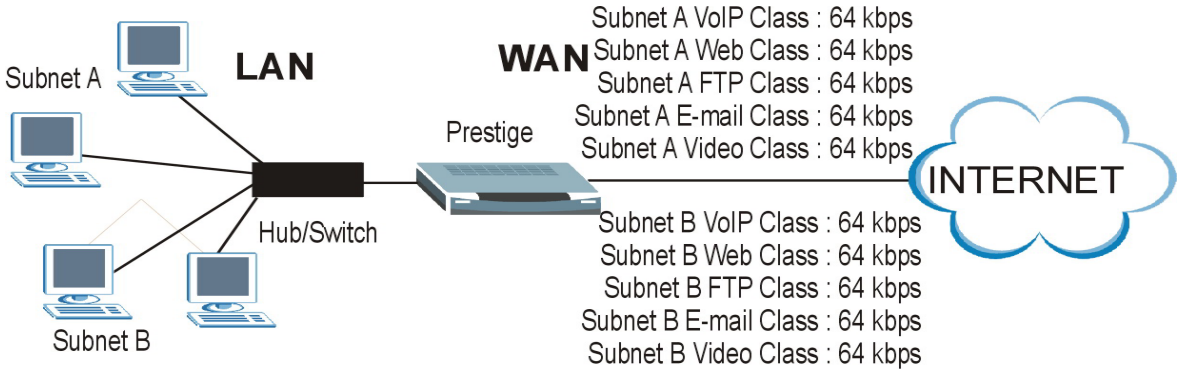


Рис. 20-3 Пример управления пропускной способностью для приложений и подсетей

20.5 Планировщик

Планировщик осуществляет распределение ресурсов пропускной способности интерфейса между различными классами потребителей. В устройстве OMNI ADSL имеется два типа планировщиков: с приоритетным и бесприоритетным обслуживанием.

20.5.1 Планировщик с приоритетным обслуживанием

При работе планировщика с приоритетным обслуживанием OMNI ADSL осуществляет передачу трафика разных классов потребителей соответственно назначенным приоритетам. Чем больше значение номера приоритета класса, тем выше его приоритет. Присвоение приложениям реального времени (таким как аудио и видео передачи) большего приоритета обеспечивает лучшее качество их работы.

20.5.2 Бесприоритетный планировщик

При работе бесприоритетного планировщика OMNI ADSL производит равномерное распределение ресурсов пропускной способности для различных классов потребителей, предупреждая тем самым возможность использования одним классом потребителей всех ресурсов пропускной способности интерфейса.

20.6 Максимальное использование пропускной способности

Опция максимального использования пропускной способности (см. *Рис. 20-7*) позволяет устройству OMNI ADSL распределить доступные ресурсы пропускной способности интерфейса (включая зарезервированные ресурсы, не использующиеся каким-либо классом потребителей) среди потребителей различных классов, нуждающихся в дополнительных ресурсах.
При включении данной опции OMNI ADSL вначале убеждается в том, что каждому классу потребителей выделен свой ресурс пропускной способности. Затем OMNI ADSL выполняет распределение доступных ресурсов пропускной способности интерфейса (не зарезервированных и не использующихся какими-либо классами потребителей) в зависимости от того, сколько классов потребителей (с учетом их приоритета) нуждается в дополнительных ресурсах. Если дополнительные ресурсы нужны только для одного класса потребителей, OMNI ADSL выделяет ему необходимое. Если дополнительные ресурсы пропускной способности нужны нескольким классам потребителей, OMNI ADSL выделяет классам с наивысшим приоритетом необходимые ресурсы (сколько требуется с учетом общего запаса), а затем - классам с меньшим приоритетом, если позволяет запас ресурсов. Распределение ресурсов среди классов потребителей с одинаковым приоритетом осуществляется устройством OMNI ADSL равномерно.

20.6.1 Резервирование ресурсов пропускной способности для трафика класса потребителей, не имеющих выделенного ресурса

Для работы трафика, не имеющего заданного фильтром ресурса, выполните следующие три последовательных действия для настройки устройства OMNI ADSL.

Оставьте часть ресурсов пропускной способности интерфейса нераспределенными.

Не включайте опцию интерфейса **Maximize Bandwidth Usage (Максимальное использование пропускной способности)**.

Не допускайте заимствования ресурсов дочерними классами потребителей, для которых родительским является корневой класс (см. *раздел 20.7*).

20.6.2 Пример применения опции максимального использование пропускной способности

Ниже приводится пример работы устройства OMNI ADSL с включенной опцией максимального использования пропускной способности интерфейса. На первом рисунке показаны все классы

потребителей, их приоритеты и значения ресурсов пропускной способности. Назначение классов сделано для подсетей. Интерфейс рассчитан на пропускную способность 10 Мбит/с. За каждой подсетью закреплен ресурс 2 Мбит/с. Наличие нераспределенного ресурса 2 Мбит/с делает возможным передачу трафика, не определенного ни в одном из фильтров, если не была установлена опция максимальной пропускной способности.

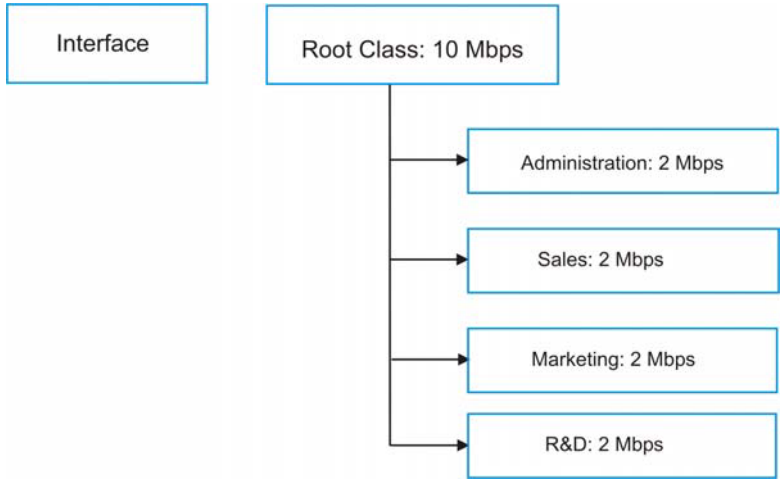


Рис. 20-4 Пример распределения ресурсов пропускной способности

На следующем рисунке приведен пример использования ресурсов при включенной опции максимального использования пропускной способности. OMNI ADSL осуществляет распределение нераспределенного ресурса пропускной способности в 2 Мбит/с среди классов, нуждающихся в дополнительных ресурсах. Если служба администрации сети использует только 1 Мбит/с из зарезервированных 2 Мбит/с, устройство OMNI ADSL выполнит также распределение оставшегося ресурса в 1 Мбит/с среди классов потребителей, нуждающихся в нем. Таким образом, OMNI ADSL осуществляет распределение общего ресурса в 3 Мбит/с из нераспределенных и неиспользуемых ресурсов пропускной способности среди классов потребителей, нуждающихся в них.

В данном случае, предполагается, что все классы потребителей, за исключением административного отдела, нуждаются в дополнительных ресурсах.

- Каждый класс потребителей получает доступ к зарезервированным для него ресурсам. Класс административного отдела пользуется только ресурсом в 1 Мбит/с из зарезервированных 2 Мбит/с.
- Классы потребителей Sales и Marketing имеют право на первоочередной доступ к дополнительным ресурсам пропускной способности поскольку обладают высшим приоритетом (6). Если каждому из них потребуется 1,5 Мбит/с или более пропускной способности, OMNI ADSL распределит имеющиеся в наличии 3 Мбит/с

незарезервированных и неиспользуемых ресурсов пропускной способности равномерно между отделами sales и marketing (по 1,5 Мбит/с дополнительно каждому из них из 3,5 Мбит/с доступных для всех классов), поскольку они имеют высшие уровни приоритета.

- Класс потребителей R&D нуждается в дополнительных ресурсах пропускной способности, но может получить только зарезервированные для него 2 Мбит/с, поскольку все незарезервированные и неиспользованные ресурсы передаются классам потребителей sales и marketing, имеющим высший приоритет.
- OMNI ADSL не разрешает отправку никакого трафика, не определенного фильтрами, поскольку все незарезервированные ресурсы пропускной способности передаются нуждающимся в них классам потребителей.

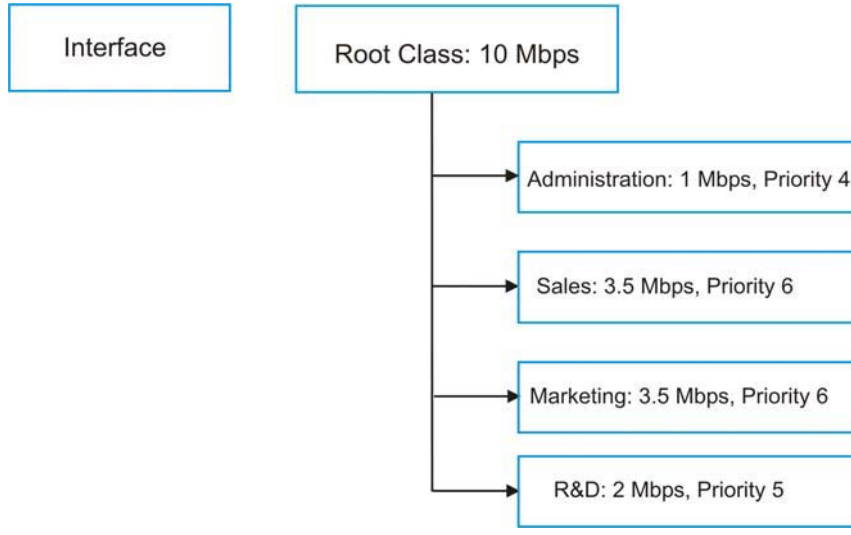


Рис. 20-5 Пример максимального использования ресурсов пропускной способности

20.7 Динамическое распределение пропускной способности

Динамическое распределение пропускной способности позволяет дочерним классам использовать ("заимствовать") неиспользуемые ресурсы пропускной способности их родительских классов, в случае если опция максимального использования пропускной способности разрешает "заимствовать" неиспользуемые и незарезервированные ресурсы пропускной способности всего интерфейса.

Включение опции динамического распределения пропускной способности применительно к дочернему классу позволяет ему воспользоваться невостребованными ресурсами его родительского класса. Невостребованные ресурсы родительского класса в первую очередь передаются дочернему классу потребителей, имеющему высший приоритет. Дочерний класс потребителей может также

воспользоваться ресурсами родительского класса следующего уровня ("дедушкин" класс), если настройки его родительского класса позволяют ему пользоваться ресурсами своего родительского класса. Таким образом, могут быть доступны ресурсы любого уровня, если их конфигурация позволяет обращение к ресурсам родительского класса (см. *раздел 20.7.1*).

В целом, выделение ресурсов пропускной способности для дочерних классов потребителей не должно превышать объемов ресурсов, выделенных для их родительских классов. В устройстве OMNI ADSL имеется планировщик, который выполняет распределение неиспользуемых ресурсов пропускной способности среди дочерних классов потребителей.

20.7.1 Пример динамического распределения пропускной способности

Здесь приведен пример управления пропускной способностью для классов потребителей с настройками для данного режима. Настройка классов выполнена применительно к иерархии отделов и отдельных пользователей, являющихся сотрудниками определенных отделов.

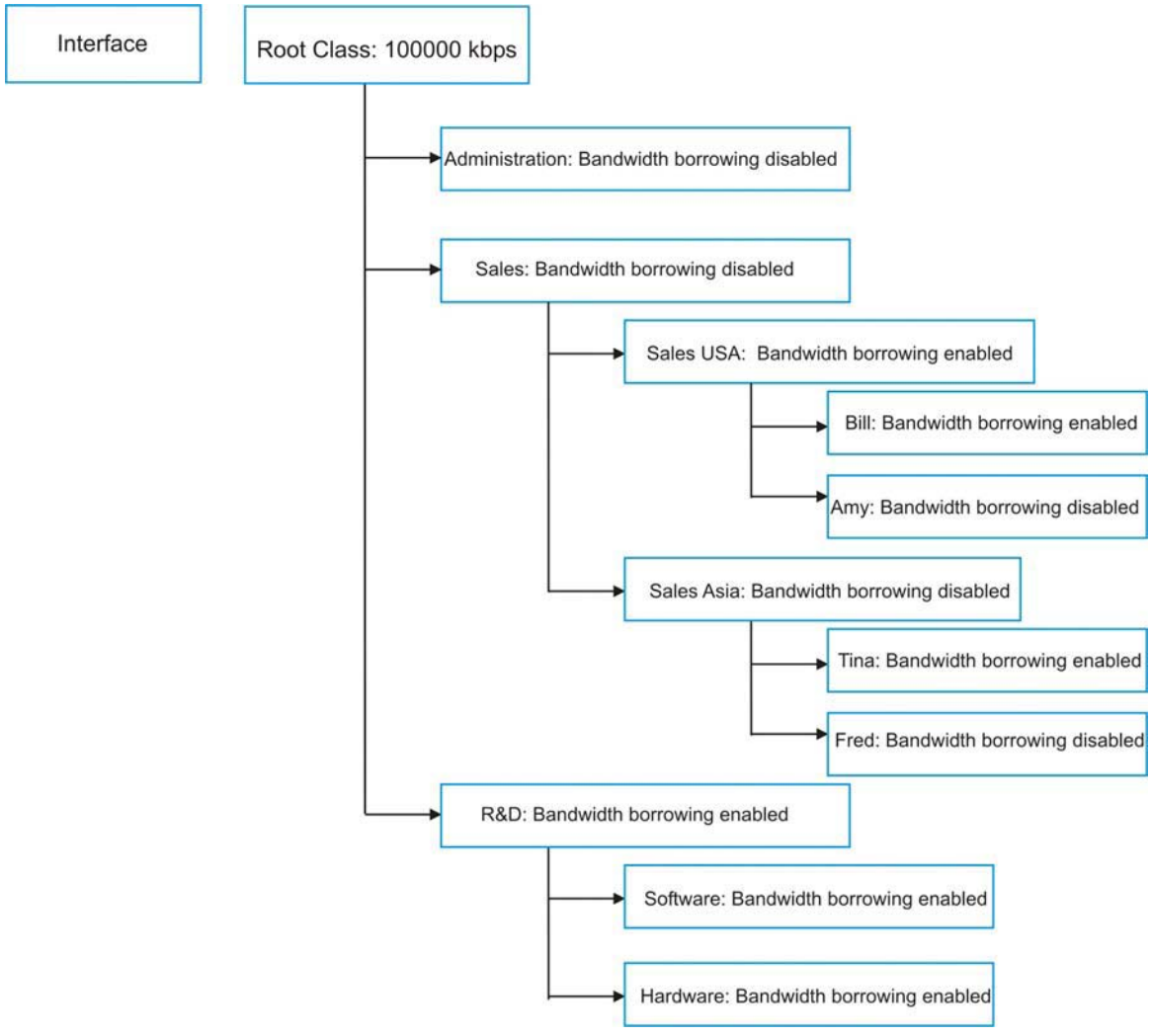


Рис. 20-6 Пример динамического распределения пропускной способности

- Класс потребителей Bill может "занять" неиспользуемые ресурсы пропускной способности у класса Sales USA, поскольку у класса Bill включена опция динамического распределения пропускной способности.

- Класс потребителей Bill может также "занять" неиспользуемые ресурсы пропускной способности у класса Sales, поскольку у класса Sales USA также включена опция динамического распределения пропускной способности.
- Класс потребителей Bill не может "занять" неиспользуемые ресурсы пропускной способности у корневого класса, поскольку у класса Sales опция динамического распределения пропускной способности отключена.
- Класс потребителей Amy не может "занять" неиспользуемые ресурсы пропускной способности у класса Sales USA, поскольку у класса Amy опция динамического распределения пропускной способности отключена.
- Классы R&D Software и Hardware могут оба "занять" неиспользуемые ресурсы пропускной способности у класса R&D, поскольку у обоих классов включена опция динамического распределения пропускной способности.
- Классы R&D Software и Hardware могут также "занять" неиспользуемые ресурсы и у корневого класса, поскольку у класса R&D также включена опция динамического распределения пропускной способностью.

20.7.2 Максимальное использование пропускной способности с применением динамического распределения пропускной способности

При настройке конфигурации интерфейса для максимального использования пропускной способности, а отдельных дочерних классов - на работу с динамическим распределением пропускной способности, устройство OMNI ADSL будет функционировать следующим образом.

1. OMNI ADSL передает трафик согласно распределению ресурсов пропускной способности между потребителями разных классов.
2. Устройство OMNI ADSL производит перераспределение неиспользуемых ресурсов родительских классов тем их дочерним классам, у которых размеры трафика превосходят размеры выделенных для них ресурсов и они имеют включенную опцию динамического распределения пропускной способности. OMNI ADSL отдает предпочтение классам с высшим приоритетом и одинаково воспринимает классы с равным приоритетом.
3. OMNI ADSL распределяет оставшиеся невостребованными незарезервированные ресурсы пропускной способности интерфейса среди любых классов потребителей, нуждающихся в этом. OMNI ADSL отдает предпочтение дочерним классам с высшим приоритетом и одинаково воспринимает классы с равным приоритетом.
4. OMNI ADSL назначает невостребованные и незарезервированные ресурсы пропускной способности для трафика потребителей, не относящихся к известным ему классам.

20.8 Настройка сводного отчета

Щелкните **BW Manager (Программа управления пропускной способностью)** , **Summary (Сводка)** для вызова экрана **Summary**.

Включите опцию управления пропускной способностью на интерфейсе и установите режим максимальной пропускной способности.

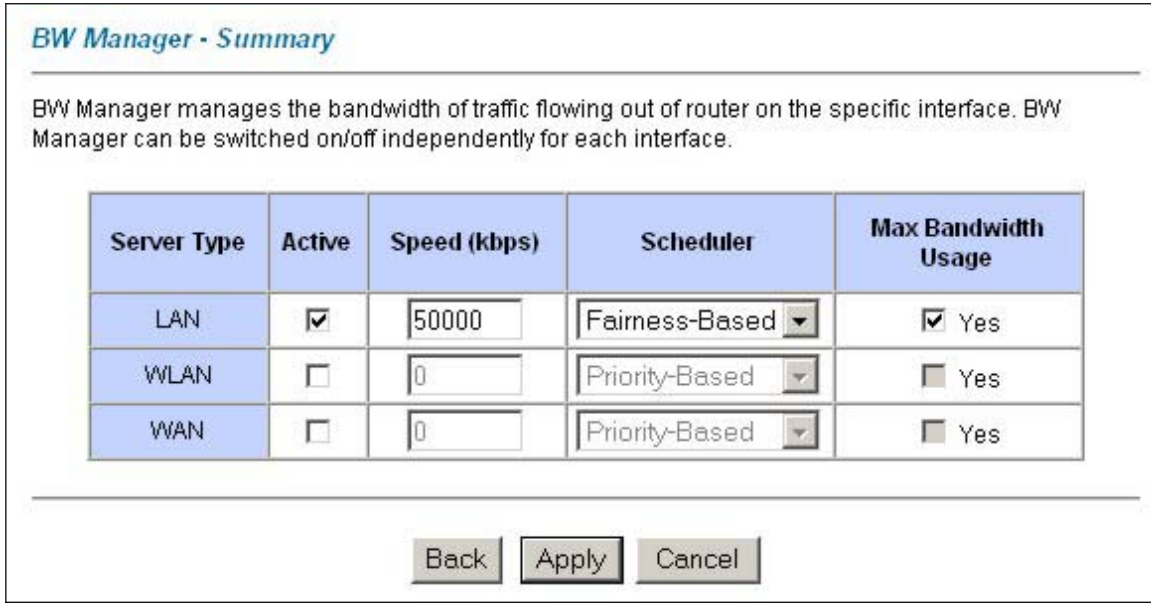


Рис. 20-7 Программа управления пропускной способностью: Summary (Сводный отчет)

В следующей таблице приведены описания полей данного экрана.

Табл. 20-2 Программа управления пропускной способностью: Summary (Сводный отчет)

ПОЛЕ	ОПИСАНИЕ
LAN WLAN WAN	В этих полях содержится информация (только для чтения) о состоянии физических интерфейсов.
Active (Активно)	Поставьте метку в окошке нужного интерфейса для включения опции управления пропускной способностью.

Табл. 20-2 Программа управления пропускной способностью: Summary (Сводный отчет)

ПОЛЕ	ОПИСАНИЕ
Speed (kbps) (Скорость, кбит/с)	Введите значение пропускной способности данного интерфейса, которое Вы хотите назначить для него при использовании опции управления пропускной способностью. Это значение будет отображаться как величина ресурса пропускной способности корневого класса потребителей интерфейса (см. *раздел 20.9*). Рекомендуется установка величины скорости передачи данных, соответствующей реальной скорости передачи данных интерфейсного соединения. Например, установите скорость передачи данных интерфейса WAN равной 1000 кбит/с, если максимальное значение скорости передачи данных соединения ADSL соответствует 1000 кбит/с.
Scheduler (Планировщик)	Выберите из выпадающего меню для выбора режима управления потоком трафика **Priority Based (Приоритетное)** или **Fairness (Бесприоритетное)**. Выберите режим **Priority Based (Приоритетное)** для управления распределением с предпочтением для классов потребителей с высшим приоритетом. Выберите режим**Fairness (Бесприоритетное)** для управления распределением среди классов потребителей с одинаковым приоритетом. См. *раздел 20.5*.
Maximize Bandwidth Usage (Максимальное использование пропускной способности)	Поставьте метку в этом окошке для того чтобы OMNI ADSL выполнил распределение всех незарезервированных и/или неиспользуемых ресурсов пропускной способности интерфейса между классами потребителей, нуждающихся в дополнительных ресурсах. Не выполняйте это назначение, если хотите зарезервировать часть ресурсов пропускной способности для потребителей, не принадлежащих к известным классам (см. *раздел 20.6.1*), или хотите установить ограничения по скорости передачи данных для этого интерфейса (см. описание поля **Speed (Скорость)**).
Back (Назад)	Щелкните **Back** для возврата к главному экрану **BW Manager (Программа управления пропускной способностью)**.
Apply (Применить)	Щелкните по кнопке **Apply (Применить)** для сохранения настроек.
Cancel (Отмена)	Щелкните по кнопке **Cancel (Отмена)** для повторной настройки данного экрана.

20.9 Конфигурирование настройки класса

На экране настройки классов отображается конфигурация классов потребителей ресурсов пропускной способности по отдельным интерфейсам. Выберите интерфейс и нужные кнопки для выполнения

описанных ниже действий. Щелкните по кнопке “+” для включения новых объектов в дереве классов или щелкните по кнопке “-“ для их исключения. В каждом интерфейсе имеется свой постоянный корневой класс потребителей. Ресурс пропускной способности для корневого класса равен скорости передачи данных, установленной для данного интерфейса (см. *раздел 20.8* для установки скорости передачи данных интерфейса). Настройка для корневого класса уровней дочерних классов.

Для подключения или исключения дочерних классов интерфейса щелкните по **BW Manager (Программа управления пропускной способностью)**, а затем по **Class Setup (Настройка классов)**. Появится следующий экран (показан с примерами классов).

В этом примере 15 Мбит/с незарезервированных ресурсов пропускной способности выделены для трафика, не имеющего назначений в фильтрах (см. *раздел 20.6.1*). Классы потребителей пропускной способности Administration и Sales USA обладают большими ресурсами, чем объединенные ресурсы пропускной способности их дочерних классов. Дочерние классы могут "занимать" дополнительные ресурсы до тех пор, пока у них включена опция динамического распределения пропускной способности (см. *раздел 20.7*).

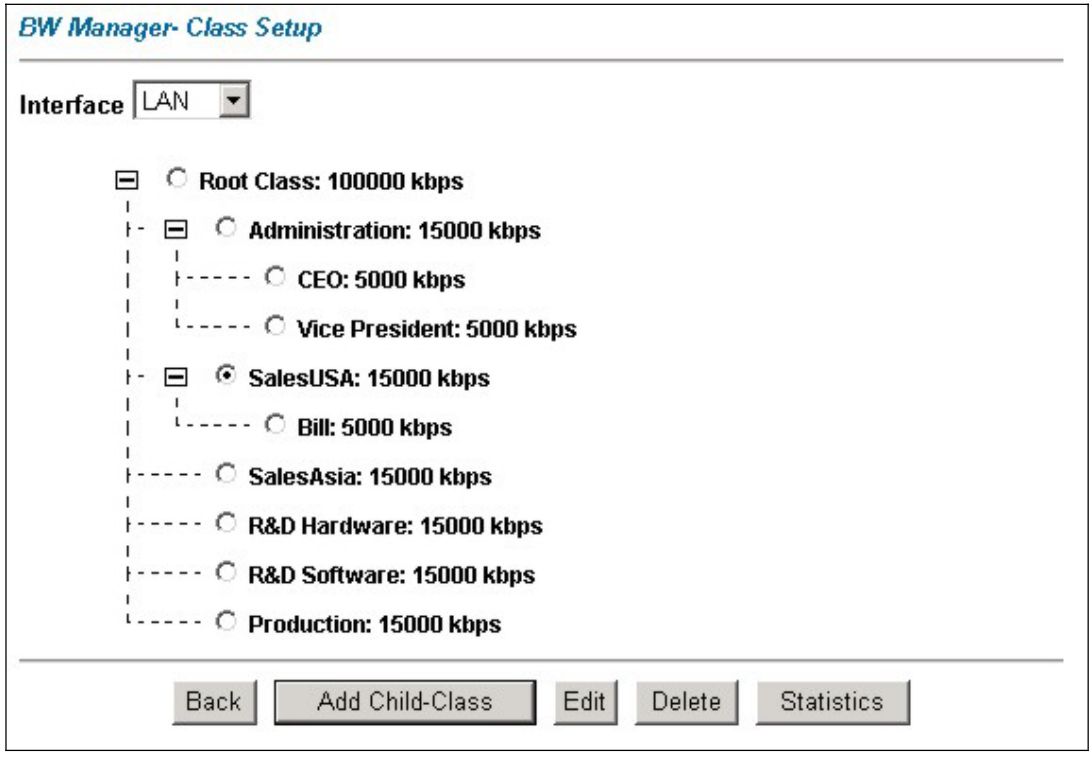


Рис.20-8 Программа управления пропускной способностью: Настройка классов

В следующей таблице приведены описания полей данного экрана.

Табл. 20-3 Программа управления пропускной способностью: Настройка классов

ПОЛЕ	ОПИСАНИЕ
Interface (Интерфейс)	Выберите интерфейс из раскрывающегося списка, для которого вы хотели бы выполнить настройку классов.
Back (Назад)	Щелкните по **Back** для возврата к главному экрану **BW Manager (Программа управления пропускной способностью)**.
Add Child-Class (Добавить дочерний класс)	Щелкните по **Add Child-class (Добавить дочерний класс)** для того чтобы добавить новый подкласс.
Edit (Редактировать)	Щелкните по **Edit (Редактировать)** для настройки выбранного класса. Нельзя выполнять редактирование корневого класса.
Delete (Удалить)	Щелкните по **Delete (Удалить)** для того чтобы удалить класс и все его дочерние классы. Нельзя удалить корневой класс.
Statistics (Статистика)	Щелкните по **Statistics (Статистика)** для отображения статуса выбранного класса.

20.9.1 Конфигурация класса из программы управления пропускной способностью

Конфигурация класса потребителей из программы управления пропускной способностью выполняется в экране **Class Configuration (Настройка класса)**. Следует воспользоваться экраном **Bandwidth Manager - Summary (Программа управления пропускной способностью - Сводный отчет)** для включения опции управления пропускной способностью на интерфейсе прежде, чем Вы будете осуществлять для него конфигурацию классов.

Для добавления дочернего класса щелкните по **BW Manager (Программа управления пропускной способностью)**, а затем по **Class Setup (Настройка класса)**. Щелкните по кнопке **Add Child-Class (Добавить дочерний класс)** для вызова следующего экрана.

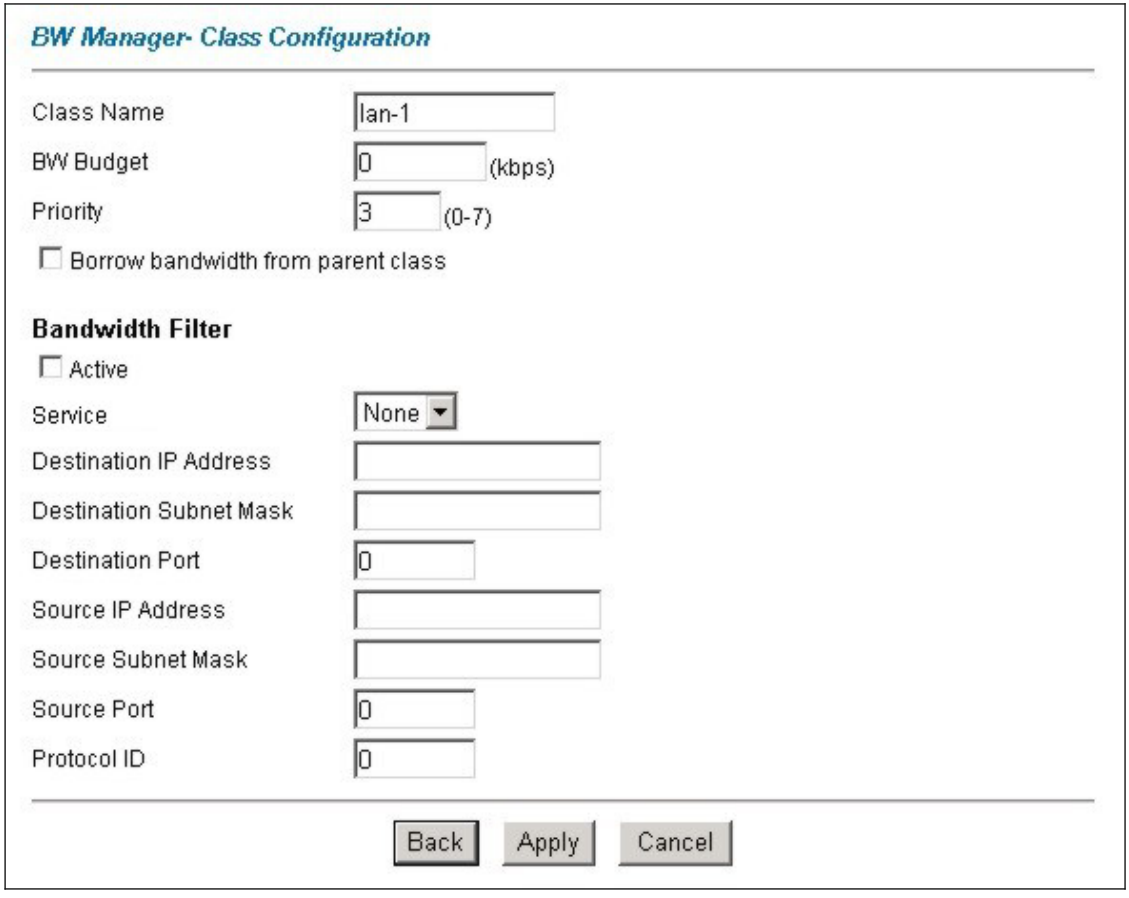


Рис. 20-9 Программа управления пропускной способностью: Настройка класса

В следующей таблице приведены описания полей данного экрана.

Табл. 20-4 Программа управления пропускной способностью: Class Configuration (Настройка класса)

ПОЛЕ	ОПИСАНИЕ
Имя класса	Воспользуйтесь автоматически сгенерированным именем или введите другое идентифицирующее имя размером до 20 буквенно-цифровых символов, включая пробелы.

Табл. 20-4 Программа управления пропускной способностью: Class Configuration (Настройка класса)

ПОЛЕ	ОПИСАНИЕ
BW Budget (Ресурсы пропускной способности) (кбит/с)	Укажите максимальное значение ресурсов пропускной способности, разрешенное для данного класса, в кбит/с. Рекомендуется выбрать для отдельного класса потребителей значение из диапазона от 20 кбит/с до 20000 кбит/с.
Priority (Приоритет)	Введите значение от 0 до 7 для определения приоритета данного класса. Чем больше значение, тем выше приоритет. По умолчанию задано 3.
Borrow bandwidth from parent class ("Заем" ресурсов родительского класса	Данная опция разрешает дочернему классу "занимать" ресурсы пропускной способности родительского класса, если он не пользуется ими. Процесс динамического распределения ресурсов пропускной способности руководствуется значениями приоритетов дочерних классов потребителей. Это означает, что дочерний класс с высшим приоритетом (7) является первым претендентом на использование ресурсов своего родительского класса. Не следует пользоваться подобным назначением для классов, замыкающихся непосредственно на корневой класс, если хотите оставить доступными ресурсы пропускной способности для других видов трафика (см. *20.6.1*) или если хотите установить скорость передачи данных интерфейса, соответствующей скорости работы ближайшего к нему сетевого устройства (см. описание поля **Speed (Скорость)** в *Табл. 20-2*).
Bandwidth Filter (Фильтр пропускной способности) OMNI ADSL пользуется фильтром для идентификации принадлежности трафика определенному классу потребителей ресурсов пропускной способности.	
Active (Активно)	Поставьте флажок в окошке для назначения данному классу фильтра управления пропускной способностью.

Табл. 20-4 Программа управления пропускной способностью: Class Configuration (Настройка класса)

ПОЛЕ	ОПИСАНИЕ
Service (Тип обслуживания)	Вместо выполнения настройки полей **Destination Port (Порт назначения)**, **Source Port (Порт источника)** и **Protocol ID (Идентификатор протокола)** можно выбрать предварительно заданный сервис . Протокол SIP (инициализации сеансов) является сигнальным протоколом, использующимся в Интернет-телефонии, при передаче срочных сообщений и других приложений VoIP (протокола передачи голосовой информации через IP). Выберите **SIP** из раскрывающегося списка для настройки данного полосового фильтра для трафика с использованием протокола SIP. На момент написания руководства SIP считалась только предварительно определенной услугой. При выборе опции **None** класс потребителей будет обращаться ко всем видам услуг до тех пор, пока одна из них не будет указана в настройке полей **Destination Port (Порт назначения)**, **Source Port (Порт источника)** и **Protocol ID (Идентификатор протокола)**.
Destination IP Address (IP-адрес назначения)	Введите IP-адрес назначения в десятичном виде с разделительными точками Незаполненное поле IP-адреса назначения означает - "любой IP-адреса назначения".
Destination Subnet Mask (Маска подсети назначения)	Введите значение маски подсети назначения. Это поле будет недоступным, если не указан **Destination IP Address (IP-адрес назначения)**. См. приложение для получения дополнительной информации об IP-адресовании подсетей.
Destination Port (Порт назначения)	Введите номер порта назначения. Незаполненное поле означает: любой порт назначения.
Source IP Address (IP-адрес источника)	Введите значение IP-адреса источника. Незаполненное поле IP-адреса назначения означает: любой IP-адрес источника.
Source Subnet Mask (Маска подсети источника)	Введите значение маски подсети источника. Это поле будет недоступным, если не указан **Source IP Address (IP-адрес источника)**. См. приложение для получения дополнительной информации об IP-адресовании подсетей.
Source Port (Порт источника)	Введите номер порта источника. См. следующую табл. для получения информации о некоторых популярных услугах и нумерации портов. Незаполненное поле порта источника означает: "любой номер порта источника".

Табл. 20-4 Программа управления пропускной способностью: Class Configuration (Настройка класса)

ПОЛЕ	ОПИСАНИЕ
Protocol ID (Идентификатор протокола)	Введите значение идентификатора (номера) протокола (вида услуги), например: 1 для ICMP, 6 для TCP или 17 для UDP. Незаполненное поле идентификатора протокола означает: "любой номер протокола".
Back (Назад)	Щелкните по **Back** для возврата к главному экрану **BW Manager (Программа управления пропускной способностью)**.
Apply (Применить)	Щелкните по **Apply (Применить)** для сохранения внесенных изменений.
Cancel (Отмена)	Щелкните по **Cancel (Отмена)** для повторной настройки данного экрана.

Табл. 20-5 Услуги и номера портов

УСЛУГА	НОМЕР ПОРТА
ECHO	7
FTP (Протокол передачи файлов)	21
SMTP (Простой протокол пересылки почты)	25
DNS (Служба имен доменов)	53
Finger	79
HTTP (Протокол передачи гипертекста или WWW, Web)	80
POP3 (Почтовый протокол)	110
NNTP (Сетевой протокол передачи новостей)	119
SNMP (Простой протокол управления сетью)	161
Прерывание SNMP	162
PPTP (Туннельный протокол "точка-точка")	1723

20.9.2 Статистика управления пропускной способностью

Для отображения информации о производительности сети необходимо пользоваться экраном **Bandwidth Management Statistics (Статистика управления пропускной способностью)** . Щелкните

по кнопке **Statistics (Статистика)** на экране **Class Setup (Настройка класса)** для вызова экрана **Statistics** .

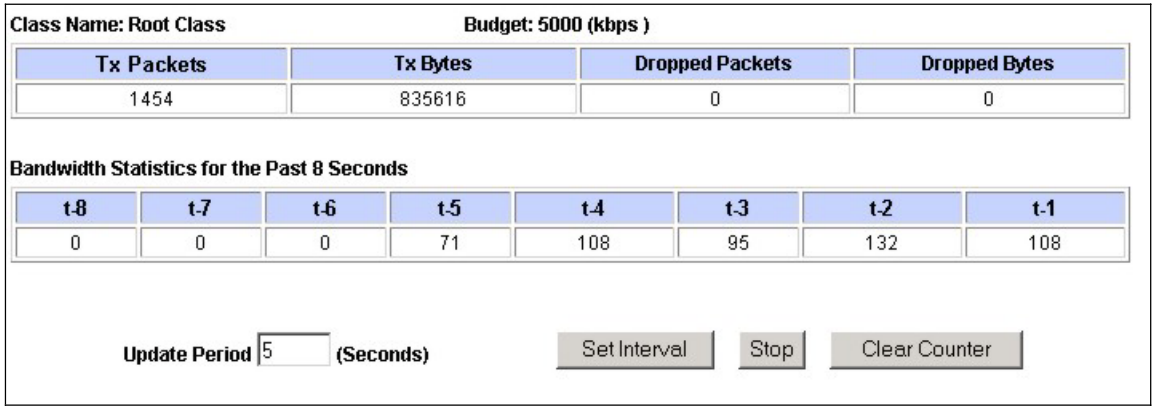


Рис. 20-10 Статистика управления пропускной способностью

В следующей таблице приведены описания полей данного экрана.

Табл. 20-6 Статистика управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Class Name (Имя класса)	В этом поле отображается имя класса, показанного на странице статистики.
Budget (kbps) (Ресурсы, кбит/с)	В этом поле отображается величина ресурсов пропускной способности, назначенных для данного класса.
Tx Packets (Передано пакетов)	В данном поле отображается значение общего числа переданных пакетов.
Tx Bytes (Передано байт)	В данном поле отображается значение общего объема переданных данных в байтах.
Dropped Packets (Сброшенные пакеты)	В данном поле отображается значение общего числа сброшенных пакетов.

Табл. 20-6 Статистика управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Dropped Bytes (Сброшенные байты)	В данном поле отображается значение общего объема сброшенных данных в байтах.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1) (Статистика управления пропускной способностью за последние 8 секунд (от t-8 до t-1)	
В этом поле отображаются статистические данные управления пропускной способностью (в бит/с) за последние интервалы времени от 1 до 8 секунд. Например, t-1 означает: "одну секунду назад".	
Update Period (seconds) (Период обновления, в секундах)	Введите значение временного интервала в секундах для задания частоты обновления информации.
Set Interval (Установка интервала)	Щелкните по **Set Interval (Установка интервала)** для инициализации нового значения интервала обновления, введенного выше в поле **Update Period (Период обновления)**.
Stop Update (Остановка обновления)	Щелкните по **Stop Update (Остановка обновления)** для прекращения работы браузера по обновлению статистики управления пропускной способностью.
Clear Counter (Очистка счетчика)	Щелкните по **Clear Counter (Очистка счетчика)** для обнуления статистики управления пропускной способностью.

20.10 Configuring Monitor (Настройка монитора)

Для отображения всех используемых устройством OMNI ADSL ресурсов пропускной способности и назначений щелкните по **BW Manager (Программа управления пропускной способностью)**, а затем по **Monitor (Монитор)**. Появится экран следующего вида.

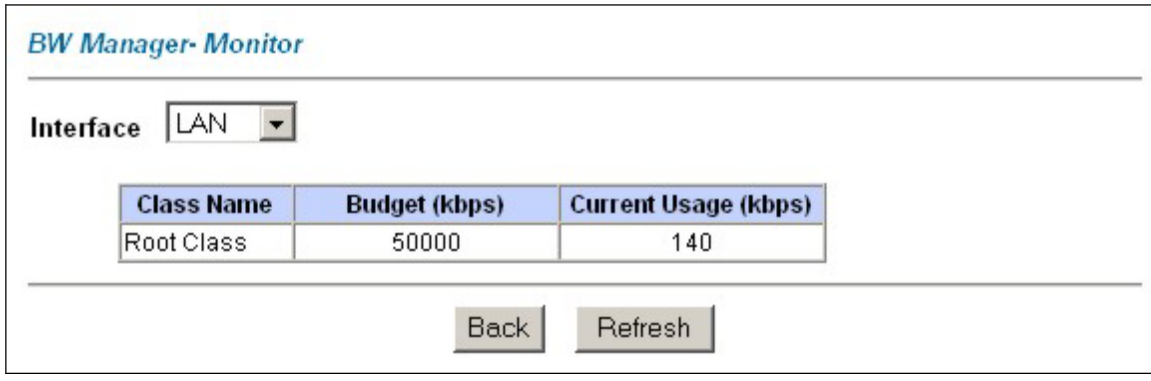


Рис. 20-11 Монитор программы управления пропускной способностью

В следующей таблице приведены описания полей данного экрана.

Табл. 20-7 Монитор программы управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Interface (Интерфейс)	Выберите из раскрывающегося списка интерфейс для отображения его ресурсов пропускной способности, использующихся различными классами пользователей.
Class Name (Имя класса)	В этом поле отображается имя класса.
Budget (kbps) (Ресурсы, кбит/с)	В этом поле отображается величина ресурсов пропускной способности, назначенных для данного класса.
Current Usage (kbps) (Текущее использование пропускной способности, кбит/с)	В этом поле отображается величина пропускной способности, используемых каждым классом.
Back (Назад)	Щелкните по **Back** для возврата к главному экрану **BW Manager (Программа управления пропускной способностью)**.
Refresh (Обновить)	Щелкните по **Refresh (Обновить)** для обновления содержания страницы.

Part VIII:

Сопровождение

В данной части рассматривается работа с экранами сопровождения.

Chapter 21
Сопровождение

В данной главе представлена информация о системе, включая сведения о микропрограммном обеспечении ZyNOS, IP-адресах портов и статистике трафика через порты.

21.1 Описание сопровождения

Пользуйтесь экранами сопровождения для отображения информации о системе, загрузки нового микропрограммного обеспечения, управления конфигурацией и перезапуска устройства OMNI ADSL.

21.2 Экран состояния системы

Щелкните по **System Status (Состояние системы)** для вызова следующего экрана, которым можно пользоваться для контроля работы устройства OMNI ADSL. Отметим, что содержимое этих полей доступно только для чтения и предназначено для диагностических целей.

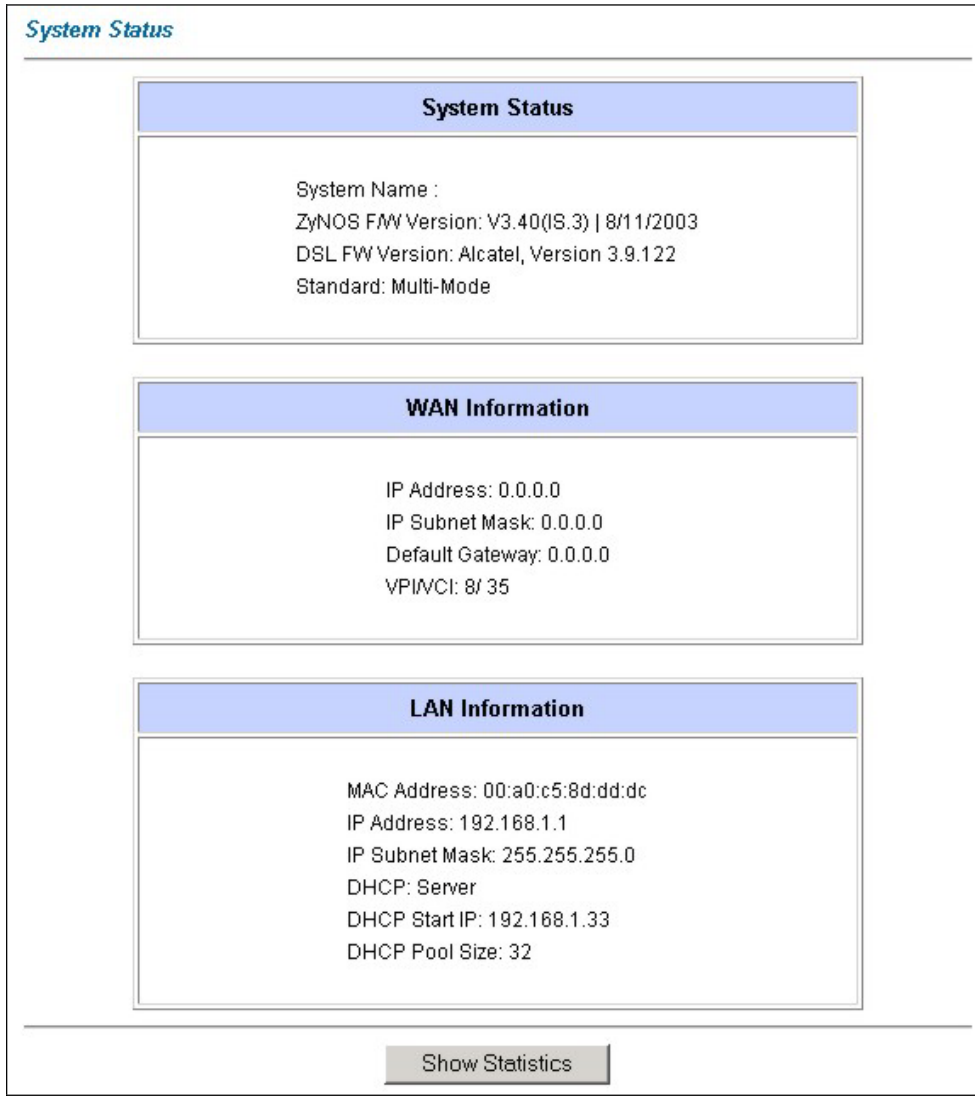


Рис. 21-1 Состояние системы

В следующей таблице приведены описания полей данного экрана.

Табл. 21-1 Состояние системы

ПОЛЕ	ОПИСАНИЕ
System Status (Системный статус)	
System Name	Имя Вашего маршрутизатора OMNI ADSL, необходимое для целей его идентификации.
ZyNOS F/W Version	Наименование версии микропрограммного обеспечения ZyNOS и даты его создания. ZyNOS является сетевой операционной системой, разработанной компанией ZyXEL.
DSL FW Version	Микропрограммное обеспечение версии DSL, предназначенное для Вашей модели OMNI ADSL.
Standard	Стандарт, использующийся Вашей моделью OMNI ADSL.
WAN Information (Информация о глобальной сети)	
IP Address	IP-адреса порта WAN.
IP Subnet Mask	Маска подсети IP-порта WAN.
Default Gateway	IP-адрес шлюза (если он используется), назначенный по умолчанию.
VPI/VCI	Идентификаторы виртуального пути (VPI) и виртуального канала (VCI), установленные в первом экране мастер-программы.
LAN Information (Информация о локальной сети)	
MAC Address	MAC-адрес (протокола управления доступом к среде) или адрес Ethernet, являющийся уникальным для Вашего устройства OMNI ADSL.
IP Address	IP-адрес порта LAN.
IP Subnet Mask	Маска подсети IP-адреса порта LAN.
DHCP	Функция DHCP порта WAN - **Server (Сервер)**, **Relay (Ретранслятор)** (не для всех моделей OMNI ADSL) или **None**.
DHCP Start IP	Начальный адрес из пула непрерывных IP-адресов.

Табл. 21-1 Состояние системы

ПОЛЕ	ОПИСАНИЕ
DHCP Pool Size	Количество адресов в пуле непрерывных IP-адресов.
Show Statistics	Щелкните по **Show Statistics (Показать статистику)** для отображения статистических данных, характеризующих работу маршрутизатора, таких как количество отправленных или полученных каждым портом пакетов.

21.2.1 Статистические сведения о системе

Щелкните **Show Statistics (Показать статистику)** в экране **System Status (Состояние системы)** для вызова следующего экрана. В состав информации "только для чтения" входят сведения о состоянии портов и отдельные статистические сведения о пакетах данных. Туда также входят сведения о суммарном времени соединения для системы и интервале (-ах) между запросами устройств. Поле **Poll Interval(s)** является реконфигурируемым.

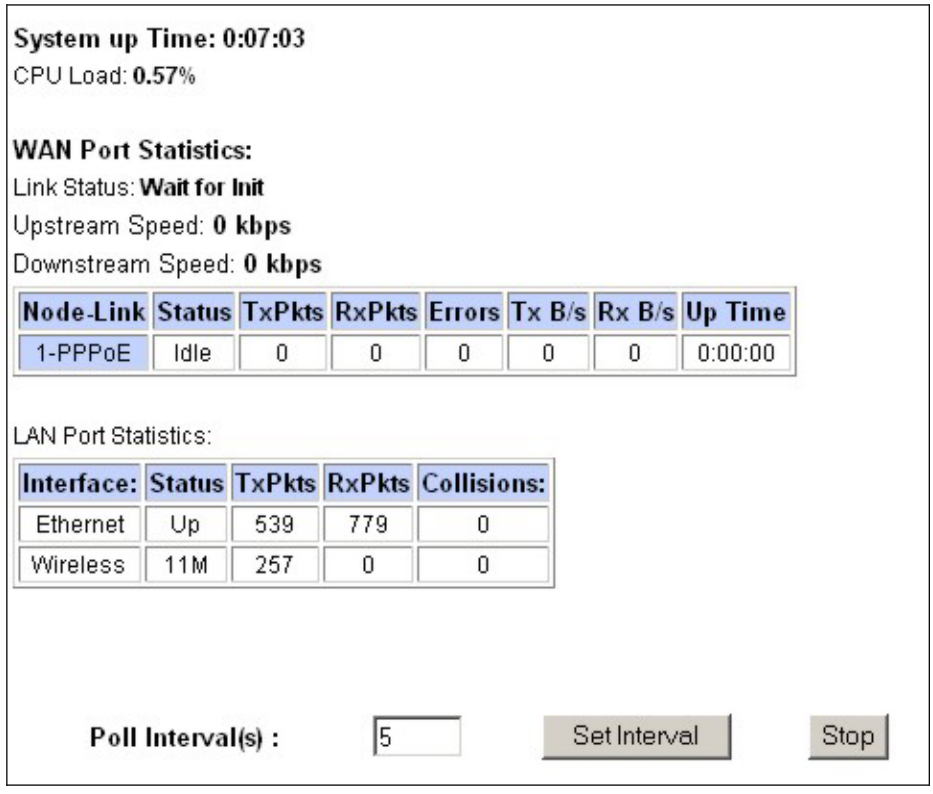


Рис. 21-2 Состояние системы: отображение статистических сведений

В следующей таблице приведены описания полей данного экрана.

Табл. 21-2 Состояние системы: Отображение статистических сведений

ПОЛЕ	ОПИСАНИЕ
System up Time	Время работы системы с начала эксплуатации.
CPU Load	Сведения о загрузке процессора в процентах.
WAN Port Statistics	Статистика порта WAN.
Link Status	Состояние канала связи с WAN.

Табл. 21-2 Состояние системы: Отображение статистических сведений

ПОЛЕ	ОПИСАНИЕ
Transfer Rate	Скорость передачи данных в кбит/с.
Upstream Speed	Скорость передачи устройства OMNI ADSL.
Downstream Speed	Скорость приема устройства OMNI ADSL.
Node-Link	Значение индекса удаленного узла и тип связи, включая PPPoA, ENET, RFC 1483 и PPPoE.
LAN Port Statistics	Статистика порта LAN.
Interface	Это поле отображает тип порта.
Status	Для порта WAN: скорость передачи данных через порт и настройки дуплексной связи, если применяется инкапсуляция Ethernet, или значения **down** (линия отключена), **idle** (линия (ppp) свободна), **dial** (вызов), или **drop** (сброс вызова), если применяется инкапсуляция PPPoE. Для порта LAN: скорость передачи данных через порт и настройки дуплексной связи.
TxPkts	Количество переданных через порт пакетов.
RxPkts	Количество полученных через порт пакетов.
Errors	Количество пакетов с ошибкой на канале.
Tx B/s	Число байтов, переданных за последнюю секунду.
Rx B/s	Число байтов, полученных за последнюю секунду.
Up Time	Значение времени наработки данного порта с начала работы.
Collisions	Количество конфликтов при передаче через данный порт.
Poll Interval(s)	Введите значение временного интервала обновления статистических сведений для браузера.
Set Interval	Щелкните по этой кнопке для включения нового значения интервала запросов, заданного выше в поле **Poll Interval**.

Табл. 21-2 Состояние системы: Отображение статистических сведений

ПОЛЕ	ОПИСАНИЕ
STOP	Щелкните по этой кнопке для остановки обновления статистики о работе системы.

21.3 Экран таблицы DHCP

DHCP (Dynamic Host Configuration - Протокол динамического конфигурирования хост-машины, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получить при начальной загрузке конфигурацию TCP/IP с сервера. OMNI ADSL можно сконфигурировать как сервер DHCP или отключить эту функцию. При конфигурации в качестве сервера, OMNI ADSL предоставляет клиентам конфигурацию TCP/IP. Установка **None** отключает данную функцию, и в этом случае необходимо иметь другой сервер DHCP в локальной сети, или произвести настройку компьютера вручную.

Щелкните по **MAINTENANCE (СОПРОВОЖДЕНИЕ)**, а затем по закладке **DHCP Table (Таблица DHCP)**. Данная информация (только для чтения) относится к Вашему статусу DHCP. В таблице DHCP отображается информация о текущем состоянии DHCP (включая **IP Address (IP-адрес)**, **Host Name (Имя хоста)** и **MAC Address (MAC-адрес)**) всех клиентов сети, пользующихся данным сервером DHCP.

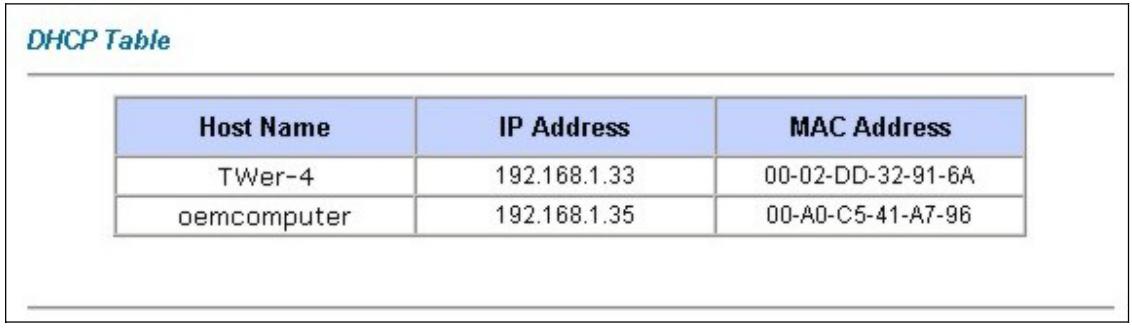


Рис. 21-3 Таблица DHCP

В следующей таблице приведены описания полей данного экрана.

Табл. 21-3 Таблица DHCP

ПОЛЕ	ОПИСАНИЕ

Табл. 21-3 Таблица DHCP

ПОЛЕ	ОПИСАНИЕ
Host Name	Имя хост-компьютера.
IP Address	IP-адрес, соответствующий значению поля **Host Name (Имя хоста)**.
MAC Address	В этом поле отображается MAC-адрес компьютера, соответствующий имени хоста. Каждое устройство Ethernet имеет свой уникальный MAC-адрес. MAC-адрес присваивается устройству изготовителем и состоит из шести пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02.

21.4 Экраны беспроводных LAN

На этих экранах отображается информация (только для чтения) о беспроводной локальной сети устройства OMNI ADSL.

21.4.1 Список соединений

На этом экране отображается MAC-адрес (-а) клиентов беспроводной LAN, зарегистрированных в настоящее время в сети. Щелкните по **Wireless LAN (Беспроводная LAN)**, а затем по **Association List (Список соединений)** для вызова следующего экрана.

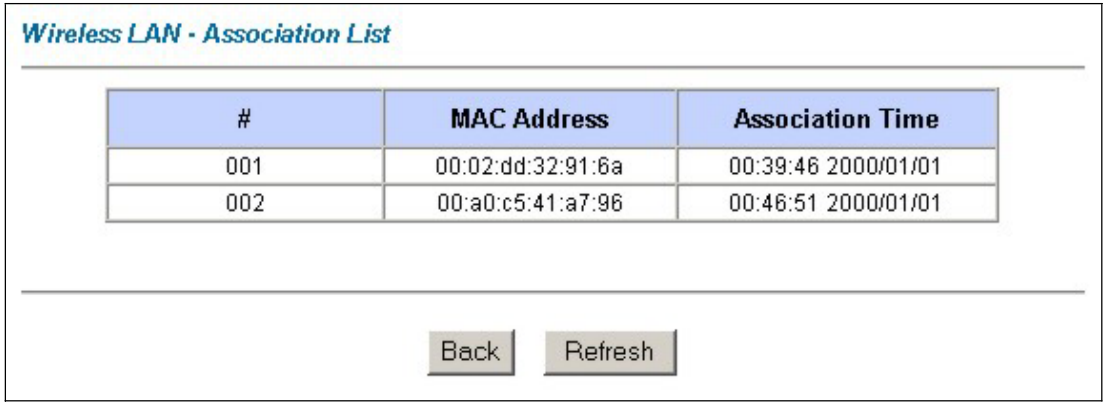


Рис. 21-4 Список соединений

В следующей таблице приведены описания полей данного экрана.

Табл. 21-4 Список соединений

ПОЛЕ	ОПИСАНИЕ
#	Порядковый номер подключенного клиента беспроводной LAN.
MAC Address	В этом поле отображается MAC-адрес подключенной беспроводной станции. Каждое устройство Ethernet имеет свой уникальный MAC-адрес. MAC-адрес присваивается устройству изготовителем и состоит из шести пар шестнадцатиричных символов, например, 00:A0:C5:00:00:02.
Association Time	В этом поле отображается продолжительность подключения беспроводной станции к устройству OMNI ADSL.
Back	Щелкните **Back** для перехода к главному экрану **Wireless LAN (Беспроводная LAN)**.
Refresh	Щелкните **Refresh (Обновить)** для обновления информации в таблице.

21.4.2 Таблица использования канала

На этом экране отображается состояние каналов в рабочем диапазоне устройства OMNI ADSL. Щелкните по **Wireless LAN (Беспроводная LAN)**, а затем по **Channel Usage Table (Таблица использования каналов)** для вызова следующего экрана.

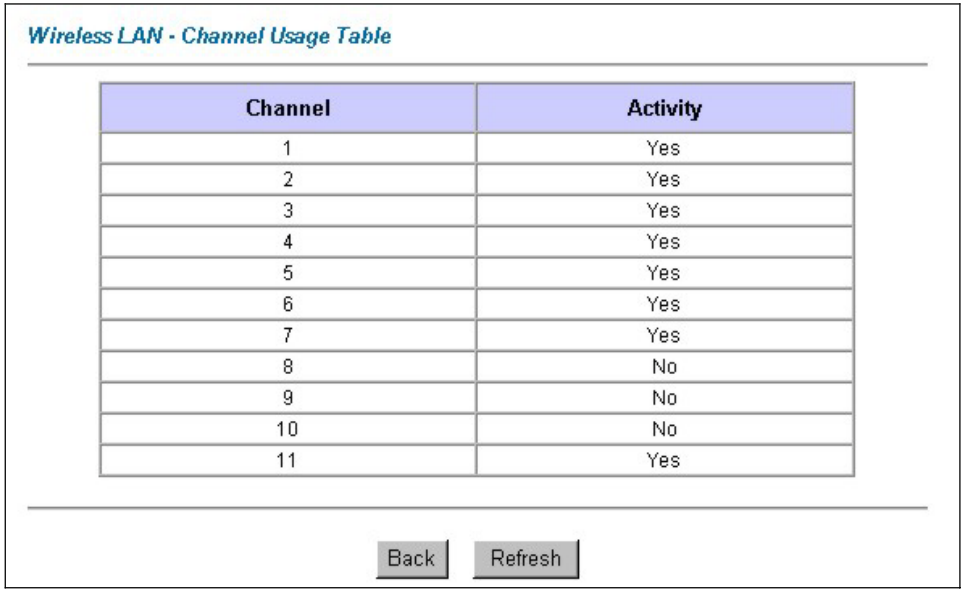


Рис. 21-5 Channel Usage Table (Таблица использования каналов)

В следующей таблице приведены описания полей данного экрана.

Табл. 21-5 Таблица использования каналов

ПОЛЕ	ОПИСАНИЕ
Channel	Порядковый номер канала.
IP Address	В этом поле отображается **Yes** , если канал (в рабочем диапазоне устройства OMNI ADSL) используется другой точкой доступа или специальной сетью.
Back (Назад)	Щелкните по **Back (Назад)** для перехода к главному экрану **Wireless LAN (Беспроводная LAN)**.
Refresh (Обновить)	Щелкните по **Refresh (Обновить)** для обновления информации в таблице.

21.5 Диагностические экраны

На этих экранах отображается информация (только для чтения), которая должна помочь в идентификации проблем устройства OMNI ADSL.

Щелкните по **Diagnostic (Диагностика)** для вызова следующего экрана.

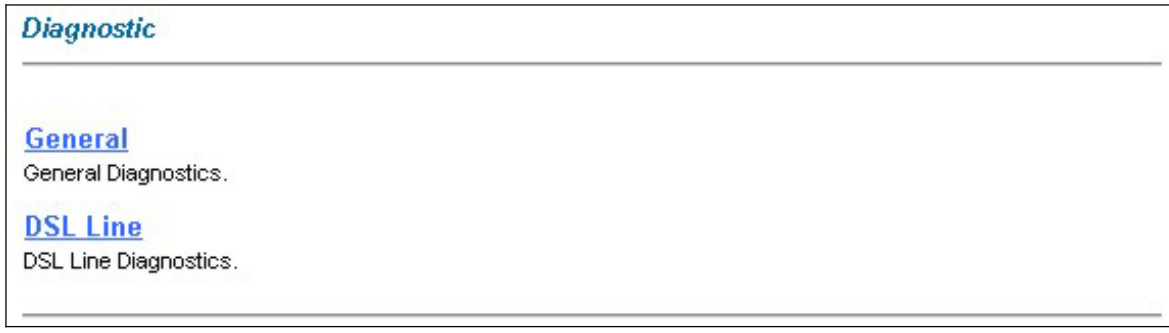


Рис. 21-6 Диагностика

21.5.1 Экран общей диагностики

Щелкните по **Diagnostic (Диагностика)**, а затем по **General (Общая)** для вызова следующего экрана.

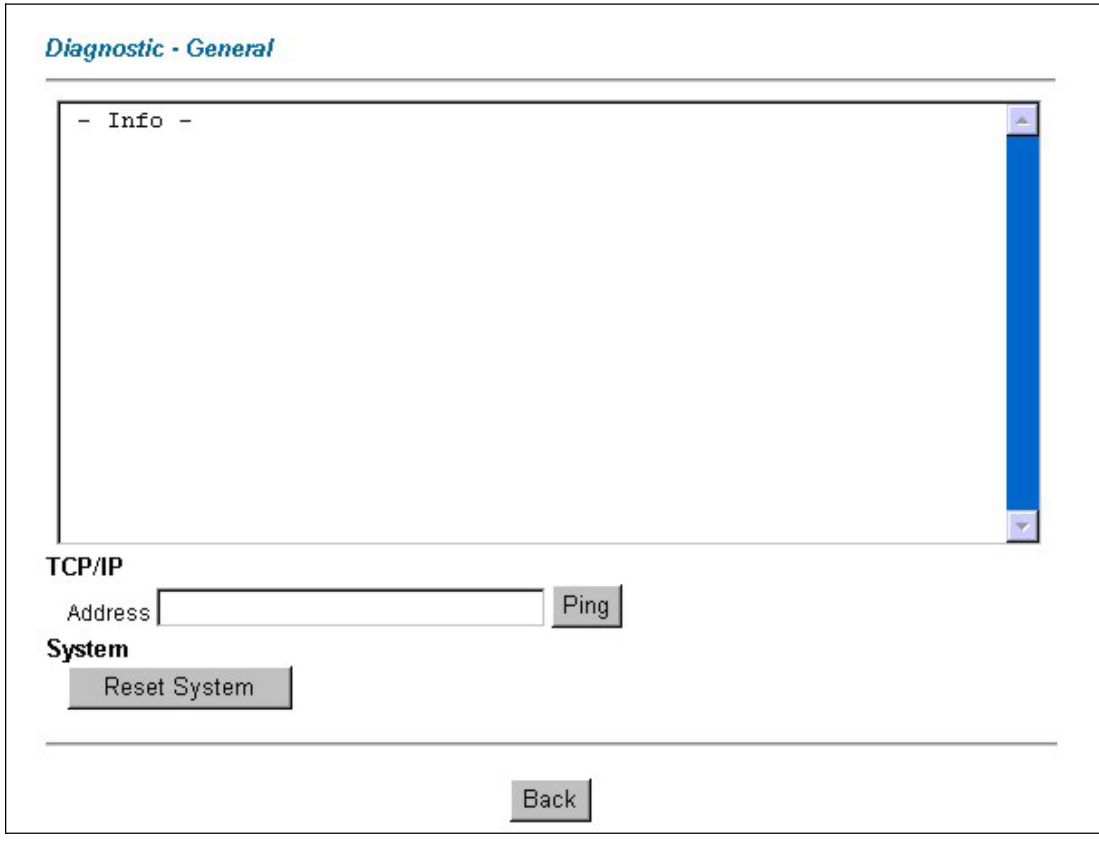


Рис. 21-7 Общая диагностика

В следующей таблице приведены описания полей данного экрана.

Табл. 21-6 Общая диагностика

ПОЛЕ	ОПИСАНИЕ
TCP/IP Address	Введите значение IP-адреса компьютера, соединение с которым нужно проверить эхо-тестированием.
Ping	Щелкните по этой кнопке для выполнения эхо-тестирования заданного IP-адреса.

Табл. 21-6 Общая диагностика

ПОЛЕ	ОПИСАНИЕ
Reset System	Щелкните по этой кнопке для перезагрузки OMNI ADSL. Появится предупреждающее диалоговое окно с запросом подтверждения решения перезагрузить систему. Щелкните **OK** для продолжения.
Back (Назад)	Щелкните по этой кнопке для возврата к главному экрану **Diagnostic (Диагностика)**.

21.5.2 Экран диагностики линии DSL

Щелкните по **Diagnostic (Диагностика)**, а затем по **DSL Line (Линия DSL)** для вызова следующего экрана.

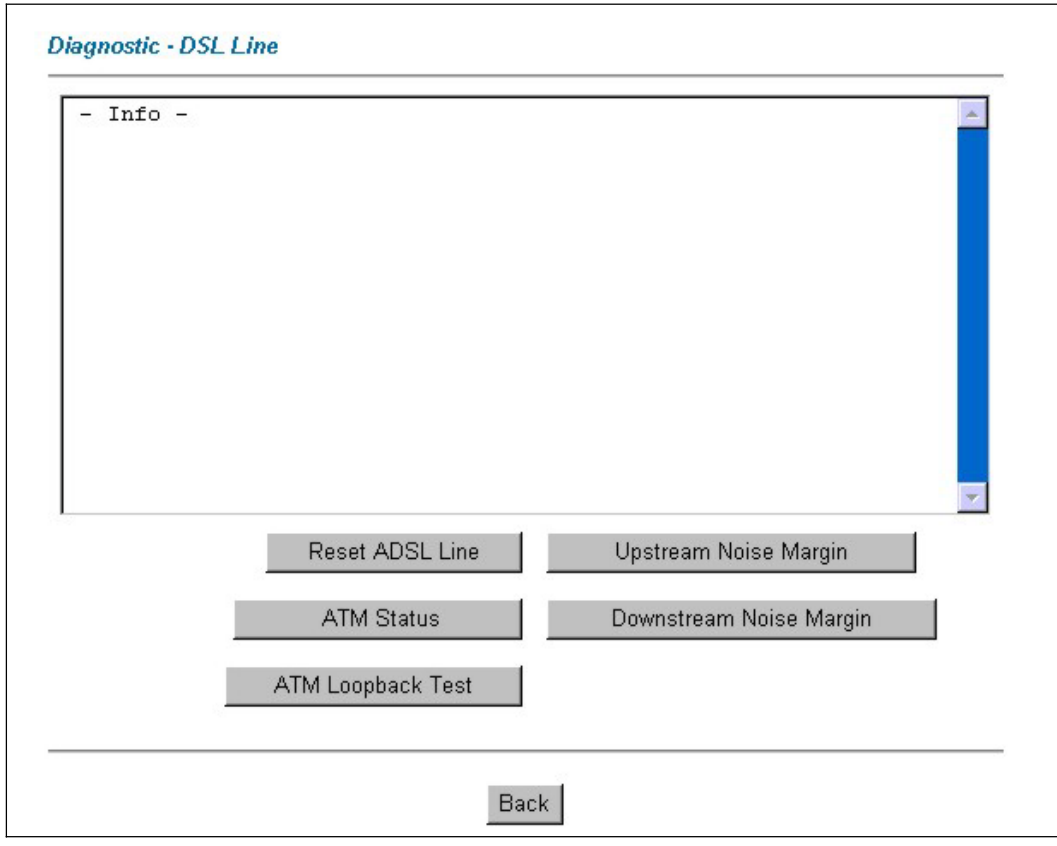


Рис. 21-8 Диагностика линии DSL

В следующей таблице приведены описания полей данного экрана.

Табл. 21-7 Диагностика линии DSL

ПОЛЕ	ОПИСАНИЕ
Reset ADSL Line	Щелкните по этой кнопке для повторного подключения линии ADSL. В большом текстовом окне над ней будут отображаться сведения о ходе и результатах этой операции, например: "Start to reset ADSL (Пуск повторного подключения ADSL) Loading ADSL modem F/W (Загрузка микропрограммного обеспечения модема ADSL)... Reset ADSL Line Successfully! ("Линия ADSL успешно подключена!")
ATM Status	Щелкните по этой кнопке для отображения сведений о статусе ATM (асинхронного режима передачи).
ATM Loopback Test	Щелкните по этой кнопке для проверки ATM тестом "петля". Перед выполнением этого теста убедитесь, что выполнена конфигурация, по крайней мере, одного постоянного виртуального канала (PVC) с соответствующими идентификаторами виртуального пути и канала (VPIs/VCIs). OMNI ADSL осуществляет отправку пакета OAM F5 в адрес коммутатора DSLAM/ATM с обратной ретрансляцией ("петлей") в адрес устройства OMNI ADSL. Проверка ATM с помощью теста "петля" полезна для поиска и устранения неисправностей в сетях DSLAM и ATM.
Upstream Noise Margin	Щелкните по этой кнопке с целью отображения предела помехоустойчивости для входящего потока данных.
Downstream Noise Margin	Щелкните по этой кнопке с целью отображения предела помехоустойчивости для исходящего потока данных.
Back	Щелкните по этой кнопке для возврата к главному экрану **Diagnostic (Диагностика)**.

21.6 Экран микропрограммного обеспечения

Найдите микропрограммное обеспечение на сайте www.zyxel.com в файле, в имени которого (обычно) используется наименование модели системы с расширением "*.bin", например, "OMNI ADSL.bin". Процесс загрузки осуществляется с использованием протокола HTTP (протокола передачи гипертекста) и может занять до двух минут. После успешной загрузки систему следует перезагрузить. См. главы *Микропрограммное обеспечение и Файл конфигурации сопровождения* в

разделах, где дается описание работы системной консоли для обновления микропрограммного обеспечения с использованием команд FTP/TFTP .

Пользуйтесь только микропрограммным обеспечением, предназначенным именно для Вашей модели устройства OMNI ADSL. См. предупреждающие наклейки в нижней части устройства OMNI ADSL.

Щелкните по **Firmware (Микропрограммное обеспечение)** для вызова следующего экрана. Следуйте инструкциям на экране для загрузки микропрограммного обеспечения для Вашей модели устройства OMNI ADSL.

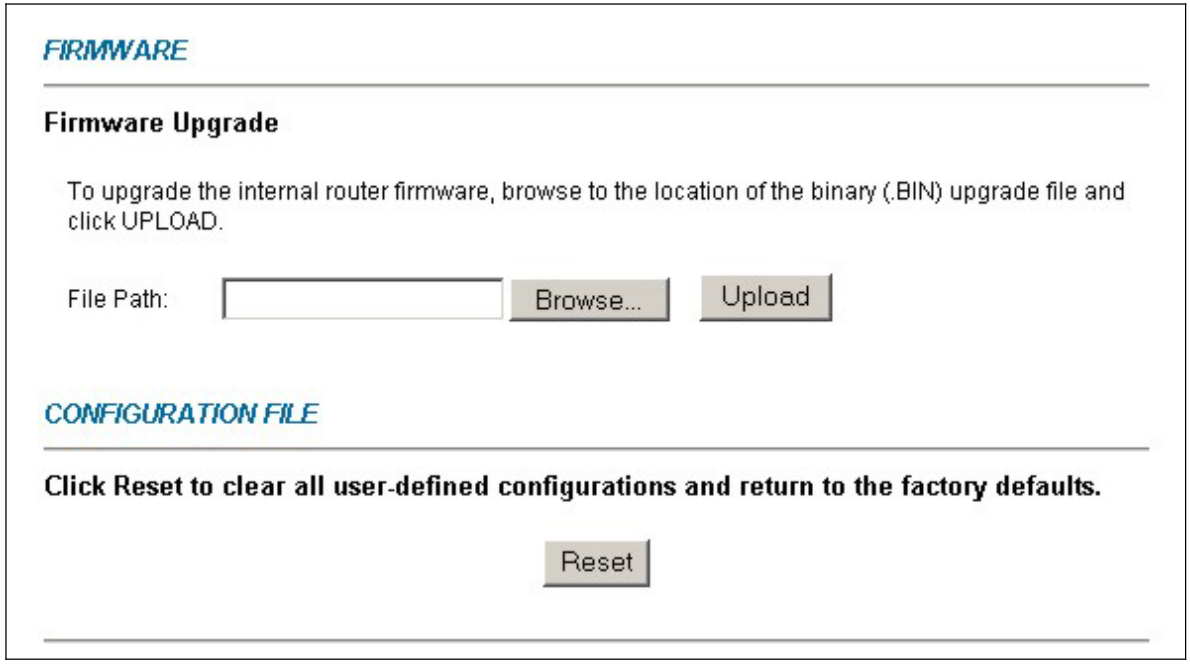


Рис. 21-9 Обновление микропрограммного обеспечения

В следующей таблице приведены описания полей данного экрана.

Табл. 21-8 Обновление микропрограммного обеспечения

ПОЛЕ	ОПИСАНИЕ
File Path	Введите в этом поле сведения о местоположении файла, который нужно загрузить, или щелкните **Browse... (Обзор...)** для его отыскания.

Табл. 21-8 Обновление микропрограммного обеспечения

ПОЛЕ	ОПИСАНИЕ
Browse... (Обзор...)	Щелкните **Browse... (Обзор...)** для поиска файла с расширением имени .bin, который нужно загрузить. Помните, что zip-файлы перед их загрузкой необходимо разархивировать.
Upload	Щелкните **Upload (Загрузка)** для запуска процесса загрузки. Операция может продолжаться до двух минут.
Reset	Щелкните по этой кнопке для удаления введенной пользователем информации о конфигурации и восстановлении настроек устройства OMNI ADSL, заданных изготовителем по умолчанию. См. раздел *Восстановление настроек устройства OMNI ADSL*.

Не выключайте OMNI ADSL во время загрузки микропрограммного обеспечения!

После появления экрана **Firmware Upload in Process (Идет загрузка микропрограммного обеспечения)** , подождите две минуты перед повторной загрузкой OMNI ADSL.

OMNI ADSL в это время автоматически перезапустится, что вызовет временное отключение от сети. При этом в некоторых операционных системах, можно увидеть на рабочем столе следующую иконку.

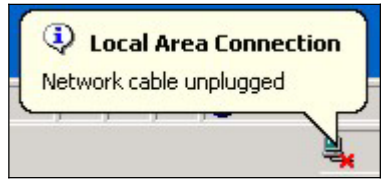


Рис. 21-10 Временное отключение от сети

Через две минуты повторите загрузку и проверьте новую версию микропрограммного обеспечения по экрану **System Status (Экран состояния системы)**.

Если загрузка оказалась неудачной, появится следующий экран. Щелкните **Back** для возврата к экрану **Firmware (Микропрограммное обеспечение)**.

Рис. 21-11 Сообщение об ошибке

Part IX:

Общая настройка системной консоли

В этой части приводится описание конфигурации системной консоли (SMT) для общей настройки маршрутизатора, настройки LAN, настройки беспроводной LAN, доступа в Интернет, удаленных узлов, удаленных узлов TCP/IP, статической маршрутизации и трансляции сетевых адресов (NAT).

См. разделы данного руководства, посвященные описанию Web-конфигуратора, содержащие необходимую информацию о технических параметрах, задаваемых с его помощью и с помощью системной консоли.

Chapter 22
Знакомство с системной консолью

В этой главе объясняется доступ к системной консоли и работа на ней, дается описание ее меню.

22.1 Введение к SMT

Системная консоль OMNI ADSL - SMT (System Management Terminal) является интерфейсом, управляемым из меню, доступ к которому осуществляется из терминального эмулятора через консольный порт или через Telnet-соединение.

22.1.1 Процедура настройки SMT через консольный порт

Выполните следующие действия для доступа к устройству OMNI ADSL через консольный порт.

Выполните настройку коммуникационной программы эмуляции терминала следующим образом: эмуляция терминала VT100, без контроля четности, 8 бит данных, 1 стоп-бит, установка потока данных - "none", скорость порта 9600 бит/с.

Нажмите [ENTER] (Ввод) для вызова экрана ввода пароля - SMT password screen. По умолчанию установлен пароль 1234.

22.1.2 Процедура настройки SMT через Telnet

Ниже описан порядок подключения к OMNI ADSL через Telnet.

Step 1. Загрузите Windows, щелкнете по **Start** (как правило, в левом нижнем углу), **Run**, а затем наберите "telnet 192.168.1.1" (IP-адрес по умолчанию) и щелкните **OK**.

Step 2. В поле **Password (Пароль)** введите “1234”.

Step 3. После ввода пароля можно будет увидеть главное меню.

Следует отметить, что если в течение пяти минут (время ожидания, заданное по умолчанию) после регистрации ничего не будет введено, OMNI ADSL автоматически отменит регистрацию и очистит экран. Тогда Вам придется заново подключаться к OMNI ADSL через Telnet.

22.1.3 Ввод пароля

После нажатия клавиши [ENTER] появляется экран регистрации и предлагает ввести пароль, как показано ниже.

При первой регистрации следует ввести пароль по умолчанию "1234". При вводе пароля набираемые символы на экране отображаются как символы "*".

Если в течение пяти минут после регистрации ничего не будет введено, OMNI ADSL автоматически отменит регистрацию и очистит экран.

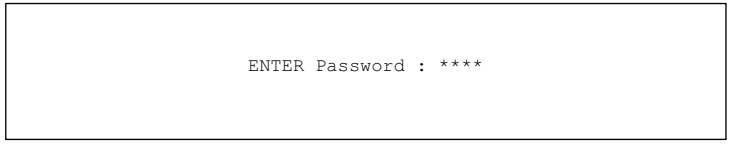


Рис. 22-1 Экран регистрации

22.1.4 Обзор меню SMT OMNI ADSL

В качестве примера в данном руководстве используется меню SMT модели OMNI ADSL LAN H/HW-31. Меню в различных моделях OMNI ADSL SMT отличаются незначительно.

На следующем рисунке представлено описание различных экранных форм, содержащих меню SMT OMNI ADSL.

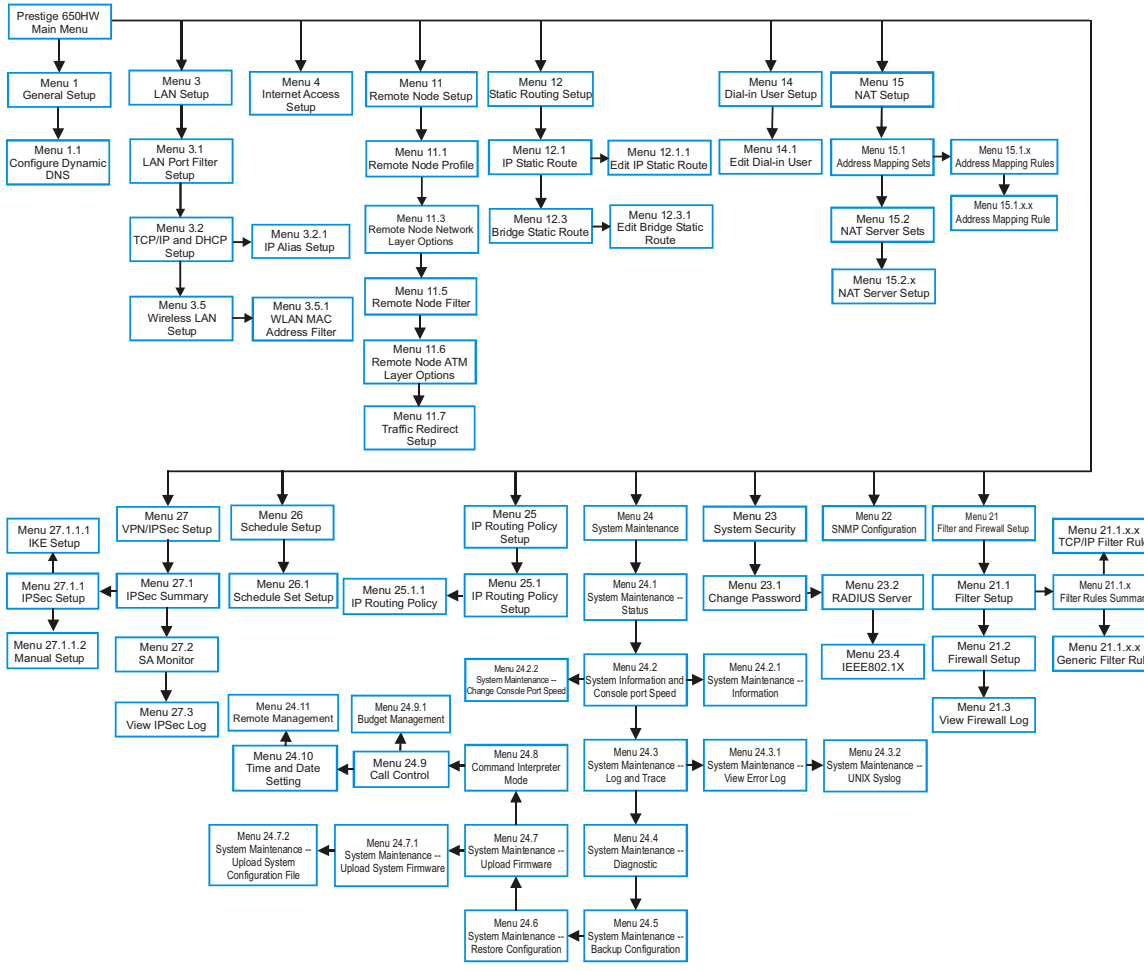


Рис. 22-2 Описание меню SMT OMNI ADSL P650H/HW-31

22.2 Работа с интерфейсом SMT

Интерфейс SMT (System Management Terminal) предназначен для конфигурирования OMNI ADSL.

Прежде, чем приступать к конфигурированию, следует ознакомиться с базовыми командами, приведенными в следующей таблице.

Табл. 22-1 Команды главного меню

ОПЕРАЦИЯ	КЛАВИША	ОПИСАНИЕ
Переход к другому меню	[ENTER]	Для перехода к нужному подменю введите его номер и нажмите клавишу [ENTER].
Возврат к предыдущему меню	[ESC]	Для возврата к предыдущему меню нажмите клавишу [ESC].
Переход к "скрытому" меню	Нажмите клавишу [SPACE BAR] (Пробел) для изменения **No** на **Yes**, а затем нажмите клавишу [ENTER].	Поля, начинающиеся с "Edit", ведут к скрытым меню и имеют настройку по умолчанию **No**. Нажмите [SPACE BAR] для изменения **No** на **Yes**, а затем нажмите клавишу [ENTER] для перехода к скрытому меню.
Перемещение курсора	Клавиша [ENTER] или клавиши со стрелками "вверх/вниз".	Находясь в меню, для перехода к следующему полю нажмите клавишу [ENTER]. Для перемещения по полям можно пользоваться клавишами со стрелками "вверх/вниз".
Ввод информации	Введите информацию или нажмите клавишу [SPACE BAR], а затем нажмите клавишу [ENTER].	Имеется два типа заполняемых полей. В поле первого типа вводится требуемая информация. Поля второго типа предназначены для просмотра списков выбора с помощью клавиши пробела.
Обязательные поля	<? > или **ChangeMe**	Все поля, содержащие символ <?> подлежат обязательному заполнению. В противном случае новая конфигурация не будет сохранена. Все поля, содержащие **ChangeMe**, не должны быть оставлены незаполненными, для того чтобы можно было сохранить новую конфигурацию.
Поля N/A	<N/A>	Некоторые поля могут содержать символ <N/A>. Это означает, что данная опция недоступна.

Табл. 22-1 Команды главного меню

Сохранение конфигурации	[ENTER]	При появлении сообщения "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации. После сохранения данных, как правило, происходит возврат к предыдущему меню.
Выход из SMT	Введите 99 и нажмите клавишу [ENTER].	Для завершения работы с SMT при появлении сообщения Главного меню введите 99 и нажмите клавишу [ENTER].

После ввода пароля SMT выводит на экран главное меню, показанное ниже.

```
            Copyright (c) 1994 - 2003 ZyXEL Communications Corp.

                          OMNI ADSL LAN H/HW-31 Main Menu

  Getting Started                       Advanced Management
    1. General Setup                      21. Filter and Firewall Setup
    3. LAN Setup                          22. SNMP Configuration
    4. Internet Access Setup              23. System Security
                                          24. System Maintenance
  Advanced Applications                   25. IP Routing Policy Setup
    11. Remote Node Setup                 26. Schedule Setup
    12. Static Routing Setup              27. VPN/IPSec Setup
    14. Dial-in User Setup
    15. NAT Setup                         99. Exit



                          ENTER Menu Selection Number:
```

Рис. 22-3 Главное меню SMT для P650H/HW-31

22.2.1 Сводка функций интерфейса SMT

Табл. 22-2 Краткий обзор главного меню для P650H/HW-31

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
1	General Setup (Настройка общих параметров)	Это меню используется для настройки общих параметров.
3	LAN Setup (Настройка локальной сети)	Это меню используется для настройки общих параметров беспроводной LAN (только в OMNI ADSL LAN H/HW) и LAN-соединения.
4	Internet Access Setup (Настройка доступа в Интернет)	Простая и быстрая настройка подключения к Интернету.

Табл. 22-2 Краткий обзор главного меню для P650H/HW-31

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
11	Remote Node Setup (Настройка удаленного узла)	Используется при настройке удаленного узла для соединения локальных сетей, включая соединение с Интернетом.
12	Static Routing Setup (Настройка статических маршрутов)	Данное меню используется для настройки статических маршрутов.
14	Dial-in User Setup (Настройка удаленного коммутируемого пользователя)	Это меню используется для установки настроек пользователя в OMNI ADSL LAN H/HW.
15	NAT Setup (Настройка NAT)	Данное меню используется для определения внутренних серверов, когда функция NAT включена.
21	Filter and Firewall Setup (Настройка фильтров и функций межсетевого экрана)	Настройте фильтры, включите/отключите межсетевой экран и просмотрите журнал межсетевого экрана (только в OMNI ADSL LAN H/HW).
22	SNMP Configuration (Конфигурирование SNMP)	Данное меню используется для настройки параметров, относящихся к SNMP
23	System Security (Защитные функции системы)	Это меню используется для настройки параметров безопасности беспроводных соединений (только в OMNI ADSL LAN H/HW) и изменения пароля.
24	System Maintenance (Сопровождение системы)	Данное меню содержит системный статус, диагностическую информацию, данные о загрузке программного обеспечения и т. д.
25	IP Routing Policy Setup (Настройка стратегии маршрутизации IP)	Используется для конфигурирования стратегии маршрутизации IP.
26	Schedule Setup (Составление плана)	Составление расписания исходящих вызовов.
27	VPN/IPSec Setup (Настройка VPN/IPSec)	Используйте данное меню для настройки VPN-соединений OMNI ADSL LAN H/HW.
99	Exit (Выход)	Используется для выхода из SMT и возврата к чистому экрану.

22.3 Изменение системного пароля

Для изменения пароля устройства OMNI ADSL, заданного по умолчанию, выполните следующие действия.

Step 1. Введите 23 в Главном меню для вызова Меню **23 - Защитные функции системы**.

Step 2. Введите 1 для вызова **Меню 23.1 - Защитные функции системы - Изменить пароль** , показанного ниже.

Step 3. Введите существующий системный пароль в поле **Old Password (Старый пароль)**, например - “1234”, и нажмите [ENTER].

```
         Меню 23.1 - "Защитные функции системы - Изменение
пароля"

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

Рис. 22-4 Меню 23 - Системный пароль

Step 4. Введите новый системный пароль (до 30 символов) в поле **New Password (Новый пароль)** и нажмите [ENTER].

Step 5. Введите новый системный пароль еще раз в поле **Retype to confirm (Повторный ввод для подтверждения)** и нажмите [ENTER].

Заметим, что при вводе пароля его символы отображаются в виде символов "*".

Chapter 23
Настройка общих параметров

Меню 1 - Настройка общих параметров *содержит административную информацию и системные данные.*

23.1 Настройка общих параметров

Меню 1 - Настройка общих параметров содержит административную и общесистемную информацию (показано ниже). Поле **System Name** используется только для идентификации, однако, поскольку некоторые Интернет-провайдеры выполняют проверку этого имени, сюда следует ввести "Имя компьютера" - "Computer Name".

- В Windows 95/98 щелкните по **Start (Пуск)**, **Settings (Настройки)**, **Control Panel (Панель управления)**, **Network (Сеть)**. Щелкните по закладке **Identification**, запишите имя, указанное в поле **Computer Name** и введите его в поле **System Name** модема OMNI ADSL.
- В Windows 2000 щелкните по **Start (Пуск)**, **Settings (Настройки)**, **Control Panel (Панель управления)**, а затем дважды щелкните по **System (Система)**. Щелкните по закладке **Network Identification** (Идентификация сети), а затем по кнопке **Properties** (Свойства). Запишите имя, указанное в поле **Computer Name** (Имя компьютера) и введите его в поле **System Name** (Системное имя) модема OMNI ADSL.
- В Windows XP, щелкните по **Start (Пуск)**, **My Computer (Мой компьютер)**, **View system information (Отображение сведений о системе)**, а затем щелкните по закладке **Computer Name (Имя компьютера)**. Запишите имя, указанное в поле **Full Computer Name**, и введите его в поле **System Name** модема OMNI ADSL.

Запись **Domain Name (Имя домена)** сообщается клиентам DHCP локальной сети. Если имя домена не будет указано, то будет использоваться имя домена, полученное с помощью DHCP от Интернет-провайдера. В то время как имя хоста (System Name) необходимо вводить на каждом компьютере, имя домена может быть присвоено устройством OMNI ADSL с помощью DHCP.

23.2 Настройка меню 1

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

```
                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:
```

Рис. 23-1 Меню 1 - Настройка общих параметров

Необходимо заполнить обязательные поля. См. приведенную ниже таблицу для получения дополнительной информации об этих полях.

Табл. 23-1 Меню 1 - Настройка общих параметров

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
System Name (Системное имя)	В целях идентификации введите идентифицирующее имя. Оно может состоять из 30 алфавитно-цифровых символов. В имени запрещается использование пробелов, но разрешено использование тире “-” и подчеркивания “_”.	
Location (optional) (Местоположение (дополнительно))	Введите местонахождение OMNI ADSL (до 31 символа).	MyHouse
Contact Person's Name (optional) (Имя ответственного лица (не обязательно))	Введите имя ответственного за OMNI ADSL лица (до 30 символов).	JohnDoe
Domain Name (Имя домена)	Введите имя домена, если оно известно. Если это поле останется незаполненным, Интернет-провайдер может назначить доменное имя с помощью DHCP. Следует перейти в меню 24.8 и ввести "sys domainname", чтобы увидеть текущее доменное имя, которым пользуется шлюз. Для удаления содержимого этого поля просто нажмите [SPACE BAR]. Имя домена, введенное Вами, имеет приоритет над именем домена, назначенным Интернет-провайдером.	zyxel.com.tw
Edit Dynamic DNS (Изменить конфигурирование динамического DNS)	Нажмите клавишу [SPACE BAR] для выбора **Yes** или **No** (по умолчанию). Выберите **Yes** для настройки **Меню 1.1 — Конфигурирование динамического DNS** (обсуждается далее).	**No**

Табл. 23-1 Меню 1 - Настройка общих параметров

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Route IP (Маршрутизация IP)	Установите в этом поле **Yes** для включения или **No** - для отключения функции маршрутизации IP. Можно включить функцию маршрутизации IP для доступа в сеть Интернет.	**Yes**
Bridge (Мост)	Включение/Отключение межсетевого моста для не поддерживаемых устройством протоколов (например, SNA) или не заданных для включения в предыдущем поле **Route IP (Маршрут IP)**. Выберите **Yes** для включения функции межсетевого моста; выберите **No** для ее отключения.	**No**

23.2.1 Конфигурирование динамического DNS

Если Вы используете частный IP-адрес глобальной сети, использование динамического DNS невозможно.

Для конфигурирования динамического DNS перейдите в **Меню 1 — Настройка общих параметров** и выберите **Yes** в поле **Edit Dynamic DNS (Редактирование динамического DNS)**. После нажатия [ENTER] на экране появится **Меню 1.1— Конфигурирование динамического DNS**, показанное ниже.

```
                    Menu 1.1 - Configure Dynamic DNS

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

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

Рис. 23-2 Меню 1.1 - Конфигурирование динамического DNS

Инструкции по конфигурированию параметров динамического DNS даны в приведенной ниже таблице.

Табл. 23-2 Меню 1.1 - Конфигурирование динамического DNS

ПОЛЕ	ОПИСАНИЕ	Пример
Service Provider (Провайдер услуг)	Имя Вашего провайдера услуг динамических DNS.	WWW.DynDNS.ORG (по умолчанию)

Табл. 23-2 Меню 1.1 - Конфигурирование динамического DNS

ПОЛЕ	ОПИСАНИЕ	Пример
Active (Активно)	Выберите **Yes** нажатием клавиши [SPACE BAR], а затем активизируйте динамический DNS нажатием клавиши [ENTER].	**Yes**
Host (Хост)	Введите имя домена, присвоенное устройству OMNI ADSL провайдером динамического DNS.	me.dyndns.org
EMAIL (Адрес электронной почты)	Введите адрес Вашей электронной почты.	mail@mailserver
USER (ПОЛЬЗОВАТЕЛЬ)	Введите имя пользователя.	
Password	Введите выданный вам пароль.	
Enable (Разрешить групповой символ) Wildcard	OMNI ADSL поддерживает DYNDNS Wildcard. Нажмите [SPACE BAR], а затем [ENTER] для выбора **Yes** или **No.** Это поле недоступно (**N/A**), если Вы выбрали в качестве провайдера услуг клиент DDNS.	**No**
По завершении работы в Меню при появлении сообщения "Press ENTER to Confirm…" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены.		

Chapter 24
Настройка локальной сети

В этой главе рассказывается о том, как выполнить конфигурирование настроек Вашей локальной сети.

24.1 Настройка локальной сети

В этом разделе описывается выполнение конфигурирования сети Ethernet с использованием **Меню 3** — **Настройки локальной сети**. Введите 3 в Главном меню для вызова Меню 3.

```
                    Menu 3 - LAN Setup


              1. LAN Port Filter Setup
              2. TCP/IP и DHCP Setup

              5. Wireless LAN Setup


                   ENTER Menu Selection Number:
```

Рис. 24-1 Меню 3 - Настройки локальной сети

24.1.1 Общая настройка Ethernet

Данное меню позволяет задать набор(-ы). фильтров, которые должны применяться к трафику Ethernet. Необходимость в фильтрации трафика Ethernet возникает редко; тем не менее, наборы фильтров могут быть полезными для блокировки отдельных пакетов, уменьшения объема трафика и предотвращения несанкционированного доступа.

```
                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:
```

Рис. 24-2 Меню 3.1 - Настройка фильтра порта локальной сети

Если нужно определить фильтры, тогда следует сначала обратиться к главе *Настройка набора фильтров*, а затем вернуться к данному меню, чтобы определить наборы фильтров.

24.2 Настройка Ethernet, зависящая от протокола

В зависимости от протоколов для прикладных задач необходимо сконфигурировать соответствующую настройку Ethernet, как описано ниже.

- Для настройки TCP/IP Ethernet см. главу *Организация доступа в Интернет*.
- Для настройки межсетевого моста для Ethernet см. главу *Настройка межсетевого моста*.

24.3 Настройка TCP/IP и DHCP для Ethernet

Конфигурирование OMNI ADSL для TCP/IP осуществляется в меню 3.2 .

Для редактирования меню 3.2 введите 3 в главном меню для перехода в **меню 3 - Настройка Ethernet**. После появления меню 3 нажмите 2, а затем нажмите [ENTER] для вызова **Меню 3.2 — Настройка TCP/IP и DHCP для Ethernet**, как показано ниже:

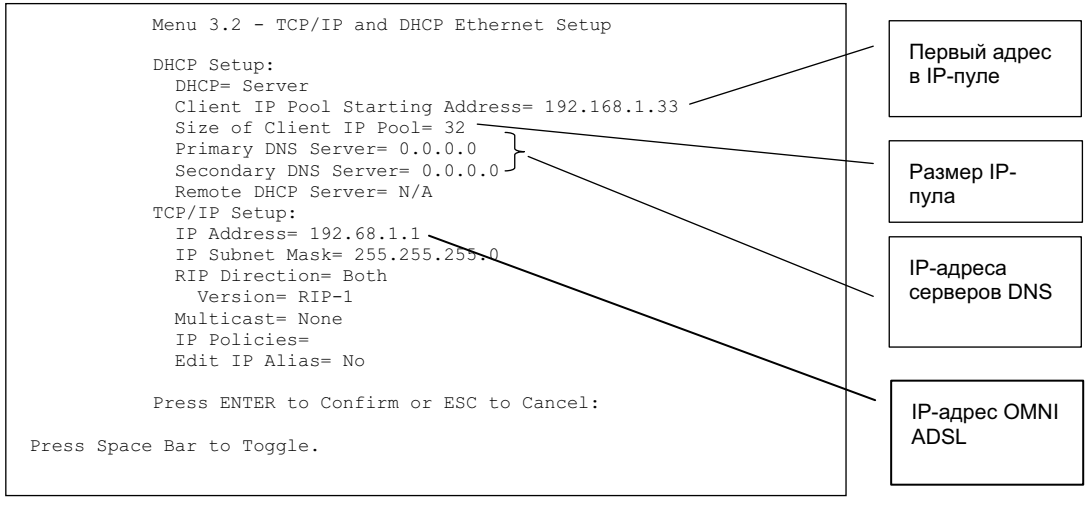


Рис. 24-3 Меню 3.2 Настройка TCP/IP и DHCP для Ethernet

Следуйте указаниям по конфигурированию DHCP, представленным в приведенной ниже таблице.

Табл. 24-1 Поля меню настроек DHCP для Ethernet

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
DHCP Setup (Настройка DHCP)		
DHCP	Если в данном поле установлено **Server**, то OMNI ADSL может назначать IP-адреса, IP-шлюз (по умолчанию) и адреса серверов DNS для Windows 95, Windows NT и других систем, поддерживающих клиентов DHCP. Если установлено **None**, функция сервера DHCP отключена. Если установлено **Relay (Ретранслятор)**, OMNI ADSL выступает в качестве фиктивного сервера DHCP и ретранслирует запросы и ответы DHCP между удаленным сервером и клиентами. В данном случае следует в поле Remote DHCP Server ввести IP-адрес действительного удаленного сервера DHCP. Если используется DHCP, необходимо задать следующие параметры:	**Server** (по умолчанию)
Client IP Pool Starting Address (Начальный адрес клиентского IP-пула)	В этом поле задается первый адрес из пула непрерывных IP-адресов.	192.168.1.33
Size of Client IP Pool (Размер клиентского IP-пула)	В этом поле задается размер или счетчик пула непрерывных IP-адресов.	32
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 DHSP)	Если в указанном выше поле **DHCP** установлено **Relay**, введите IP-адрес действительного удаленного сервера DHCP.	

При конфигурировании параметров TCP/IP для порта Ethernet следует воспользоваться приведенной ниже таблицей.

Табл. 24-2 Поля меню настройка TCP/IP для Ethernet

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
TCP/IP Setup (Настройка TCP/IP)		
IP Address (IP-адрес)	Введите IP-адрес (локальной сети) OMNI ADSL в десятичном виде с разделительными точками.	192.168.1.1
IP Subnet Mask (Маска подсети IP)	OMNI ADSL автоматически вычисляет маску подсети на основании назначенного IP-адреса. Пока не реализована структура подсетей, следует использовать маску подсети, вычисленную OMNI ADSL.	255.255.255.0
RIP Direction (Направление RIP)	Выберите направление RIP нажатием клавиши [SPACE BAR], а затем одну из следующих опций: **Both (Оба)**, **In Only (На прием)**, **Out Only (На передачу)** или **None**.	**Both** (по умолчанию)
Version (Версия)	Выберите версию RIP нажатием клавиши [SPACE BAR], а затем одну из следующих опций: **RIP-1**, **RIP-2B** или **RIP-2M**.	**RIP-1** (по умолчанию)
Multicast (Многоадресная рассылка)	IGMP (Internet Group Multicast Protocol - Протокол многоадресной рассылки) - это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. OMNI ADSL поддерживает как версию 1 IGMP (**IGMP-v1**), так и версию 2 (**IGMP-v2**). Нажмите [SPACE BAR] для включения многоадресной рассылки IP или выберите **None** для ее отключения.	**None** (по умолчанию)
IP Policies (Стратегии IP)	Создайте стратегии с помощью меню 25 (см. *главу Стратегия маршрутизации IP*) и примените их к интерфейсу ЛВС OMNI ADSL. Можно применить до четырех наборов стратегий IP (из двенадцати), введя их номера через запятую.	2,4,7,9
Edit IP Alias (Редактирование псевдонима IP)	OMNI ADSL поддерживает три логических интерфейса LAN через отдельный физический интерфейс Ethernet, при этом сам OMNI ADSL выступает в качестве шлюза для каждой сети ЛВС. Нажмите клавишу [SPACE BAR] для изменения **No** на **Yes** и нажмите клавишу [ENTER] для перехода в меню 3.2.1	**No** (по умолчанию)

Chapter 25
Настройка беспроводной LAN

В этой главе описывается, как сконфигурировать настройки беспроводной LAN в меню 3.5 системной консоли. Содержание данной главы относится только к моделям OMNI ADSL LAN H и OMNI ADSL LAN HW.

25.1 Описание беспроводных LAN

Для получения основных сведений о сетях этого типа см. главу об экранах беспроводной LAN .

25.2 Подключение сетевой радиокарты PCMCIA

Для использования дополнительной возможности работы в беспроводных сетях следует применять только сетевые радиокарты PCMCIA серии ZyAIR .

Step 1. Выключите OMNI ADSL.

Запрещается вставлять и вынимать сетевую радиокарту при включенном устройстве OMNI ADSL.

Step 2. Отыщите на устройстве OMNI ADSL слот с маркировкой **Wireless LAN** .

Step 3. Направьте контактный разъем сетевой радиокарты ZyAIR в сторону слота, так чтобы сторона со светодиодом была обращена вверх, и вставьте радиокарту в слот .

Вставляйте радиокарту в слот без нажима, не допуская изгибов и перекосов платы.

Step 4. Включите OMNI ADSL. Светодиод **WLAN** LED должен загореться.

25.3 Настройка беспроводной LAN

Для настройки OMNI ADSL как беспроводной точки доступа следует использовать меню 3.5. Для редактирования меню 3.5, введите 3 в главном меню для перехода в **Меню 3 – Настройка локальной сети**. После появления меню 3, нажмите 5, а затем клавишу [ENTER] для вызова **Меню 3.5 – Настройка беспроводной LAN** , как показано ниже.

```
   Menu 3.5- Wireless LAN Setup

ESSID= Wireless
Hide ESSIS = No
Channel ID= CH01 2412MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP= Disable
     Default Key= N/A
     Key1= N/A
     Key2= N/A
     Key3= N/A
     Key4= N/A
Edit MAC Address Filter= No

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

Рис. 25-1 Меню 3.5 - Настройка беспроводной LAN

Следующая таблица описывает поля данного меню.

Табл. 25-1 Описание полей настройки беспроводной LAN

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
ESSID (Расширенный идентификатор набора услуг)	ESSID (Extended Service Set IDentifier - Расширенный идентификатор набора услуг) идентифицирует набор услуг, к которым получает доступ беспроводная станция. Беспроводные станции, подключенные к одной точке доступа должны иметь одинаковый ESSID. Введите идентифицирующее имя (до 32 символов) для набора услуг беспроводной связи.	**Wireless (Беспроводной)**
Hide ESSID (Скрытый ESSID)	Нажмите [SPACE BAR] и укажите **Yes** для того чтобы скрыть ESSID в исходящем сигнальном кадре и исключения возможности получения ESSID какой-либо станцией путем пассивного сканирования.	**No**
Channel ID (Идентификатор канала)	Нажмите клавишу [SPACE BAR] для выбора канала, что позволит установить рабочую частоту/канал с учетом местоположения сети.	**CH01 2412MHz**

Табл. 25-1 Описание полей настройки беспроводной LAN

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
RTS Threshold (Допустимый размер RTS)	Допустимый размер сообщения RTS (количество байтов) для включения квитирования RTS/CTS. Данные с размером кадра больше этой величины будут передаваться квитированием RTS/CTS. Установка значения этого параметра больше максимальной величины MSDU (MAC service data unit) приведет к отключению квитирования RTS/CTS. Установка значения данного параметра равного нулю приведет к отключению квитирования RTS/CTS . Введите значение от 0 до 2432.	**2432**
Frag. Threshold (Допустимые размеры фрагментации)	Допустимые размеры (количество байтов) фрагментации передаваемых сообщений. Это максимальный размер фрагмента данных, который может быть отправлен. Введите значение от 256 до 2432.	**2432**
WEP (Протокол WEP)	Протокол WEP (Wired Equivalent Privacy - эквивалентно конфиденциальности проводных сетей) обеспечивает шифрование данных для предупреждения несанкционированного приема данных, передающихся в беспроводной сети. Выбор опции **Disable (Отключен)** позволяет беспроводной станции связаться с точкой доступа без шифрования данных. Выбор опции **64-битовый ключ WEP** или **128-битовый ключ WEP** определяет способ шифрования данных. Использование протокола WEP вызывает уменьшение производительности.	**Отключение**
Default Key (Значение ключа по умолчанию)	Введите число, соответствующе значению активного ключа.	

Табл. 25-1 Описание полей настройки беспроводной LAN

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Key 1 to Key 4 (Ключи 1-4)	Если выбрана опция **64-bit WEP (64-битовый ключ WEP)** в поле **WEP Encryption (Шифрование WEP)**, введите 5 символов или 10 шестнадцатиричных цифр ("0-9", "A-F") с символами 0x впереди для каждого ключа (1-4). Если выбрана опция **128-bit WEP (128-битовый ключ WEP)** в поле **WEP Encryption (Шифрование WEP)**, введите 13 символов или 26 шестнадцатиричных цифр ("0-9", "A-F") с символами 0x впереди для каждого ключа (1-4). Имеется четыре ключа шифрования данных для защиты данных от несанкционированного прослушивания пользователей беспроводной сети. Значения ключей должны быть установлены одинаковыми как для точки доступа, так и для компьютеров беспроводной станции.	
Edit MAC Address Filter (Редактирование MAC-адреса фильтра)	Для редактирования MAC-адреса нажмите клавишу [SPACE BAR] для выбора опции **Yes** и нажмите клавишу [ENTER] для вызова меню 3.5.1.	**No**
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

25.3.1 Фильтр MAC-адреса беспроводной LAN

Следующий уровень защиты обеспечивается фильтром MAC-адреса. Для разрешения подключения беспроводной станции к устройству OMNI ADSL, введите MAC-адрес сетевой радиокарты для данной беспроводной станции в таблице MAC-адресов.

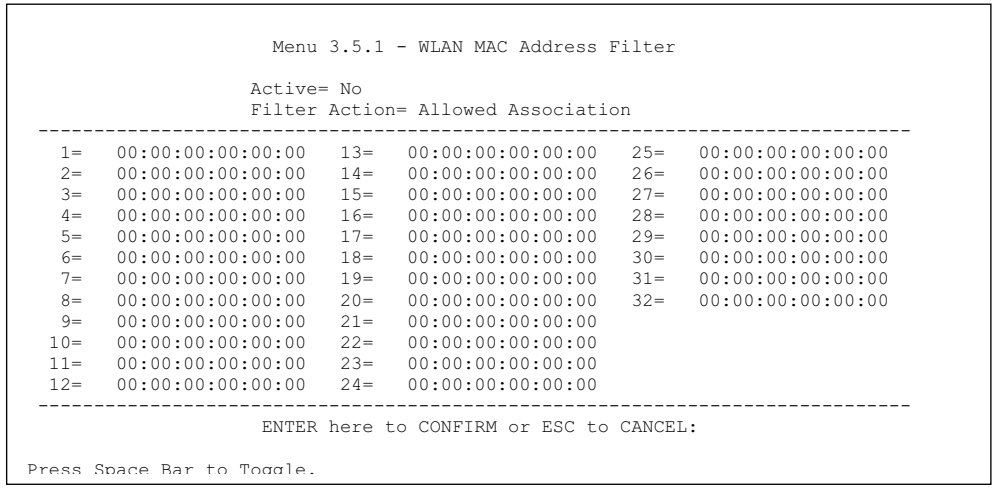


Рис. 25-2 Меню 3.5.1 фильтрации MAC-адресов WLAN

Следующая таблица описывает поля данного меню.

Табл. 25-2 Меню 3.5.1 фильтрации MAC-адресов WLAN

ПОЛЕ	ОПИСАНИЕ
Active	Для включения функции фильтрации MAC-адресов нажмите клавишу [SPACE BAR] для выбора опции **Yes** и нажмите клавишу [ENTER].
Filter Action	Выберите действие фильтра применительно к списку MAC-адресов в таблице фильтров MAC-адресов. Для установки запрета доступа к устройству OMNI ADSL нажмите клавишу [SPACE BAR] для выбора **Deny Association (Запрет подключения)** и нажмите клавишу [ENTER]. Для MAC-адресов, не включенных в список, доступ к маршрутизатору будет невозможен. По умолчанию действует опция **Allowed Association (Разрешенное соединение)**, разрешающая подключение к маршрутизатору OMNI ADSL. Для MAC-адресов не включенных в список доступ к маршрутизатору будет невозможен.
MAC Address Filter (Фильтр MAC-адреса)	
Address 1….	Введите в данные адресные поля значения MAC-адресов (в формате

Табл. 25-2 Меню 3.5.1 фильтрации MAC-адресов WLAN

ПОЛЕ	ОПИСАНИЕ
	XX:XX:XX:XX:XX:XX) радиостанций, которым разрешен или запрещен доступ к ресурсам устройства OMNI ADSL.
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.	

Chapter 26
Доступ в Интернет

В данной главе описывается конфигурирование интерфейсов локальной и глобальной сети в OMNI ADSL для доступа в сеть Интернет.

26.1 Описание доступа в сеть Интернет

См. главу с описанием работы мастер-программы Web-конфигуратора и экранов LAN и WAN для получения более подробной информации о полях системной консоли, рассматривающихся в настоящей главе.

26.2 IP Policies (Стратегии IP)

Как правило, маршрутизация основывается *только* на адресе назначения, поэтому маршрутизатор выбирает самый короткий путь для пересылки пакета. Маршрутизация на базе стратегии IP (IPPR) предоставляет возможность игнорировать схему маршрутизации, заданную по умолчанию, и изменить процесс пересылки пакета на базе стратегии, определенной сетевым администратором. Маршрутизация на базе стратегии применяется к входящим пакетам, рассылаемым по интерфейсу, и осуществляется перед обычной маршрутизацией. Стратегии следует создать в Меню 25 SMT (см. главу *Маршрутизация на базе стратегии IP*) и применить их к интерфейсам локальной и/или глобальной сети OMNI ADSL в Меню 3.2 (LAN) и 11.3 (WAN).

26.3 Псевдоним IP

Псевдоним IP позволяет разделить физическую сеть, созданную на основе одного интерфейса Ethernet, на несколько логических сетей. OMNI ADSL поддерживает три логических интерфейса LAN через один физический интерфейс Ethernet, при этом сам OMNI ADSL выступает в качестве шлюза для каждой сети LAN.

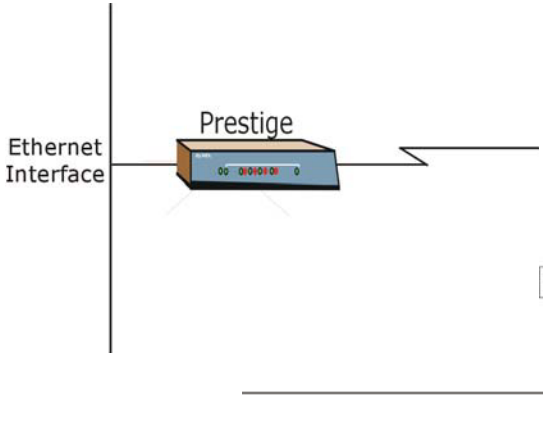


Рис. 26-1 Физическая сеть

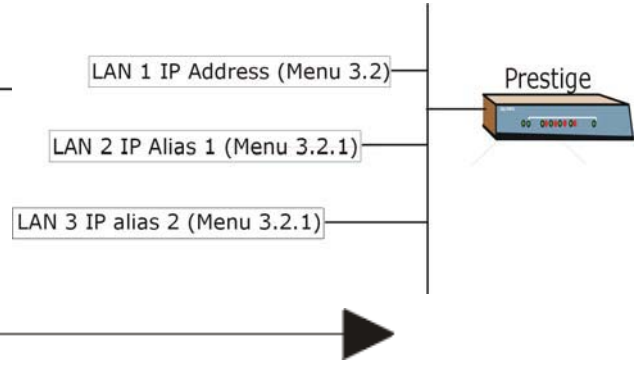


Рис. 26-2 Разделение на логические сети

Для конфигурирования псевдонима IP на OMNI ADSL используйте меню 3.2.1.

26.4 Настройка псевдонима IP

Сконфигурируйте первую сеть с помощью Меню 3.2. Установите курсор в поле **Edit IP Alias (Редактирование псевдонима IP)**, нажатием клавиши [SPACE BAR] **, выберите Yes и нажмите клавишу** [ENTER] для настройки второй и третьей сети.

```
                Menu 3.2 - Настройка TCP/IP и DHCP для Ethernet

               DHCP Setup:
                DHCP= Server
                Client IP Pool Starting Address= 192.168.1.33
                Size of Client IP Pool (размер клиентского IP-пула)= 32
                Primary DNS Server= 0.0.0.0
                Secondary DNS Server (Дополнительный сервер DNS)= 0.0.0.0
                Remote DHCP Server= N/A
               TCP/IP Setup (Настройка TCP/IP):
                  IP Address= 192.168.1.1
                  IP Subnet Mask (Маска подсети IP)= 255.255.255.0
                  RIP Direction= None
                    Version= N/A
                  Multicast= None
                  IP Policies=
                  Edit IP Alias= Yes

               Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Рис. 26-3 Меню 3.2 настройки TCP/IP и DHCP

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

```
                        Menu 3.2.1 - IP Alias Setup

                    IP Alias 1= No
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      RIP Direction= N/A
                      Version= N/A
                      Incoming protocol filters= N/A
                      Incoming protocol filters= N/A
                    IP Alias 2= No
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      RIP Direction= N/A
                      Version= N/A
                      Incoming protocol filters= N/A
                      Incoming protocol filters= N/A

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

Рис. 26-4 Меню 3.2.1 - Настройка псевдонима IP

В следующей таблице приведены указания по конфигурированию параметров псевдонима IP.

Табл. 26-1 Меню 3.2.1 - Настройка псевдонима IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
IP Alias (Псевдоним IP)	Выберите **Yes** для конфигурирования сети LAN в OMNI ADSL.	**Yes**
IP Address (IP-адрес)	Введите IP-адрес OMNI ADSL в десятичном виде с разделительными точками.	192.168.1.1
IP Subnet Mask (Маска подсети IP)	OMNI ADSL автоматически вычисляет маску подсети на основании назначенного IP-адреса. Пока не реализована структура подсетей, следует использовать маску подсети, вычисленную OMNI ADSL	255.255.255.0
RIP Direction (Направление RIP)	Выберите направление RIP нажатием клавиши [SPACE BAR] для задания одной из следующих опций:**None**, **Both (Оба)**, **In Only (Только прием)** или **Out Only (Только передача)**.	**None**
Version (Версия)	Выберите версию RIP нажатием клавиши [SPACE BAR], а затем одну из следующих опций: **RIP-1**, **RIP-2B** или **RIP-2M**.	**RIP-1**
Incoming Protocol Filters (Входные фильтры протоколов)	Введите набор(-ы) фильтров, которые должны применяться к входящему трафику между этим узлом и OMNI ADSL.	
Outgoing Protocol Filters (Исходящие фильтры протоколов)	Введите набор(-ы) фильтров, которые должны применяться к исходящему трафику между этим узлом и OMNI ADSL.	
По завершении работы в Меню при появлении сообщения "Press ENTER to Confirm…" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены.		

26.5 Настройка маршрутизации IP

Первым шагом является включение функции маршрутизации IP в **Меню 1 - Настройка общих параметров**.

Для редактирования Меню 1 введите 1 в Главном меню и нажмите клавишу [ENTER]. Установите нажатием клавиши [SPACE BAR] **Yes** в поле **Route IP** .

```
                    Menu 1 - General Setup

                System Name= P650HW
                Location= location
                Contact Person's Name=
                Domain Name=
                Edit Dynamic DNS= No

                Route IP= Yes
                Bridge= No

  Нажмите клавишу [ENTER] для подтверждения или клавишу [ESC] для отме
```

Рис. 26-5 Меню 1 - Настройка общих параметров

26.6 Конфигурирование доступа в Интернет

Меню 4 позволяет настроить все параметры доступа в Интернет в одной экранной форме. Фактически, меню 4 представляет собой упрощенную настройку для одного из четырех удаленных узлов, доступную через меню 11. Прежде, чем выполнять конфигурирование OMNI ADSL для доступа в Интернет, необходимо получить соответствующую информацию по подключению пользователя у Интернет-провайдера.
Для записи учетных данных следует пользоваться таблицей *Учетная информация для сети Интернет* в *Кратком руководстве/Ознакомительном курсе/Ускоренном вводном курсе*. В случае использования инкапсуляции PPPoA или PPPoE необходима только информация о регистрационном имени и пароле, предоставляемая Интернет-провайдером. Если используется инкапсуляция ENET ENCAP, необходимо знать только IP-адрес шлюза инкапсуляции Ethernet.

Находясь в Главном меню, введите 4 для вывода **Меню 4 – Настройка доступа в Интернет**, как показанного ниже.

```
                Menu 4 - Internet Access Setup

          ISP's Name= MyISP
          Encapsulation= ENET ENCAP
          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= Dynamic
            IP Address= N/A
          Network Address Translation (Трансляция сетевых адресов)= S
            Address Mapping Set= N/A

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

Рис. 26-6 Меню 4 - "Настройка доступа в Интернет"

В следующей таблице содержатся указания по конфигурированию OMNI ADSL для доступа в Интернет.

Табл. 26-2 Меню 4 - Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
ISP's Name (Имя Интернет-провайдера)	Введите имя Вашего Интернет-провайдера (Эта информация необходима только для идентификации).	MyISP
Encapsulation (Инкапсуляция)	Клавишей [SPACE BAR] **выберите метод** инкапсуляции, использующийся Вашим Интернет-провайдером, а именно: **PPPoE**, **PPPoA**, **RFC 1483** или **ENET ENCAP**.	ENET ENCAP
Multiplexing (Мультиплексирование)	Нажатием клавиши [SPACE BAR] выберите метод мультиплексирования, использующийся Вашим Интернет-провайдером, а именно: на базе **VC** или на базе **LLC**.	LLC
VPI # (Номер VPI)	Введите присвоенное значение идентификатора виртуального пути (VPI).	8
VCI # (Номер идентификатора виртуального канала)	Введите присвоенное значение идентификатора виртуального канала (VCI).	35
ATM QoS Type (Тип качества услуги ATM)	Нажатием клавиши [SPACE BAR] выберите значение **CBR** для указания фиксированной (постоянной) скорости передачи данных. Выберите значение **UBR** (неопределенной скорости передачи данных в битах) для приложений нечувствительных к временным ограничениям, таким как E-Mail. Выберите значение **VBR** (переменной скорости передачи) для пульсирующего трафика и при одновременном использовании полосы частот несколькими приложениями.	UBR
Peak Cell Rate (PCR) (Пиковая скорость ячеек (PCR))	Максимальная скорость, с которой отправитель может передавать ячейки. Введите пиковую скорость ячеек.	0
Sustain Cell Rate (Поддерживаемая скорость ячеек) (SCR)= 0	Поддерживаемая скорость ячеек (SCR) - это средняя скорость ячеек при пульсирующем трафике по принципу "включено-выключено", а также один из параметров пульсирующего трафика. Введите значение SCR, оно должно быть меньше значения PCR.	0

Табл. 26-2 Меню 4 - Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Maximum Burst Size (Максимальный размер пакета) (MBS)=0	Обозначает максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите значение MBS, которое должно быть менее 65535.	0
My Login (Регистрационное имя)	Настройка полей **My Login (Регистрационное имя)**и **My Password (Пароль)** выполняется только для PPPoA и PPPoE инкапсуляции. Введите зарегистрированное имя пользователя, данное Интернет-провайдером. При использовании инкапсуляции PPPoE это поле заполняется по форме user@domain, где имя домена идентифицирует служебное имя PPPoE.	N/A
My Password (Пароль)	Введите пароль для данного регистрационного имени.	N/A
ENET ENCAP Gateway (Шлюз ENET ENCAP)	При использовании инкапсуляции **ENET ENCAP** введите IP-адрес шлюза, предоставленного Интернет-провайдером .	N/A
Idle Timeout (Время простоя)	В этом поле указывается время простоя в секундах до того, как OMNI ADSL производит автоматическое отключение сеанса связи PPPoE.	0
IP Address Assignment (Назначение IP-адреса)	Нажатием клавиши [SPACE BAR] выберите **Static (Статический)** или **Dynamic (Динамический)** тип назначения IP-адреса.	Dynamic
IP Address (IP-адрес)	Если используется, введите IP-адрес, предоставленный Интернет-провайдером.	N/A
Network Address Translation(Трансляция сетевых адресов)	Нажатием клавиши [SPACE BAR] выберите одну из функций **None**, **SUA Only** или **Full Feature**. Для получения дополнительной информации о функции SUA (Подключение одиночного пользователя) см. главу *NAT*.	SUA Only
Address Mapping Set (Набор преобразований адресов)	Для получения дополнительной информации введите номер набора преобразования адресов (1-8) для использования с NAT см. главу *NAT* .	N/A
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

Если все настройки верны, OMNI ADSL должен автоматически подключиться к сети Интернет. Если подключение не будет успешным, на экран будет выведено сообщение об ошибке. Следует внимательно ознакомиться с ним и предпринять необходимые шаги для устранения неполадок.

Chapter 27
Конфигурирование удаленного узла

В этой главе отражены вопросы конфигурирования удаленного узла.

27.1 Описание настройки удаленного узла

В данном разделе описываются не зависящие от протокола параметры удаленного узла. Удаленный узел необходим для отправки вызова на удаленный шлюз. Удаленный узел представляет как удаленный шлюз, так и как сеть за ним. При настройке доступа в Интернет в Меню 4 фактически конфигурируются параметры одного из удаленных узлов.

В **Меню 11- Настройка удаленного узла** вначале выберите пункт remote node (удаленный узел). После этого можно будет отредактировать настройки узла в меню 11.1, а также выполнить конфигурирование отдельных настроек в трех подменю, а именно, отредактировать опции IP и моста в меню 11.3; редактировать опции ATM в меню 11.6 и настройки фильтра в меню 11.5.

27.2 Настройка удаленного узла

В данном разделе описываются не зависящие от протокола параметры удаленного узла.

27.2.1 Настройки пользователя для удаленного узла

Для конфигурирования удаленного узла следует выполнить описанные ниже действия:

Step 1. В Главном меню введите 11 для вызова **Меню 11 - Настройка удаленного узла.**

Step 2. После появления Меню 11, показанного на следующем рисунке, введите номер удаленного узла, который нужно сконфигурировать.

```
                Меню 11 - "Настройка удаленного узла"

                  1. My ISP (ISP, SUA)
                  2. ________
                  3. ________
                  4. ________
                  5. ________
                  6. ________
                  7. ________
                  8. ________


                        ENTER Node # to Edit:
```

Рис. 27-1 Меню 11 - Настройка удаленного узла

27.2.2 Сценарии инкапсуляции и мультиплексирования

Для доступа в сеть Интернет следует пользоваться методами инкапсуляции и методом мультиплексирования, рекомендованными Вашим Интернет-провайдером. для получения необходимой информации о методах инкапсуляции и мультиплексирования для соединений LAN-to-LAN, например, между локальной сетью филиала и головным офисом корпорации, обращайтесь за консультацией к Интернет-провайдеру. Предполагается, что предварительно должно быть установлено соглашение о методах мультиплексирования и инкапсуляции, поскольку они не распознаются автоматически. Выбор метода(-ов) зависит от числа имеющихся виртуальных каналов (VC) и требований к составу необходимых для работы протоколов. Инкапсуляция ENET ENCAP требует передачи дополнительной служебной информации, что делает этот метод нерациональным для соединения локальных сетей. Далее приведено несколько примеров комбинаций, более предпочтительных для реализации этой задачи.

Сценарий 1. Один виртуальный канал, множество протоколов

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

Сценарий 2. Один виртуальный канал, один протокол (IP)

Инкапсуляция **RFC-1483** с мультиплексированием **на базе VC** требует минимального количества служебной информации (0 октет). Однако, если в дальнейшем возникнет необходимость в

поддержке множества протоколов, более надежной может оказаться инкапсуляция **PPPoA**, а не **RFC-1483**, так как в этом случае не придется переконфигурировать компьютеры.

Сценарий 3. Множество виртуальных каналов

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

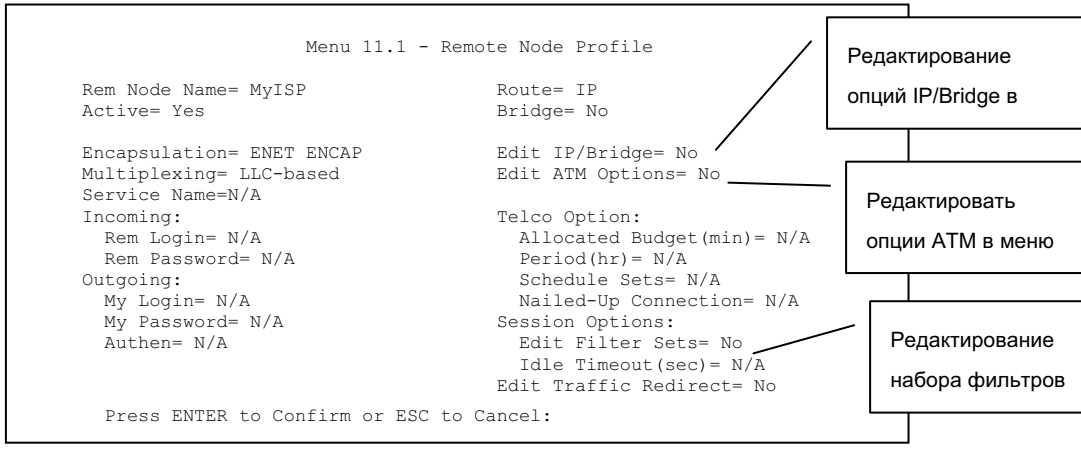


Рис. 27-2 Меню 11.1 - Настройки пользователя для удаленного узла

Заполните поля в Меню **11.1 – Настройки пользователя для удаленного узла**, как описано в следующей таблице.

Табл. 27-1 Меню 11.1 - Настройки пользователя для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Rem Node Name (Имя удаленного узла)	Введите уникальное идентифицирующее имя для данного узла (до восьми символов).	MyISP
Active (Активно)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите **Yes** (для включения) или **No** (для отключения узла) Неактивные узлы обозначаются в Меню 11 SMT знаком минуса ("–").	**Yes**

Табл. 27-1 Меню 11.1 - Настройки пользователя для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Encapsulation (Инкапсуляция)	**PPPoA** относится к RFC-2364 (Инкапсуляция PPP через уровень 5 адаптации ATM). Если выбран протокол RFC-1483 (Мультипротокол инкапсуляции через уровень 5 адаптации ATM) протокола **ENET ENCAP**, то поля **Rem Login**, **Rem Password**, **My Login**, **My Password** и **Authen** - недоступны (**N/A**).	**ENET ENCAP**
Multiplexing (Мультиплексирование)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите использующийся Интернет-провайдером метод мультиплексирования: **на базе VC** или **на базе LLC**.	**LLC-based**
Service Name (Служебное имя)	При использовании инкапсуляции **PPPoE** введите здесь служебное имя PPPoE.	N/A
Incoming (Входящий):		
Rem Login (Регистрационное имя удаленного узла)	Введите регистрационное имя, которое данный удаленный узел будет использовать при вызове OMNI ADSL. Регистрационное имя и пароль удаленного узла (**Rem Password**) будут использоваться для аутентификации данного узла.	
Rem Password (Пароль удаленного узла)	Введите пароль, который данный удаленный узел будет использовать при вызове OMNI ADSL.	
Outcoming (Выходящий):		
My Login (Регистрационное имя)	Введите регистрационное имя, назначенное Интернет-провайдером, которое OMNI ADSL будет использовать при вызове данного удаленного узла.	
My Password (Пароль)	Введите пароль, назначенный Интернет-провайдером, который OMNI ADSL будет использовать при вызове данного удаленного узла.	
Authen (Аутентификация)	В данном поле устанавливается протокол аутентификации, применяемый для исходящих вызовов. В этом поле используются следующие опции: **CHAP**/**PAP** – OMNI ADSL будет принимать **CHAP** или **PAP** при запросе данного удаленного узла.	

Табл. 27-1 Меню 11.1 - Настройки пользователя для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
	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)	В данном поле определяется протокол, используемый при маршрутизации. Возможные опции: **IP** и **None.**	**IP**
Bridge (Мост)	Если межсетевой мост включен, OMNI ADSL будет пересылать любой пакет, который он не маршрутизирует, на удаленный узел. В противном случае, такие пакеты будут сброшены. Выбрать **Yes** для включения или **No** для отключения.	**No**
Edit IP/Bridge (Редактирование IP/моста)	Нажатием клавиши [SPACE BAR] выберите **Yes**, а затем нажмите клавишу [ENTER] для вызова **Меню 11.3 – Параметры сетевого уровня удаленного узла**.	**No**
Edit ATM Options (Редактирование функций ATM)	Нажмите клавишу пробела для выбора **Yes**, а затем нажмите клавишу [ENTER] для вывода **Меню 11.6 – Параметры уровня ATM для удаленного узла**.	**No**
Telco Option (Функция Telco)		
Allocated Budget (min) (Бюджет времени, в мин)	Этим значением задается потолок (в минутах) по совокупной продолжительности исходящих вызовов для данного удаленного узла. Значение по умолчанию - 0, т.е. нет ограничений.	
Period (hr) (Период обновления, в часах)	В этом поле указывается время обновления бюджета (в часах). Например, если разрешено вызывать данный удаленный узел на протяжении максимум 10 минут в час, то значение **Allocated Budget** составляет 10 (минут), а значение **Period** - 1 (час).	
Schedule Sets (Набор планов)	Данное поле доступно только при инкапсуляции **PPPoE** и **PPPoA**. В этом пункте можно задать до четырех наборов планов. Для получения подробной информации см. главу *Call Scheduling (Расписание связи)*.	
Nailed up Connection (Полупостоянное соединение)	Данное поле доступно только при инкапсуляции **PPPoE** и **PPPoA**. Это поле определяет, желательно ли сделать соединение с данным удаленным узлом полупостоянным соединением.	
Session Options		

Табл. 27-1 Меню 11.1 - Настройки пользователя для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
(Опции сеанса связи)		
Edit Filter Sets (Редактирование набора фильтров)	Нажмите клавишу пробела для выбора **Yes**, а затем нажмите клавишу [ENTER] для перехода в Меню 11.5 для редактирования наборов фильтров. Для получения более подробной информации см. раздел *Фильтры для удаленного узла*.	**No** (по умолчанию)
Idle Timeout (sec) (Время ожидания, в сек)	Введите время в секундах в диапазоне (0-9999), в течение которого не происходит обмен, когда OMNI ADSL находится в состоянии ожидания (трафик по направлению к удаленному узлу отсутствует), до автоматического отключения OMNI ADSL удаленного узла. 0 означает, что ограничений по продолжительности сеанса нет.	
Edit Traffic Redirect (Перенаправление трафика)	Нажмите клавишу пробела для выбора **Yes**, а затем нажмите клавишу [ENTER] для перехода в Меню 11.7 для редактирования перенаправления трафика. Для получения более подробной информации см. раздел *Перенаправление трафика* . Это поле имеется не во всех моделях.	**No** (по умолчанию)
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

27.2.3 Протокол аутентификации исходящих вызовов

По понятным причинам рекомендуется использовать максимально надежный протокол аутентификации. Однако некоторые реализации оборудования используют в настройках пользователя специфические протоколы аутентификации. Если для такого устройства будет задан протокол аутентификации, отличающийся от установленного в настройках пользователя, вызов будет автоматически разъединен. Если вызов разъединяется непосредственно после успешной аутентификации, следует убедиться, что используется правильный протокол аутентификации для данного устройства.

27.3 Metric (Метрика)

Метрика представляет собой "стоимость передачи". Маршрутизатор выбирает лучший маршрут передачи данных, обладающий самой низкой "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве своего рода единицы "стоимости". Минимальное значение равно 1 и соответствует прямому соединению. Значение метрики должно быть в диапазоне от "1" до "15". Если оно больше "15", это означает что канал не установлен. Чем меньше это значение, тем ниже "стоимость" маршрута.

На основании метрики устанавливается приоритетность маршрутов выхода OMNI ADSL в Интернет. Если оба заданных по умолчанию маршрута имеют одинаковые метрики, OMNI ADSL пользуется предварительно установленными приоритетами:

1. Обычный маршрут: выбирается Интернет-провайдером
2. Маршрут с перенаправленным трафиком

Маршрутизация на базе стратегии IP игнорирует маршрутизацию, заданную по умолчанию, и имеет более высокий приоритет по отношению ко всем упоминавшимся ранее маршрутам (см. главу *Маршрутизация на базе стратегии IP*).

Например, если обычный маршрут имеет метрику "1", а маршрут с перенаправленным трафиком - "2", то первый выступает в качестве основного маршрута, заданного по умолчанию. Если по обычному маршруту не удается подключиться к сети Интернет, то OMNI ADSL пытается воспользоваться маршрутом с перенаправленным трафиком.

27.4 Параметры сетевого уровня для удаленного узла

Для настройки параметров TCP/IP следует выполнить ряд действий по редактированию в Меню **11.3** – Параметры сетевого уровня удаленного узла, как показано ниже.

Step 1. В Меню 11.1 убедитесь, что **IP** входит в число протоколов в поле **Route**.

Step 2.

Переместите курсор в поле **Edit IP/Bridge** и для выбора **Yes** нажмите клавишу [SPACE BAR], а затем клавишу [ENTER] - для вызова **Menu 11.3** – **Параметры сетевого уровня для удаленного узла.**

```
               Menu 11.3 - Remote Node Network Layer Options

   IP Options:                          Bridge Options:
      IP Address Assignment= Dynamic      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= Full Feature
        Address Mapping Set= 2
      Metric= 2
      Private= No
      RIP Direction= None
         Version= RIP-1
      Multicast= None
      IP Policies= 3,4,5,6

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

Рис. 27-3 Меню 11.3 Опции сетевого уровня для удаленного узла

В следующей таблице дается описание полей Меню **11.3 – Параметры сетевого уровня для удаленного узла**.

Табл. 27-2 Меню 11.3 - Опции сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
IP Address Assignment (Назначение IP-адреса)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите **Dynamic**, если удаленным узлом используется динамически назначаемый IP-адрес или **Static**, если им используется статический (фиксированный) IP-адрес. Такую настройку можно выполнить только для узла ISP (это относится также к настройке из меню 4). Для остальных типов узлов устанавливается признак **Static**.	**Dynamic**
Rem IP Addr (IP-адрес удаленного узла)	IP-адрес, заданный в предыдущем меню.	

Табл. 27-2 Меню 11.3 - Опции сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Rem Subnet Mask (Маска подсети для удаленного узла)	Введите значение маски подсети, назначенное для удаленного узла.	
My WAN Addr (Адрес WAN)	В некоторых реализациях, в частности, производных от UNIX, каналы WAN и LAN должны иметь отдельные сетевые номера IP, при этом каждый конец должен иметь уникальный адрес внутри сетевого номера WAN. Если это именно тот случай, введите IP-адрес, назначенный порту WAN OMNI ADSL. Примечание: относится к локальному адресу устройства OMNI ADSL, а не к адресу удаленного маршрутизатора.	
NAT	Нажатием клавиш [SPACE BAR] и [ENTER] выберите **Full Feature**, если у устройства OMNI ADSL есть несколько общедоступных IP-адресов в глобальной сети. Если OMNI ADSL имеет только один общедоступный IP-адрес в глобальной сети, выберите режим **SUA Only**. В SMT используется набор преобразований адресов 255 (меню 15.1 - см. раздел *30.3.1*). Выберите опцию **None** для отключения NAT.	**SUA Only**
Address Mapping Set (Набор преобразований адресов)	Если в поле **NAT** выбрана опция **Full Feature**, следует выполнить конфигурирование набора преобразования адресов в меню 15.1. Выберите один из наборов серверов NAT (2-10) в меню 15.2 (для получения более подробной информации см. главу *Трансляция сетевых адресов*) и введите здесь его номер. Если в поле **NAT** выбрана опция **SUA Only**, системная консоль будет пользоваться набором серверов NAT 1 в меню 15.2 (для получения более подробной информации см. главу *Трансляция сетевых адресов*).	2
Metric (Метрика)	Метрика определяет "стоимость" передачи и используется для целей маршрутизации. Маршрутизация IP использует счетчик переходов по сети в качестве своего рода единицы "стоимости". Минимальное значение равно 1 и соответствует прямому соединению. 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, обычно, хорошо работают значения 2 или 3.	2

Табл. 27-2 Меню 11.3 - Опции сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Private (частный)	Этот параметр определяет, будет ли OMNI ADSL включать данный маршрут к удаленному узлу в циркулярную рассылку RIP. Если установлено **Yes**, данный маршрут считается частным и не включается в циркулярную рассылку RIP. Если установлено **No**, данный маршрут к удаленному узлу является доступным для других хост-машин через циркулярную рассылку RIP.	**No**
RIP Direction (Направление RIP)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите одну из следующих опций RIP Direction: **Both**, **In Only**, **Out Only** или **None**.	**None**
Version (Версия)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите одну из следующих форм RIP: **RIP-1**, **RIP-2B** или **RIP-2M**.	**RIP-1**
Multicast (Многоадресная рассылка)	**IGMP-v1 устанавливает** IGMP для версии 1, **IGMP-v2** устанавливает IGMP для версии 2 и опция **None отключает** IGMP.	**None**
IP Policies (Стратегии IP)	Возможно применение до четырех наборов стратегий IP (из 12) перечислением их номеров, разделенных запятыми. Вначале сконфигурируйте наборы фильтров в меню 25 (см. главу *Маршрутизация на базе стратегии IP*), а затем примените их здесь.	3, 4, 5, 6
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

27.4.1 Поле "My WAN Addr": пример IP-адреса

На следующем рисунке приводится пример IP-адресов, призванный разъяснить смысл поля **My Wan Addr** в меню 11.3. Для ознакомления с кратким разъяснением, что такое IP-адрес в глобальной сети см. рис. *Адресование в локальной и глобальной вычислительных сетях* в главе с описанием работы Web-конфигуратора при настройке LAN . В поле **My WAN Addr** отображается адрес локального WAN IP устройства OMNI ADSL (на приведенном ниже рисунке это 172.16.0.1), в то время как в поле **Rem IP Addr** отображается адрес клиентского устройства WAN IP (на приведенном ниже рисунке это 172.16.0.2).

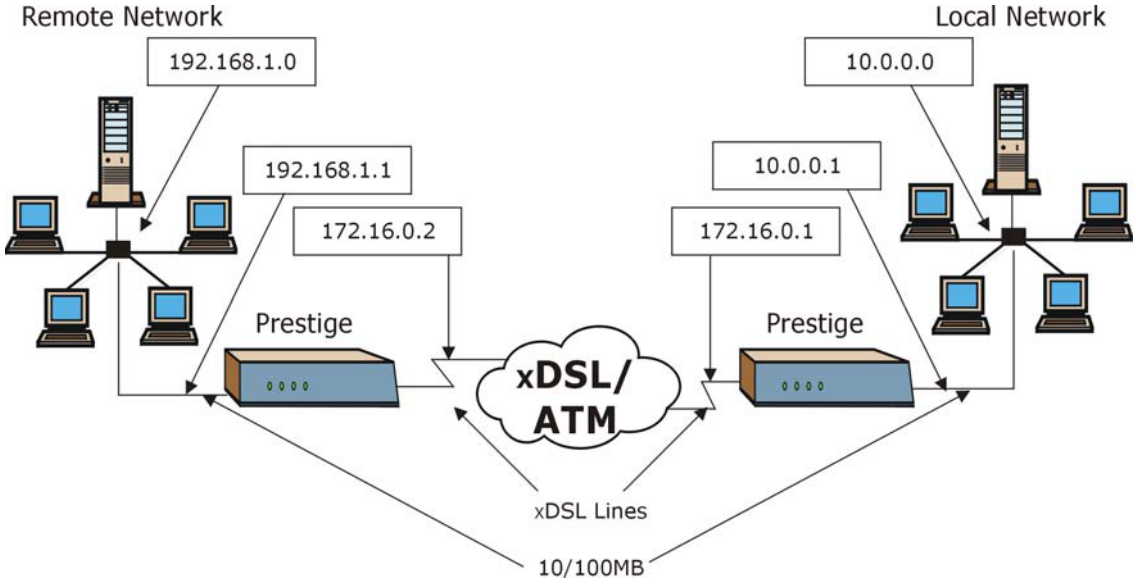


Рис. 27-4 Пример IP-адреса для соединения локальных сетей на базе TCP/IP

27.5 Фильтр удаленного узла

Установите курсор в поле **Edit Filter Sets** в меню 11.1, а затем нажатием клавиши [SPACE BAR] выберите опцию **Yes**. Нажмите клавишу [ENTER] для вызова Меню **11.5** – Фильтр удаленного узла.

В **Меню 11.5 – Фильтр удаленного узла** задайте набор(-ы) фильтров для применения к входящему и исходящему трафику между данным удаленным узлом и OMNI ADSL, а также для блокировки инициирования вызовов определенными пакетами. В каждом поле фильтров можно определить до 4 наборов фильтров, разделенных запятой, напр., 1, 5, 9, 12, .

В этом поле допускается ввод пробелов. OMNI ADSL поставляется с готовым набором фильтров, NetBIOS_WAN, который блокирует пакеты NetBIOS (фильтр протокола вызовов = 1). Его можно включить в набор фильтров вызовов, если Вы не хотите, чтобы пакеты NetBIOS инициировали вызовы на удаленный узел.

```
                    Menu 11.5 - Remote Node Filter

                         Input Filter Sets:
                           protocol filters= 11, 12
                             device filters=
                         Output Filter Sets:
                           protocol filters=
                             device filters=

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

Рис. 27-5 Меню 11.5 - Фильтр для удаленного узла (RFC 1483 или инкапсуляция ENET)

```
                    Menu 11.5 - Remote Node Filter

                         Input Filter Sets:
                           protocol filters= 11, 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:
```

Рис. 27-6 Меню 11.5 - Фильтр для удаленного узла (инкапсуляция PPPoA или PPPoE)

27.5.1 Правила фильтров для защиты Web-конфигуратора в сети Интернет

В Web-конфигураторе откройте экран **Security (Защита)**, показанный ниже. Выберите предварительно заданные правила фильтров и щелкните по **Apply (Применить)**. Данная функция имеется не во всех моделях.

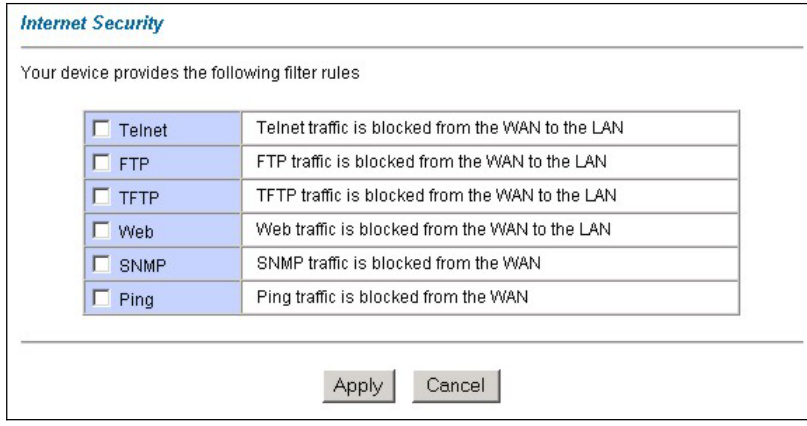


Рис. 27-7 Безопасность сети Интернет

Если правила фильтров уже применяются в Web-конфигураторе, наборы фильтров 11 и 12 будут автоматически применяться в поле **protocol filters (фильтры протокола)** под **Input Filter Sets (Наборы входных фильтров)** в меню 11.5 системной консоли.

Ранее применявшиеся номера набора фильтров протокола входящего потока данных SMT уничтожаются, как только в Web-конфигураторе будут применены правила фильтров Internet Security **(Безопасность в сети Интернет).Для восстановления прежних или применения новых наборов фильтров необходимо повторно ввести значения номеров набора фильтров вместе с наборами фильтров 11 и 12. Например, для того чтобы применить наборы фильтров 1 и 2 введите “1, 2, 11, 12”.**

27.5.2 Наборы фильтров Web-конфигуратора

Когда правила фильтров применяются при использовании Web-конфигуратора, наборы фильтров 11 и 12 автоматически генерируются в меню 21 системной консоли. Данная функция доступна не во всех моделях.

```
                    Menu 21 - Filter Set Configuration

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


                  ENTER Filter Set Number to Configure= 0
```

Рис. 27-8 Меню 21- Конфигурация набора фильтров (P650R и P650R-E)

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

```
                        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. 27-9 Меню 21.11- WebSet 11

```
                        Menu 21.12 - 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 N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                                N D N
3 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=69                               N D N
4 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80                                N D N
5 Y IP   Pr=1, SA=0.0.0.0, DA=0.0.0.0, DP=0                                 N D N
6 N

                ENTER Filter Rule Number (1-6) to Configure
```

Рис. 27-10 Меню 21.12- WebSet 12

Не следует редактировать наборы фильтров 11 и 12. Они используются исключительно Web-конфигуратором. Любые правила, сконфигурированные Вами в наборах 11 и 12, будут уничтожены и заменены при применении сгенерированных Web-конфигуратором правил фильтров.

27.6 Редактирование опций уровня ATM

Действия, которые нужно выполнить для редактирования **Меню 11.6 - Remote Node ATM Layer Options (Опции уровня ATM для удаленного узла)**, показаны ниже.

Установите курсор в поле **Edit ATM Options** в меню 11.1, а затем нажатием клавиши [SPACE BAR] выберите опцию **Yes**. Нажмите клавишу [ENTER] для перехода в **Меню 11.6 – Remote Node ATM Layer Options (Опции уровня ATM для удаленного узла).**

В OMNI ADSL существует два варианта Меню 11.6, в зависимости от выбранного в Меню 11.1 метода мультиплексирования - **на базе VC** или **на базе LLC** и инкапсуляции **PPP**.

27.6.1 Мультиплексирование на базе VC (инкапсуляция non-PPP)

Для мультиплексирования **на базе VC**, по предварительному соглашению, определенному виртуальному каналу назначается некоторый протокол, например, VC1, который будет поддерживать протокол IP. Для каждого протокола должны быть назначены отдельные номера идентификаторов виртуального пути (VPI) и виртуального канала (VCI).

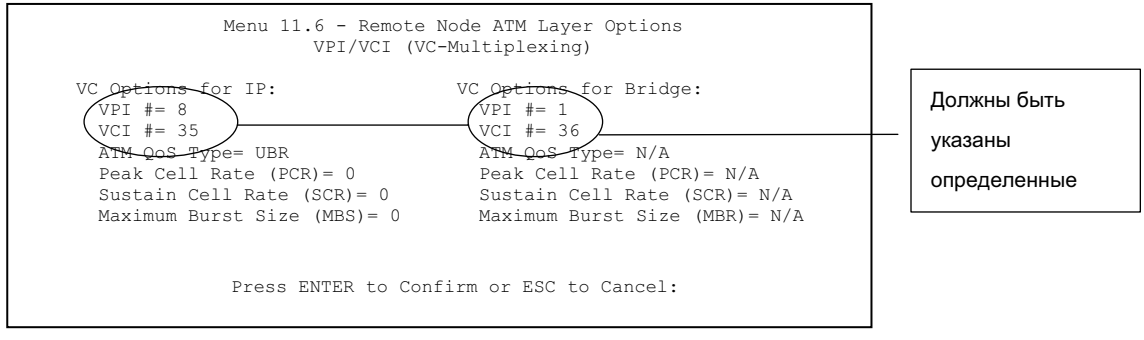


Рис. 27-11 Меню 11.6 для мультиплексирования на базе VC

27.6.2 Мультиплексирование на базе LLC или инкапсуляция PPP

При мультиплексировании **на базе LLC** или инкапсуляции **PPP** один виртуальный канал передает несколько протоколов с идентифицирующей информацией, которая содержится в заголовке каждого пакета.

```
                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:
.
```

Нужно указать только один блок номеров VPI и VCI.

Рис. 27-12 Меню 11.6 для мультиплексирования на базе LLC или инкапсуляции PPP

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

27.7 Перенаправление трафика

В случае невозможности подключения OMNI ADSL к сети Интернет осуществляется перенаправление трафика LAN к резервному шлюзу. Пример подобной ситуации показан на рис. ниже.

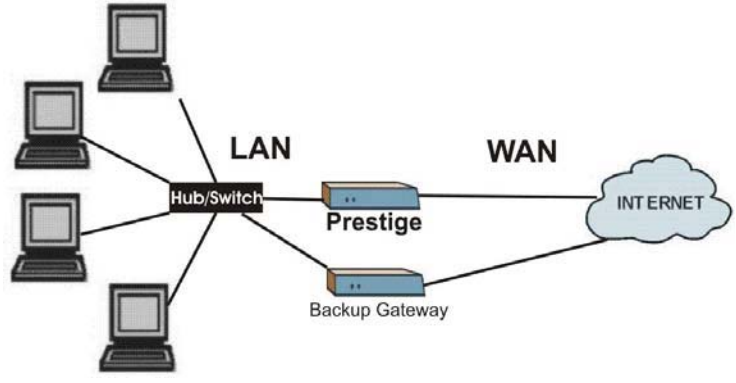


Рис. 27-13 Пример настройки перенаправления трафика

Для настройки параметров перенаправления трафика введите 11 в главном меню для вызова **Menu 11.1– Настройки пользователя для удаленного узла** , показанного ниже.

```
                Menu 11.1 - Remote Node Profile

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

Encapsulation= ENET ENCAP               Edit IP/Bridge= No
Multiplexing= LLC-based                 Edit ATM Options= No
Service Name=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
                                        Edit Traffic Redirect= Yes

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

Рис. 27-14 Меню 11.1 – Настройки пользователя для удаленного узла

Для настройки свойств перенаправления трафика нажатием клавиши [SPACE BAR] выберите опцию **Yes** в поле **Edit Traffic Redirect (Редактирование перенаправления трафика)**, а затем нажмите клавишу [ENTER].

Табл. 27-3 Меню 11.1 – Настройки пользователя для удаленного узла (поле "Перенаправление трафика")

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Edit Traffic Redirect (Перенаправление трафика)	Нажатием клавиши [SPACE BAR] выберите опцию **Yes** и нажмите клавишу [ENTER] для настройки **Меню 11.7 – Настройка перенаправления трафика**.	**Yes**
Нажать клавишу [ENTER] при появлении сообщения: Press ENTER to Confirm ..., чтобы сохранить конфигурацию. Для отмены изменений в любой момент нажмите клавишу [ESC].		

27.7.1 Настройка перенаправления трафика

Пользуясь **Меню 11.7 — Настройка перенаправления трафика**, сконфигурируйте параметры, определяющие, в каких случаях OMNI ADSL будет пересылать трафик WAN к резервному шлюзу,

```
                Menu 11.7 - Traffic Redirect Setup

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



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

Рис. 27-15 Меню 11.7 - Настройка перенаправления трафика

Следующая таблица описывает поля данного меню.

Табл. 27-4 Меню 11.7 - Настройка перенаправления трафика

ПОЛЕ	ОПИСАНИЕ
Active (Активно)	Нажатием клавиши [SPACE BAR] выберите опцию **Yes** (для включения) или **No** (для отключения) функции настройки перенаправления трафика. По умолчанию установлено **No**. Если в поле **Active** установлена опция **Yes**, то пока используется инкапсуляция PPPoE в этом экране необходимо сконфигурировать все поля (за исключением полей **Check WAN IP Address (IP-адрес WAN)** и **Timeout (Время ожидания)**). Если при использовании инкапсуляции PPPoE не будет выполнена настройка этих полей, то OMNI ADSL проверит канал PPPoE для установления, имеется ли соединение с WAN.
Configuration (Конфигурация):	
Backup Gateway IP Address (Резервное сохранение IP-адреса шлюза)	Введите IP-адрес резервного шлюза в десятичном виде с разделительными точками. OMNI ADSL автоматически пересылает трафик на этот IP-адрес, если отсутствует соединение OMNI ADSL с сетью Интернет.

Табл. 27-4 Меню 11.7 - Настройка перенаправления трафика

ПОЛЕ	ОПИСАНИЕ
Metric (Метрика)	В этом поле устанавливаются значения приоритетов маршрутов, использующихся устройством OMNI ADSL. Метрика представляет "стоимость передачи". Маршрутизатор выбирает лучший маршрут передачи данных, обладающий самой низкой "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве своего рода единицы "стоимости". Минимальное значение равно 1 и соответствует прямому соединению. Значение метрики должно быть от "1" до "15", Если оно больше "15", это означает что канал не установлен. Чем меньше это значение, тем ниже "стоимость" маршрута.
После окончания работы в этом меню при появлении сообщения "Press [ENTER] to confirm or [ESC] to cancel" нажмите клавишу [ENTER] для сохранения конфигурации или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.	

Chapter 28
Настройка статического маршрута

В этой главе описывается настройка статического маршрута IP.

28.1 Описание статического маршрута IP

Статические маршруты сообщают OMNI ADSL информацию о маршрутизации, которую он не может получить автоматически другими средствами. Такая ситуация может возникнуть, если, напр., был запрещен обмен пакетами RIP в локальной сети, или если удаленная сеть не подключена напрямую к удаленному узлу.

Каждый удаленный узел определяет только ту сеть, к шлюзу которой он непосредственно подключен, при этом OMNI ADSL не владеет никакой информацией о других сетях. Например, на рисунке показано, что OMNI ADSL получает информацию о сети N2 через маршрутизатор удаленного узла 1. Тем не менее, OMNI ADSL не может маршрутизировать пакеты в сеть N3, так как он "не знает", как получить к ней доступ через маршрутизатор удаленного узла 1 (через маршрутизатор 2). Статические маршруты позволяют предоставить OMNI ADSL сведения о сетях, находящихся за удаленными узлами.

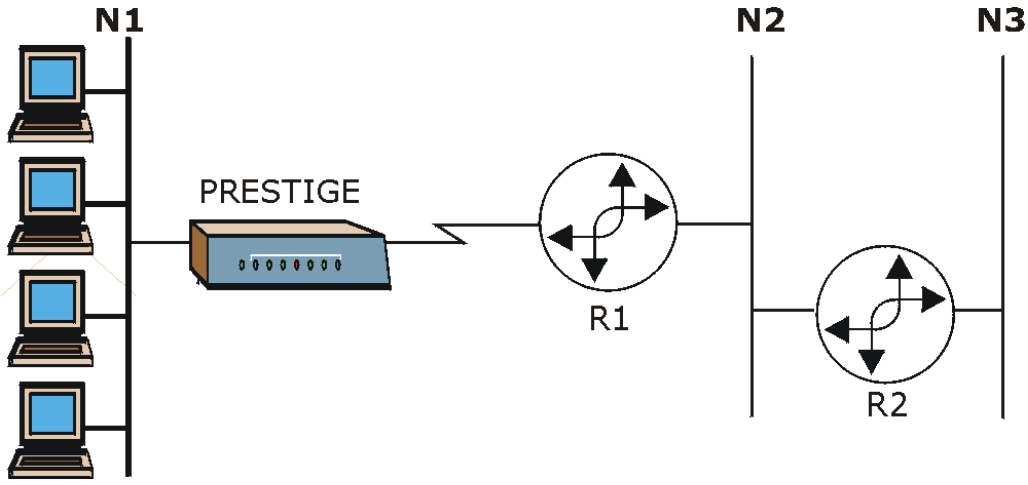


Рис. 28-1 Пример топологии статической маршрутизации

28.2 Конфигурирование статического маршрута IP

Step 1. Чтобы выполнить настройку статического маршрута IP, следует использовать **Меню 12 - Static Route Setup**, показанного ниже.

```
Menu 12 - Static Route Setup

        1. IP Static Route
        3. Bridge Static Route


Please enter selection:
```

Рис. 28-2 Меню 12 - Настройка статического маршрута

Step 2. В Меню 12 выберите 1 для вызова **Меню 12.1 — IP Static Route Setup (Настройка статического маршрута)**, показанного ниже.

```
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:
```

Рис. 28-3 Меню 12.1 - Настройка статического маршрута IP (P650H/HW)

Step 3. Теперь введите номер статического маршрута, выбранного для конфигурирования.

```
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:
```

Рис. 28-4 Меню 12.1.1 - Редактирование статического маршрута IP

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

Табл. 28-1 Меню 12.1.1 - Редактирование статического маршрута IP

ПОЛЕ	ОПИСАНИЕ
Route # (Номер маршрута)	Порядковый номер статического маршрута, выбранный в меню 12.1.

Табл. 28-1 Меню 12.1.1 - Редактирование статического маршрута IP

ПОЛЕ	ОПИСАНИЕ
Route Name (Имя маршрута)	Введите идентифицирующее имя для данного маршрута. Эта информация нужна только для идентификации.
Active (Активно)	Это поле позволяет включать/выключать статический маршрут.
Destination IP Address (IP-адрес назначения)	Данный параметр определяет IP-адрес сети конечного адресата. Маршрутизация всегда основывается на сетевом номере. Если нужно определить маршрут к отдельной хост-машине, следует использовать маску подсети 255.255.255.255 в поле маски подсети, чтобы сетевой номер стал идентичен ID хост-машины.
IP Subnet Mask (Маска подсети IP)	Введите маску подсети для данного пункта назначения. См. порядок назначения *IP Subnet Mask (Маски подсети IP)* в данном руководстве.
Gateway IP Address (IP-адрес шлюза)	Введите IP-адрес шлюза. Шлюз является ближайшей к OMNI ADSL соседней станцией, которая будет пересылать пакет дальше по назначению. В локальной сети шлюзом должен быть маршрутизатор, находящийся в том же сегменте, что и OMNI ADSL; в глобальной сети шлюзом должен быть IP-адрес одного из удаленных узлов.
Metric (Метрика)	Метрика определяет "стоимость" передачи и используется для целей маршрутизации. Маршрутизация IP использует счетчик переходов по сети в качестве своего рода единицы "стоимости". Минимальное значение равно 1 и соответствует прямому соединению. 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, обычно, хорошо работают значения 2 или 3.
Private (Частный)	Этот параметр определяет, будет ли OMNI ADSL включать данный маршрут к удаленному узлу в циркулярную рассылку RIP. Если установлена опция **Yes**, то данный маршрут считается частным и не включается в циркулярную рассылку RIP. Если установлено **No**, данный маршрут к удаленному узлу является доступным для других хост-машин через циркулярную рассылку RIP.
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.	

Chapter 29
Настройка передачи по мосту

В данной главе рассматривается конфигурирование параметров OMNI ADSL для межсетевого моста.

29.1 Описание передачи по мосту

При настроенном межсетевом мосте переадресация осуществляется на основе MAC (Media Access Control/Управление доступом к среде) или аппаратного адреса, в то время как при маршрутизации - на основе адреса сетевого уровня (IP или IPX). Передача по мосту позволяет OMNI ADSL передавать пакеты для протоколов сетевого уровня из одной сети в другую, которые OMNI ADSL не маршрутизирует, напр., SNA. Проблема заключается в том, что, по сравнению с маршрутизацией, передача по мосту генерирует значительно больший трафик для тех же самых сетевых протоколов и потребляет больше циклов ЦП и памяти.

По причинам, связанным с рентабельностью, *не* следует включать опцию передачи по мосту, пока не потребуется поддерживать протоколы, отличающиеся от использующихся в Вашей сети протоколов IP. Для протокола IP, если это требуется, доступна маршрутизация; не следует передавать по межсетевому мосту то, что OMNI ADSL может маршрутизировать.

29.2 Настройка Ethernet для моста

В основном, все пакеты, не являющиеся локальными, передаются по мосту в WAN. Маршрутизатором OMNI ADSL не поддерживается межсетевой обмен пакетами (IPX).

29.2.1 Настройка межсетевого моста для удаленного узла

Для конфигурирования независящих от протокола параметров в **Меню 11.1 – Настройки пользователя для удаленного узла** - следует выполнить процедуру, описанную в другом разделе. Параметры, связанные с межсетевым мостом, конфигурируются в **Меню 11.3 – Параметры сетевого уровня удаленного узла**.

Для настройки **Меню 11.3 – Параметры сетевого уровня удаленного узла**, показанного на следующем рисунке, необходимо выполнить описанные ниже действия:

Step 1. В меню 11.1 убедитесь, что в поле **Bridge (Мост)** установлено **Yes**.

```
                    Menu 11.1 - Remote Node Profile

Rem Node Name= ?                        Route= IP
Active= Yes                             Bridge= Yes

Encapsulation= ENET ENCAP               Edit IP/Bridge= Yes
Multiplexing= VC-based                  Edit ATM Options= No
Service Name=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
                                        Edit Traffic Redirect= No

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

Рис. 29-1 Меню 11.1 - Настройки пользователя для удаленного узла

Step 2. Переместите курсор в поле **Edit IP/Bridge**, а затем нажатием клавиши [SPACE BAR] установите значение **Yes** и нажмите клавишу [ENTER] для редактирования **Меню 11.3 – Опции сетевого уровня для удаленного узла**.

```
            Menu 11.3 - Remote Node Network Layer Options

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

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

Рис. 29-2 Меню 11.3 - Опции сетевого уровня для удаленного узла

Табл. 29-1 Меню 11.3 - Опции сетевого уровня для удаленного узла : поля настройки моста

ПОЛЕ	ОПИСАНИЕ
Bridge (menu 11.1) (Мост (меню 11.1))	Убедитесь, что в данном поле установлено **Yes**.
Edit IP/Bridge (menu 11.1) (Редактирование IP/Мост (меню 11.1))	Нажатием клавиши [SPACE BAR] выберите **Yes** и нажмите клавишу [ENTER] для вызова меню 11.3.
Ethernet Addr Timeout (min.) (menu 11.3) (Время сохранения адреса Ethernet, в мин (меню 11.3))	Введите время (в минутах), в течение которого OMNI ADSL должен сохранять информацию об адресе Ethernet в своих внутренних таблицах, пока линия отключена. Если данная информация сохраняется, то OMNI ADSL не нужно будет перекомпилировать таблицы при повторном включении линии.
После окончания работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.	

29.2.2 Настройка статического маршрута для межсетевого моста

Аналогично статическим маршрутам сетевого уровня, статический маршрут для межсетевого моста сообщает OMNI ADSL, как достичь узла до того, как будет установлено соединение. Статические маршруты для межсетевого моста конфигурируются в Меню 12.3.1, как показано ниже (перейти в Меню 12, выбрать пункт 3, а затем выбрать статический маршрут для редактирования).

```
Menu 12.3 - Bridge Static Route Setup

1. _________
2. _________
3. _________
4. _________

ENTER selection number:
```

Рис. 29-3 Меню 12.3 - Настройка статического маршрута для моста

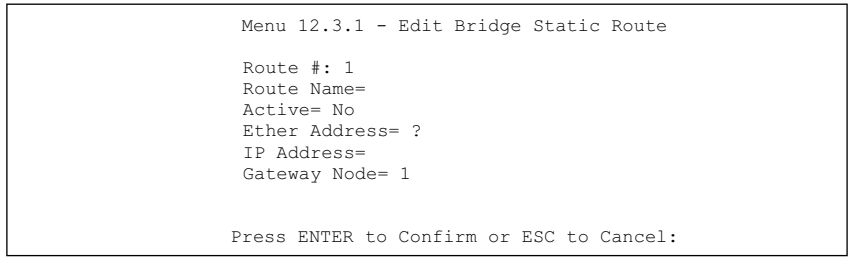


Рис. 29-4 Меню 12.3.1 - Редактирование статического маршрута для моста

В следующей таблице описывается Меню **Редактирование статического маршрута для межсетевого моста**.

Табл. 29-2 Меню 12.3.1 - Редактирование статического маршрута для моста

ПОЛЕ	ОПИСАНИЕ
Route # (Номер маршрута)	Порядковый номер маршрута, установленный в **Меню 12.3 – Настройка статического маршрута для межсетевого моста**.
Route Name (Имя маршрута)	В целях идентификации введите имя статического маршрута для межсетевого моста ().
Active (Активно)	Указывает, является ли статический маршрут активным (**Yes**) или нет (**No**).
Ether Address (Ethernet адрес)	Введите MAC-адрес машины назначения, на которую по мосту должны передаваться пакеты.
IP Address (IP-адрес)	Если доступно, введите IP-адрес машины назначения, на которую должны передаваться по мосту пакеты.
Gateway Node (Шлюзовый узел)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите номер удаленного узла (от 1 до 8), являющегося шлюзом данного статического маршрута.
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.	

Chapter 30
Трансляция сетевых адресов (NAT)

В данной главе описано, как выполнить настройку службы трансляции сетевых адресов (NAT) устройства OMNI ADSL.

30.1 Описание службы NAT

30.1.1 Сравнение режимов SUA (Подключение одиночного пользователя) и NAT

SUA (Single User Account - Подключение одиночного пользователя) является реализацией в операционной системе ZyNOS подмножества NAT, которая поддерживает два типа преобразования, **Many-to-One** и **Server**. Для ознакомления с подробным описанием набора NAT для SUA см. *раздел 30.3.1* . OMNI ADSL также поддерживает функцию **Full Feature** NAT для преобразования множества глобальных адресов во множество частных IP-адресов клиентов или серверов локальной сети с использованием способов преобразования, описание которых приведено в разделе данного руководства, посвященном Web-конфигуратору.

1. **Выберите опцию** SUA Only**, если OMNI ADSL имеет только один общедоступный IP-адрес в глобальной сети.**
2. **Если OMNI ADSL имеет несколько общедоступных IP-адресов в глобальной сети, выберите** Full Feature**.**

30.2 Применение NAT

Установка NAT производится в меню 4 или 11.3, как показано ниже. На следующем рисунке показано, как в меню 4 устанавливается NAT для доступа в сеть Интернет. Введите 4 в главном меню для вызова **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= 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:
```

Рис. 30-1 Меню 4 - Установка NAT для доступа в сеть Интернет

На следующем рисунке показан вариант установки NAT для удаленного узла с помощью меню 11.1.

Step 1. В главном меню выберите "11".

Step 2. После появления Меню 11 введите номер удаленного узла, который нужно сконфигурировать, как показано на следующем рисунке.

Step 3. Установите курсор в поле **Edit IP/Bridge** и нажатием клавиши [SPACE BAR] выберите **Yes**, а затем нажмите клавишу [ENTER] для вызова **Меню 11.3 - Опции сетевого уровня для удаленного узла.**

```
              Menu 11.3 - Remote Node Network Layer Options

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


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

Рис. 30-2 Меню 11.3 - Установка NAT для удаленного узла

В следующей таблице дано описание вариантов выбора трансляции сетевых адресов.

Табл. 30-1 Установка NAT в меню 4 и 11.3

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
NAT	Нажатием клавиш [SPACE BAR] и [ENTER] выберите **Full Feature**, если у устройства OMNI ADSL есть несколько общедоступных IP-адресов в глобальной сети. В SMT используется набор преобразований адресов, сконфигурированный и введенный в поле **Address Mapping Set (Набор преобразований адресов)** (меню 15.1 - см. раздел *30.3.1*).	**Full Feature**
	Выберите опцию **None** для отключения NAT.	**None**
	При выборе опции **SUA Only** SMT используется набор преобразований адресов 255 (меню 15.1 - см. раздел *30.3.1*). Выберите опцию **SUA Only**, если OMNI ADSL имеет только один общедоступный IP-адрес в глобальной сети.	**SUA Only**

30.3 Конфигурирование

Пользуйтесь меню и подменю наборов преобразования адресов при создании таблицы преобразования для назначения глобальных адресов компьютерам LAN. С двумя наборами преобразований адресов можно ознакомиться в меню 15.1. Сконфигурировать можно только **Set 1**

(Набор 1). **Set 255 (Набор 255)** используется для SUA. При выборе опции **Full Feature** в меню 4 или 11.3 SMT будет пользоваться **Set 1 (Набором 1)**. При выборе опции **SUA Only** SMT будет пользоваться предварительно сконфигурированным **Set 255 (Набором 255)** (только для чтения).

Набором сервера является список серверов со стороны LAN, преобразуемых во внешние порты. Для использования данного набора, правило сервера должно быть установлено внутри набора преобразования адресов NAT. Для получения дополнительной информации см. раздел о переадресовании портов в главе с описанием экранов NAT Web-конфигуратора . Для конфигурации

```
                    Menu 15 — NAT Setup

          1.    Address Mapping Sets
          2.    NAT Server Sets


                ENTER Menu Selection Number:
```

NAT необходимо ввести "15" в главном меню для вывода следующего экрана.

Рис. 30-3 Меню 15 - Настройка NAT

30.3.1 Наборы преобразований адресов

Введите "1" для вывода **Меню 15.1 — Наборы преобразований 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:
ENTER Menu Selection Number:
```

Рис. 30-4 Меню 15.1 - Наборы преобразований адресов

Набор преобразований SUA

Введите "255" для вывода на экран следующего меню (см. также *раздел 30.1.1)*. Поля в этом меню недоступны для изменений.

```
                        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                           M-1
 2.                                    0.0.0.0                           Server+
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

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

Рис. 30-5 Меню 15.1.255 - Правила преобразований адресов SUA

В следующей таблице приводится описание полей данного меню.

Меню 15.1.255 предназначено только для чтения.

Табл. 30-2 Правила преобразований адресов SUA

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Set Name (Имя набора)	Название выбранного в меню 15.1 набора или название нового создаваемого набора.	SUA
Idx (Индекс)	Индекс или номер правила.	1
Local Start IP (Начальный локальный IP-адрес)	**Local Start IP** - это начальный локальный IP-адрес (ILA).	0.0.0.0
Local End IP (Конечный локальный IP-адрес)	**Local End IP** - это конечный локальный IP-адрес (ILA). Если правило действует для всех локальных IP-адресов, то начальный IP-адрес - 0.0.0.0, конечный - 255.255.255.255.	255.255.255.255
Global Start IP (Начальный глобальный IP-адрес)	Начальный глобальный IP-адрес (IGA). В случае динамического IP-адреса, в качестве **глобального начального адреса** введите 0.0.0.0.	0.0.0.0

Табл. 30-2 Правила преобразований адресов SUA

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Global End IP (Конечный глобальный IP-адрес)	Конечный глобальный IP-адрес (IGA).	
Type (Способ)	Способы преобразования адресов. Функция **Server** позволяет задавать множество серверов различных типов. См. далее примеры.	Server
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

Наборы преобразований адресов, определяемые пользователем

Перейдем к опции "1" в меню 15.1. Введите "1" для вывода этого меню на экран. Здесь приведены только различия с предыдущим меню. Заметим, что дополнительные поля **Action** и **Select Rule** означают, что в этом экране возможна конфигурация правил. Также следует обратить внимание, что символ [?] в поле **Set Name** означает, что это поле обязательно для заполнения и в него необходимо ввести имя набора.

```
                        Menu 15.1.1 - Address Mapping Rules

  Set Name= ACL Default Set

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

                  Action= Edit          Select Rule=

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

Рис. 30-6 Меню 15.1.1 - Набор ACL заданный по умолчанию

Если оставить поле Set Name (Имя набора) **незаполненным, весь набор будет полностью удален.**

Тип, локальный и глобальный начальный/конечный IP-адреса задаются в меню 15.1.1.1 (см. далее), их значения отображаются на этом экране.

Порядок выполнения правил

Задание правил необходимо, т.к. OMNI ADSL применяет эти правила в порядке, определенном пользователем. При нахождении правила, удовлетворяющего текущему пакету, OMNI ADSL выполняет соответствующее действие, при этом остальные правила игнорируются. Если перед очередным заданным правилом имеются пустые, то это правило сдвигается на соответствующее количество пустых номеров. Например, если в текущем наборе уже сконфигурированы правила 1 - 6 и необходимо сконфигурировать правило под номером 9. На экране с итоговым набором новое правило будет 7-м, а не 9-м.

Если удалить правило 4, правила под номерами с 5 по 7 передвинутся на одну позицию вверх, таким образом, правило 5-е становится 4-м, 6-е становится 5-м и 7-е - 6-м.

Табл. 30-3 Меню 15.1.1 - Первый набор

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Set Name (Имя набора)	Введите имя для данного набора правил. Это обязательное поле. Если оставить это поле незаполненным, набор будет удален.	ACL Default Set
Action (Активно)	По умолчанию задано **Edit**. **Edit** означает переход к редактированию выбранного правила (см. следующее поле). **Insert Before** означает "вставить новое правило перед выбранным". Правила, идущие за выбранным, таким образом, сдвинутся на одну позицию вниз. **Delete** означает удалить выбранное правило, таким образом, следующие за ним правила сдвинутся на одну позицию вверх. **None** означает "отключить опцию **Select Rule".**	**Edit**
Select Rule (Выбор правила)	После выбора одной из функций **Edit**, **Insert Before** или **Delete** в предыдущем поле, происходит переход к этому полю и предлагается выбрать правило, к которому применяется данное действие.	1

Для сохранения набора следует нажать [ENTER] **внизу экрана. Это необходимо также делать при любых изменениях в наборе, в том числе**

после удаления одного из правил. Если клавиша [ENTER] не была нажата, изменения не сохранятся.

Выбор функции **Edit** в поле **Action,** и затем выбор правила - выводят на экран следующее **Меню 15.1.1.1 - Правила преобразований адресов**, в котором можно редактировать каждое правило в отдельности и конфигурировать параметры **Type (Тип)**, **Local** и **Global Start/End IPs (Локальные и глобальные начальный/конечный IP-адреса)**.

Численное значение конечного IP-адреса должно быть больше значения соответствующего ему начального IP-адреса.

```
                    Menu 15.1.1.1 Address Mapping Rule

                    Type= One-to-One

                    Local IP:
                      Start=
                      End  = N/A

                    Global IP:
                      Start= 0.0.0.0
                      End  = N/A

                    Server Mapping Set= N/A


                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Рис. 30-7 Меню 15.1.1.1 - Редактирование/Конфигурирование отдельного правила в наборе

В следующей таблице приводится описание полей данного меню.

Табл. 30-4 Меню 15.1.1.1 - Редактирование/Конфигурирование отдельного правила в наборе

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Type (Метод)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите один из пяти методов преобразования. Эти методы преобразования обсуждались в главе об экранах NAT Web-конфигуратора. Тип **Server** позволяет задавать несколько серверов различного типа за пределами NAT для данного компьютера. Примеры см. в *разделе*	**One-to-One**

Табл. 30-4 Меню 15.1.1.1 - Редактирование/Конфигурирование отдельного правила в наборе

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
	30.5.3.	
Local IP (Локальный IP-адрес)	Для преобразования типа Server поля локальных IP-адресов **недоступны**; НЕОБХОДИМО заполнить поле "Глобальный IP-адрес".	
Start (Начальный локальный IP-адрес)	Начальный локальный IP-адрес (ILA).	0.0.0.0
End (Конечный локальный IP-адрес)	Конечный локальный IP-адрес (ILA). Если правило действительно для всех локальных IP-адресов, начальный адрес следует задать как 0.0.0.0, а конечный 255.255.255.255. Это поле **недоступно** для типов преобразований One-to-One и Server.	N/A
Global IP (Глобальный IP-адрес)		
Start (Начальный внутренний глобальный IP-адрес)	Начальный внутренний глобальный IP-адрес (IGA). В случае динамического IP-адреса в качестве **глобального начального адреса** введите 0.0.0.0. Заметим, что **начальный глобальный IP-адрес** может быть равен 0.0.0.0 только для типов **Many-to-One** и **Server**.	0.0.0.0
End (Конечный внутренний глобальный IP-адрес)	Конечный внутренний глобальный IP-адрес (IGA). Это поле **недоступно** для типов преобразований **One-to-One**, **Many-to-One** и **Server**.	N/A
Server Mapping Set (Набор преобразований адреса сервера)	Возможно только когда в поле **Type** установлено **Server**. Для активации набора сервера из меню 15.2 введите число в диапазоне от 1 до 10.	
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

30.4 Конфигурирование сервера NAT

Для конфигурирования сервера следует выполнить следующие действия:

Step 1. Введите "15" в главном меню для перехода к **Меню 15 - Настройка NAT.**

Step 2. Введите 2 для отображения **Меню 15.2 - Наборы сервера NAT**, показанного ниже.

```
                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:
```

Рис. 30-8 Меню 15.2 - Установка сервера NAT

Step 3. Введите 1 для перехода в **Меню 15.2.1 - Установка сервера NAT**, показанное ниже.

```
                Menu 15.2.1 - NAT Server Setup


  Rule   Start Port No.   End Port No.   IP Address
 ------------------------------------------------------
    1.     Default          Default        0.0.0.0
    2.       21               25           192.168.1.33
    3.       0                0            0.0.0.0
    4.       0                0            0.0.0.0
    5.       0                0            0.0.0.0
    6.       0                0            0.0.0.0
    7.       0                0            0.0.0.0
    8.       0                0            0.0.0.0
    9.       0                0            0.0.0.0
   10.       0                0            0.0.0.0
   11.       0                0            0.0.0.0
   12.       0                0            0.0.0.0

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

Рис. 30-9 Меню 15.2.1 - Установка сервера NAT

Step 4. Введите номер порта в незанятое поле **Start Port No**. Для переадресации только одного порта введите его адрес в поле **End Port No**. В случае нескольких в поле **End Port No** - внесите номер последнего порта .

Step 5. В поле **IP Address** введите внутренний IP-адрес сервера. На следующем рисунке изображен компьютер, функционирующий как сервер FTP, Telnet и SMTP (порт 21, 23 и 25) с адресом 192.168.1.33.

Step 6. По завершении определения серверов при появлении сообщения: "Press ENTER to confirm …", чтобы сохранить конфигурацию нажмите [ENTER]. Для отмены изменений в любой момент нажмите клавишу [ESC].

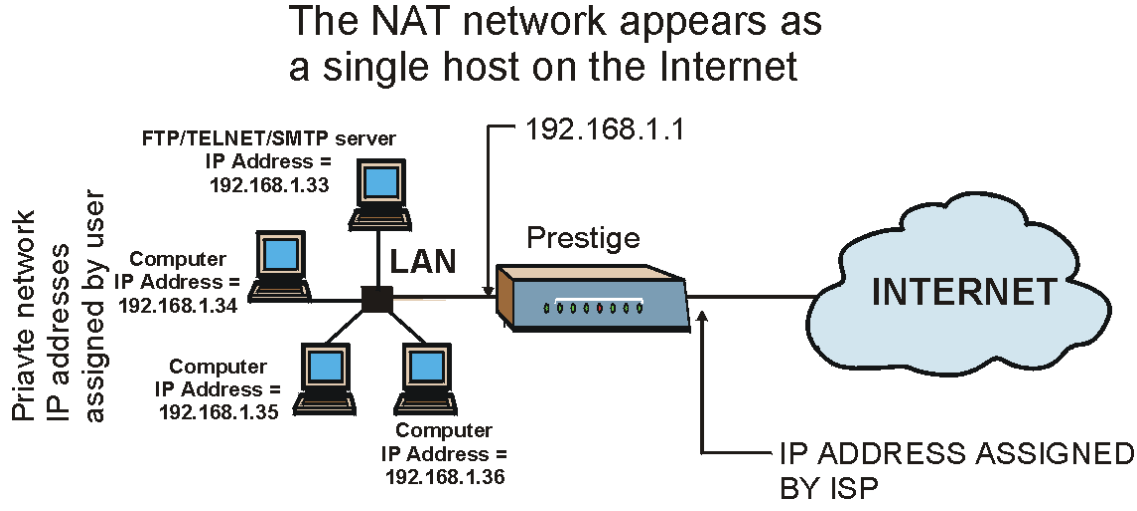


Рис. 30-10 Пример работы нескольких серверов за NAT

30.5 Общие примеры NAT

Ниже приведены несколько примеров конфигурации NAT.

30.5.1 Пример 1: Только доступ в Интернет

В следующем примере необходимо установить только одно правило, по которому все ILA (внутренние локальные адреса) преобразуются в один динамический IGA (внутренний глобальный адрес), назначаемый Интернет-провайдером.

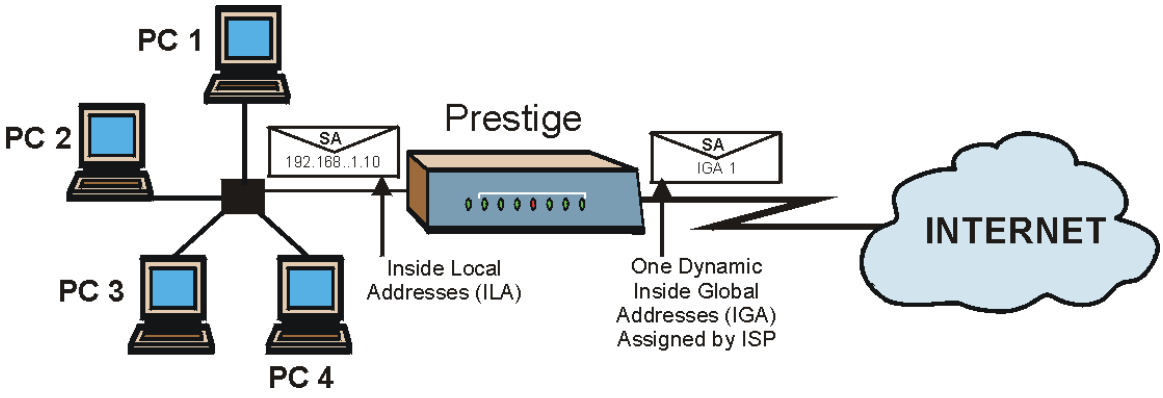


Рис. 30-11 NAT - Пример 1

```
        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:
```

Рис. 30-12 Меню 4 - Пример NAT для доступа в Интернет

В поле **Network Address Translation** в меню 4 выберите опцию **SUA Only**. Это преобразование вида Many-to-One, описанное в *разделе 30.5*. Не редактируемая опция **SUA Only** в поле **Network Address Translation** меню 4 и 11.3 специально предварительно сконфигурирована для этого случая.

30.5.2 Пример 2 Доступ в Интернет с внутреннего сервера

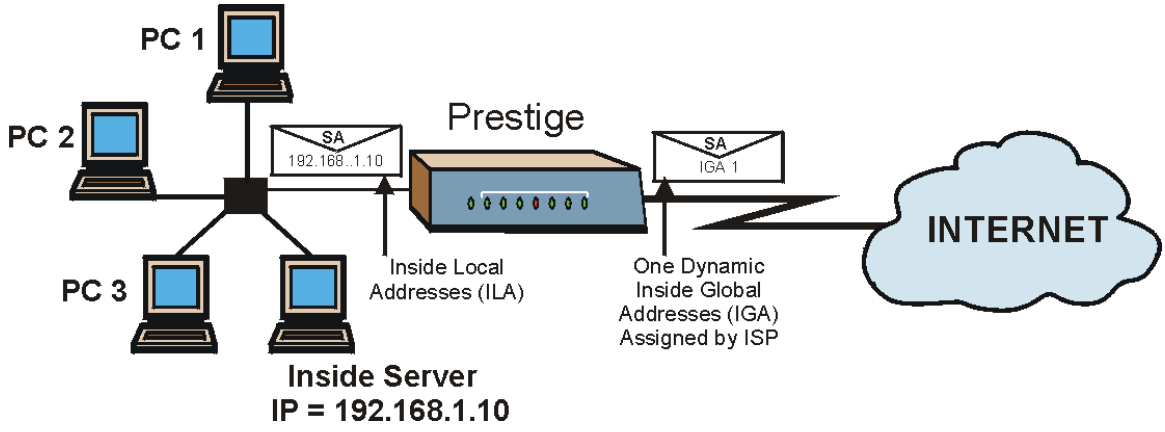


Рис. 30-13 NAT - Пример 2

В этом случае выполняются действия, аналогичные описанным выше (установить функцию **SUA Only**), и также осуществляется переход к меню 15.2 для назначения внутреннего сервера NAT, как показано на следующем рисунке.

```
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:
```

Рис. 30-14 Меню 15.2.1 - Назначение внутреннего сервера

30.5.3 Пример 3: Несколько общедоступных IP-адресов для локальной сети с внутренними серверами

В данном примере Интернет-провайдером используется 3 внутренних глобальных адреса (IGA). В организации имеется много отделов, но два из них пользуются собственным сервером FTP. Все подразделения используют один маршрутизатор. В примере резервируется один адрес IGA для каждого отдела с сервером FTP, а остальные отделы пользуются оставшимся адресом IGA. Требуется отобразить серверы FTP как первые два адреса IGA, а остальной трафик LAN - как оставшийся адрес IGA. Требуется отобразить третий адрес IGA как адрес внутреннего Web-сервера и почтового сервера. Для этого необходимо назначить четыре правила: два в двух направлениях и два в одном направлении, как показано ниже.

Rule 1. Отобразить первый IGA как первый внутренний FTP-сервер для трафика FTP в обоих направлениях (преобразование вида **1: 1**, назначение как локального, так и глобального IP-адреса).

Rule 2. Отобразить второй IGA как второй внутренний FTP-сервер для трафика FTP в обоих направлениях (преобразование вида **1 : 1**, назначение как локального, так и глобального IP-адреса).

Rule 3. Отобразить остальной исходящий трафик локальной сети как IGA3 (преобразования вида **Many : 1**).

Rule 4. Третий адрес IGA также отображается как Web-сервер и почтовый сервер LAN. Введение опции **Server** позволяет указать множество серверов различных типов как компьютеры, находящиеся за NAT локальной сети.

Ситуация, описанная в примере, может выглядеть следующим образом:

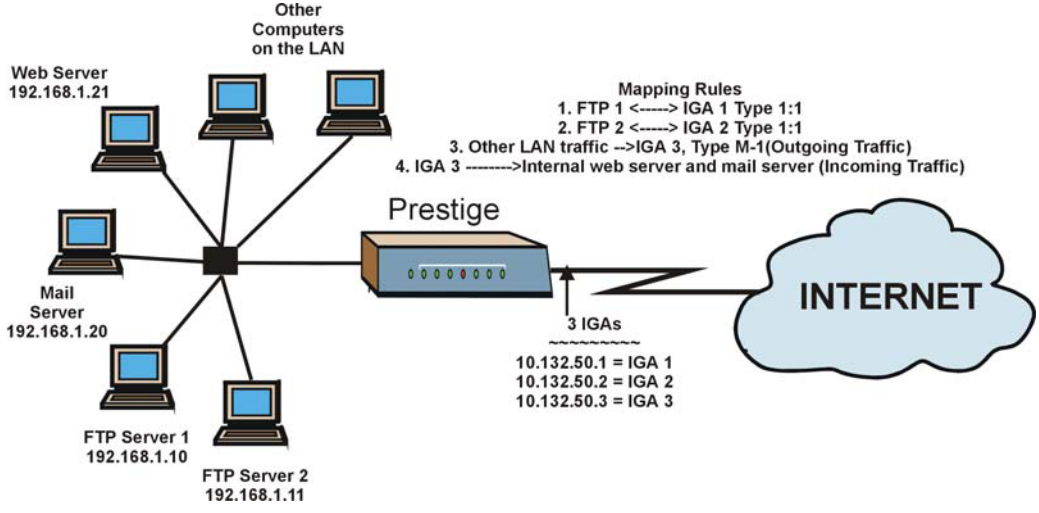


Рис 30-15 NAT - Пример 3

Step 1. В данном случае в **Меню 15.1 - Address Mapping Sets** необходимо сконфигурировать набор 1 преобразований адресов.В поле **Network Address Translation** (в меню 4 или 11.3) следует выбрать опцию **Full Feature** (см. *Рис.30-16*).

Step 2. Затем введите "15" в главном меню.

Step 3. Введите "1" для перехода к конфигурированию наборов преобразований адресов.

Step 4. Введите "1" для начала работы с новым набором. Введите имя набора, выберите **Edit Action**, и затем введите "1" в поле **Select Rule**. Нажмите [ENTER] для подтверждения.

Step 5. Выберите в поле **Type** вариант **One-to-One** (прямое преобразование для пакетов передаваемых в обоих направлениях), , и введите локальный начальный **IP-адрес** как 192.168.1.10 (IP-адрес FTP-сервера 1), а глобальный начальный **IP-адрес** как - 10.132.50.1 (первый IGA). (См. *Рис.30-17).*

Step 6. Повторите описанные выше действия применительно к правилам со 2 по 4.

Step 7. По окончании работы меню 15.1.1 должно выглядеть, как на .

```
            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:
```

Рис.30-16 Пример 3: Меню 11.3

На следующих рисунках показано, как сконфигурировать первое правило

```
                    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:

         Press Space Bar to Toggle.
```

Рис.30-17 Пример 3:Меню 15.1.1.1

```
                    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:
```

Рис.30-18 Пример 3: Окончательный вид меню 15.1.1

Теперь следует задать адрес IGA3 для его отображения также в качестве web-сервера и почтового сервера локальной сети.

Step 8. В главном меню выберите "15".

Step 9. Введите 2 в **Меню 15 - Установка NAT**.

Step 10. Введите 1 в **Меню 15.2 - Наборы серверов NAT** - для отображения следующего меню. Выполните конфигурацию как показано ниже.

```
                    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:
```

Пример 3: Меню 15.2.1

30.5.4 Пример 4: Прикладные программы, несовместимые с NAT

Некоторые приложения не поддерживают NAT-преобразование с использованием трансляции адресов портов TCP или UDP. В этом случае рекомендуется использовать преобразование адресов вида **Many-to-Many No Overload**, так как номера портов для преобразований типа **Many-to-Many No Overload** (и **One-to-One**) *не* меняются. Это иллюстрирует следующий рисунок.

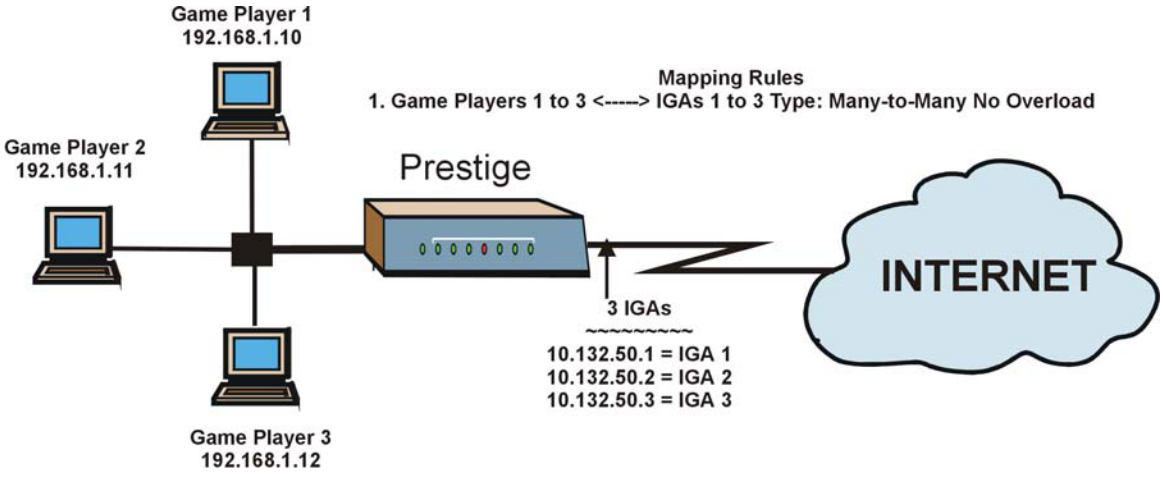


Рис 30-19 NAT - Пример 4

Некоторые приложения, например игровые программы, несовместимы с NAT, так как встраивают информацию по адресации в поток данных. Такие приложения не будут работать с NAT даже при использовании преобразований типа One-to-One **и** Many-to-Many No Overload**.**

Для работы в следующих двух меню следует выполнить действия, описанные ранее в примере 3.

```
                    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:
```

Рис.30-20 Пример 4: Menu 15.1.1.1 Address Mapping Rule

После окончания работы по конфигурированию этих параметров необходимо проверить установки в меню 15.1.1, как показано ниже.

```
                        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:
```

Рис.30-21 Пример 4: Меню 15.1.1 - Правила преобразований адресов

Part X:

Дополнительные функции управления системной консоли (SMT)

В этой части обсуждается настройка фильтрации, SNMP, система защиты, диагностика и получение информации о состоянии системы, микропрограммное обеспечение и файл конфигурации, сопровождение системы, дистанционное управление, маршрутизация на базе стратегии IP и расписание связи.

См. разделы данного руководства, посвященные описанию Web-конфигуратора, содержащие необходимую информацию о технических параметрах, задаваемых с его помощью и с помощью системной консоли.

Chapter 31
Конфигурирование фильтров

В данной главе описывается создание и применение фильтров.

31.1 О фильтрации

OMNI ADSL использует фильтры для принятия решения о разрешении или запрещении пересылки пакета данных и/или направлении вызова. Существует два варианта использования фильтров: для фильтрации данных и фильтрации вызовов. Фильтры подразделяются на фильтры устройств и фильтры протоколов. Оба типа фильтров будут рассмотрены ниже.

Фильтры данных сканируют данные, чтобы определить, следует ли разрешать пересылку пакета. Фильтры данных подразделяются на фильтры входящих данных и фильтры исходящих данных, в зависимости от направления пакета, относящегося к тому или иному порту. Фильтрация данных может быть применена как со стороны WAN, так и со стороны Ethernet. Фильтрация вызовов используется для определения, следует ли разрешать пакету инициировать вызов.

Исходящие пакеты должны сначала пройти фильтры данных, а затем фильтры вызовов. Фильтры вызовов делятся на две группы: встроенные фильтры вызовов и фильтры вызовов, определяемые пользователем. OMNI ADSL имеет встроенные фильтры вызовов, которые предотвращают инициирование вызовов административными пакетами, напр., RIP-пакетами. Эти встроенные фильтры всегда включены, и пользователь не может их изменить. Сначала OMNI ADSL применяет встроенные, а затем - пользовательские фильтры вызовов, если таковые имеются, как показано ниже.

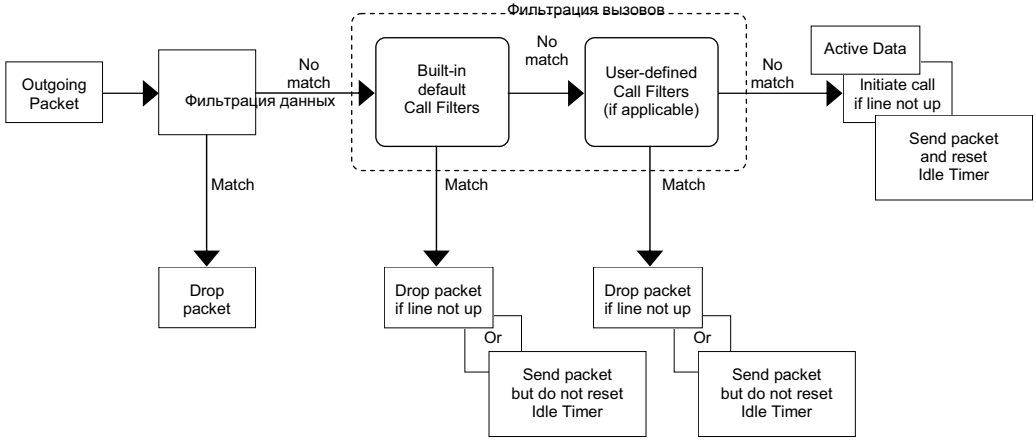


Рис. 31-1 Процесс фильтрации исходящего пакета

В Меню 21 изготовителем сконфигурированы по умолчанию два набора правил фильтра для предотвращения инициирования вызовов трафиком NetBIOS. Сводка по правилам фильтрации показана на следующих рисунках.

Этот рисунок иллюстрирует логическую схему реализации правила фильтра.

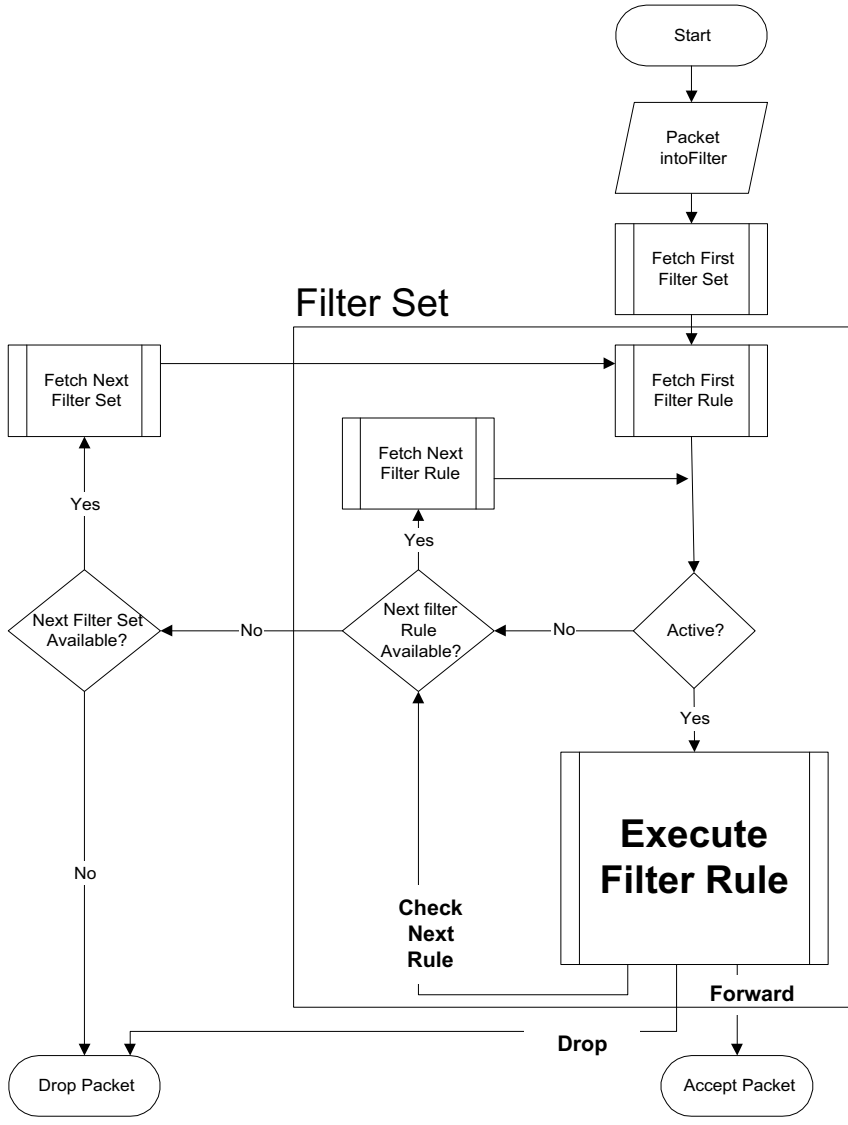


Рис. 31-2 Процесс реализации правила фильтра

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

Для входящих пакетов OMNI ADSL использует только фильтры данных. Пакеты обрабатываются в зависимости от того, достигнуто ли соответствие. В следующих разделах описывается, как сконфигурировать набор фильтров.

Структура фильтра OMNI ADSL

Набор фильтров состоит из одного или нескольких правил фильтра. В общем случае следует группировать связанные правила, напр., все правила для NetBIOS, в один набор и давать ему какое-либо идентифицирующее имя. Можно сконфигурировать до двенадцати наборов фильтров с шестью правилами в каждом наборе, итого 72 правила фильтра для системы.

31.2 Конфигурирование набора фильтров для моделей OMNI ADSL LAN H и OMNI ADSL LAN HW

Для конфигурирования набора фильтров следует выполнить описанные ниже операции.

Step 1. Введите в Главном меню "21" для перехода в **Меню 21 - Настройка фильтров и межсетевого экрана**.

Step 2. Введите "1" для перехода в **Меню 21.1 – Конфигурирование наборов фильтров** как показано ниже.

```
                    Menu 21.1 - Filter Set Configuration

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

                Enter Filter Set Number to Configure= 0

                Edit Comments= N/A

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

Рис. 31-3 Меню 21.1 - Конфигурирование наборов фильтров (P650H/HW)

Step 3. Введите номер набора фильтров, который нужно сконфигурировать (от 1 до 12), и нажмите клавишу [ENTER].

Step 4. Введите идентифицирующее имя или комментарий в поле **Edit Comments** и нажмите клавишу [ENTER].

Step 5. При появлении сообщения "Press [ENTER] to confirm…" нажмите клавишу [ENTER] для вывода **Меню 21.1.2 - Сводка по правилам фильтров** (в случае, если выбран набор фильтра 2 в Меню 21.1).

```
                    Menu 21.1.2 - Filter Rules Summary

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


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

Рис. 31-4 Сводка по правилам фильтров NetBIOS

```
                    Menu 21.1.3 - Filter Rules Summary

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

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

Рис. 31-5 Сводка по правилам фильтров NetBIOS_LAN

```
                    Menu 21.1.4 - Filter Rules Summary

# A Type                       Filter Rules                             M m n
- - ---- ------------------------------------------------------------ - - -
1 Y Gen  Off=0, Len=3, Mask=ffffff, Value=01005e                       N D F
2 N
3 N
4 N
5 N
6 N

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

Рис. 31-6 Сводка по правилам фильтров IGMP

31.3 Конфигурирование набора фильтров для моделей OMNI ADSL LAN R и OMNI ADSL LAN R-E

Для конфигурирования набора фильтров следует выполнить описанные ниже операции.

Step 1. В Главном меню введите "21" для перехода в **Меню 21 - Конфигурирование набора фильтров**.

```
                Menu 21 - Filter Set Configuration

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

              Enter Filter Set Number to Configure= 0

              Edit Comments= N/A

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

Рис. 31-7 Меню 21- Конфигурация набора фильтров (P650R и P650R-E)

Step 2. Введите номер набора фильтров, который нужно сконфигурировать (от 1 до 12), и нажмите клавишу [ENTER].

Step 3. Введите идентифицирующее имя или комментарий в поле **Edit Comments** и нажмите клавишу [ENTER].

Step 4. При появлении сообщения "Press [ENTER] to confirm…" нажмите клавишу [ENTER] для вывода **Меню 21.4 - Сводка по правилам фильтров** (в случае, если выбран набор фильтра 4 в Меню 21).

Для ознакомления со сводками по правилам NetBIOS WAN см. *Рис. 31-4* и *Рис. 31-5* - для NetBIOS LAN.

```
                    Menu 21.3 - 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:
```

Рис. 31-8 Сводка по правилам фильтра Telnet_WAN

```
                        Menu 21.4 - Filter Rules Summary

# A Type                          Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 Y Gen  Off=12, Len=2, Mask=ffff, Value=8863                               N F N
2 Y Gen  Off=12, Len=2, Mask=ffff, Value=8864                               N F D
3 N
4 N
5 N
6 N


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

Рис. 31-9 Сводка по правилам фильтра PPPoE

```
                        Menu 21.5 - Filter Rules Summary

# A Type                          Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 N
2 N
3 N
4 N
5 N
6 N


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

Рис. 31-10 Сводка по правилам фильтра FTP_WAN

31.3.1 Меню сводки по правилам фильтров

В приведенной ниже таблице дается краткое описание сокращений, использующихся в меню 21.1.x.

Табл. 31-1 Сокращения, используемые в Меню сводки правил фильтров

ПОЛЕ	ОПИСАНИЕ
#	Номер правила фильтров: от 1 до 6.
A	Active: “Y” означает, что правило фильтра активно. "N" означает, что правило фильтра неактивно.
Type	Тип правила фильтра: “GEN” для общего, “IP” для TCP/IP.
Filter Rules	Показывает параметры правила фильтра.

Табл. 31-1 Сокращения, используемые в Меню сводки правил фильтров

ПОЛЕ	ОПИСАНИЕ
M	More. "Y" означает, что есть еще правила для проверки, которые соединены с текущим правилом в цепочку правил. После того, как цепочка правил проверена, действие может быть выполнено. "N" означает, что правил для проверки больше нет. Можно задать действие, которое должно быть выполнено, напр., переслать пакет, сбросить пакет или проверить по следующему правилу. Что касается последнего варианта, то следующее правило не зависит от только что проверенного.
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, используемые для правил, зависящих от протокола, приведены ниже:

Табл. 31-2 Сокращения, используемые для правил фильтров

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

31.4 Конфигурирование правила фильтра

Для конфигурирования правила фильтра следует ввести его номер в **Меню 21.1.x - Сводка правил фильтров** - и нажать клавишу [ENTER], чтобы открыть Меню 21.1.x для данного правила.

Существует два вида правил фильтров: **TCP/IP и Generic (Общий)**. Некоторые параметры правил могут различаться в зависимости от типа правила. Нажатием клавиши [SPACE BAR] выберите тип правила, которое нужно создать в поле **Filter Type**, а затем нажмите клавишу [ENTER] для перехода в соответствующее меню.

Чтобы ускорить фильтрацию, все правила в наборе фильтров должны быть одного и того же класса, например, либо фильтрация протоколов, либо общая фильтрация. Класс набора фильтров определяется по первому созданному правилу. При применении наборов фильтров к порту одни пункты меню предназначены для наборов фильтров протоколов, а другие - для наборов фильтров устройств. Если набор фильтров для протоколов будет включен в поле набора фильтров для устройств или наоборот, OMNI ADSL предупредит об этом и блокирует сохранение.

31.4.1 Правило фильтра TCP/IP

В данном разделе описывается конфигурирование правила фильтра TCP/IP. Правила фильтра TCP/IP позволяют базировать правило на полях в заголовках IP и протоколов верхнего уровня, напр., UDP и TCP.

Для конфигурирования фильтра TCP/IP выберите правило фильтра TCP/IP в поле **Filter Type** и нажмите клавишу [ENTER] для перехода в **Меню 21.x.1 - Правило фильтра TCP/IP**, показанное ниже.

```
                        Menu 21.1.1.1 - TCP/IP Filter Rule

                    Filter #: 1,1
                    Filter Type= TCP/IP Filter Rule
                    Active= No
                    IP Protocol= 0      IP Source Route= No
                    Destination: IP Addr=
                                 IP Mask=
                                 Port #=
                                 Port # Comp= None
                         Source: IP Addr=
                                 IP Mask=
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= N/A
                    More= No            Log= None
                    Action Matched= Check Next Rule
                    Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Рис. 31-11 Меню 21.1.x.1 - Правило фильтра TCP/IP

В следующей таблице описывается конфигурирование правила фильтра TCP/IP.

Табл. 31-3 Меню 21.1.x.1 - Правило фильтра TCP/IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Filter # (Номер фильтра)	Набор фильтров и номер правила фильтра, напр., 2, 3 обозначает второй набор фильтров и третье правило фильтра второго набора.	1,1
Filter Type (Тип фильтра)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите правило. Параметры, отображаемые для каждого типа, могут различаться. Выберите одну из следующих опций: **TCP/IP Filter Rule (Правило фильтра TCP/IP)** или **Generic Filter Rule (Правило общего фильтра)**.	**TCP/IP Filter Rule**
Active (Активно)	Выберите **Yes** для включения или **No** для отключения правила фильтра.	**No** (по умолчанию)
IP Protocol (Протокол IP)	Протокол верхнего уровня, например, TCP - 6, UDP - 17, ICMP - 1. Значение должно быть в диапазоне от 0 до 255. Значение "0" соответствует опции - ANY protocol (любой протокол).	0 to 255

Табл. 31-3 Меню 21.1.x.1 - Правило фильтра TCP/IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
IP Source Route (Маршрут источника IP)	Маршрут источника IP является опциональным заголовком, определяющим маршрут, по которому пакет IP переправляется от источника в пункт назначения. Если установлено **Yes**, правило применимо к любому пакету, имеющему маршрут источника IP. Большинство IP-пакетов не имеют маршрута источника.	**No** (по умолчанию)
Destination: (Адресат:)		
IP Addr (IP-адрес)	Введите IP-адрес пункта назначения для фильтруемых пакетов. Данное поле игнорируется, если в нем установлено 0.0.0.0.	IP address
IP Mask (IP-маска)	Введите IP-маску для применения к полю Destination IP Addr.	IP mask
Port # (Номер порта)	Введите порт назначения для фильтруемых пакетов. Диапазон значений данного поля от 0 до 65535. Поле со значением 0 игнорируется.	0 to 65535
Port # Comp (Идентификатор сравнения порта)	Выберите идентификатор результата сравнения порта назначения пакета со значением, указанным в поле **Destination: Port #.** Возможные варианты - **Equal** (Равно), **Not Equal** (Не равно), **Less** (Меньше), **Greater** (Больше) или **None** (Нет).	**None**
Source (Источник):		
IP Addr (IP-адрес)	Введите IP-адрес источника для фильтруемых пакетов. Если установлено 0.0.0.0, данное поле игнорируется.	IP Address
IP Mask (IP-маска)	Введите IP-маску для применения к полю **Source: IP Addr.**	IP mask
Port # (Номер порта)	Введите порт источника для фильтруемых пакетов. Диапазон значений данного поля от 0 до 65535. Поле со значением 0 игнорируется.	0 to 65535
Port # Comp (Идентификатор сравнения порта)	Выберите идентификатор результатов сравнения порта источника пакета со значением, указанным в поле **Source: Port #.** Возможные варианты - **Equal** (Равно), **Not Equal** (Не равно), **Less** (Меньше), **Greater** (Больше) или **None** (Нет).	**None**

Табл. 31-3 Меню 21.1.x.1 - Правило фильтра TCP/IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
TCP Estab (Установлено TCP)	Применяется только если в поле IP Protocol field установлено 6 - TCP. Если задана опция **Yes,** правило соответствует пакетам, пытающимся установить соединение (я) TCP (SYN=1 и ACK=0); в противном случае правило игнорируется.	**No** (по умолчанию)
More (Продолжение списка)	Если установлено **Yes**, пакет, для которого достигнуто соответствие, передается на проверку по следующему правилу фильтра, перед тем как будут выполнены какие-либо действия; в противном случае пакет обрабатывается в соответствии с полями действий. Если для **More** установлено **Yes**, то поля **Action Matched** и **Action Not Matched** будут недоступны (N/A).	**No** (по умолчанию)
Log (Журнал)	Выберите функцию журнальной регистрации из следующего: **None** - Пакеты не регистрируются в журнальном файле. **Action Matched** - Регистрируются только пакеты, соответствующие параметрам правила. **Action Not Matched** - Регистрируются только пакеты, не соответствующие параметрам правила. **Both** – Все пакеты регистрируются в журнальном файле.	**None**
Action Matched (Действие при соответствии)	Выберите действие для пакета, соответствующего правилу. Возможные варианты - **Check Next Rule** (Проверить по следующему правилу), **Forward** (Переслать) или **Drop** (Сбросить).	**Check Next Rule** (по умолчанию)
Action Not Matched (Действие при несоответствии)	Выберите действие для пакета, для которого совпадение не произошло. Возможные варианты - **Check Next Rule** (Проверить по следующему правилу), **Forward** (Переслать) или **Drop** (Сбросить).	**Check Next Rule** (по умолчанию)
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

Следующий рисунок иллюстрирует логическую схему фильтра IP.

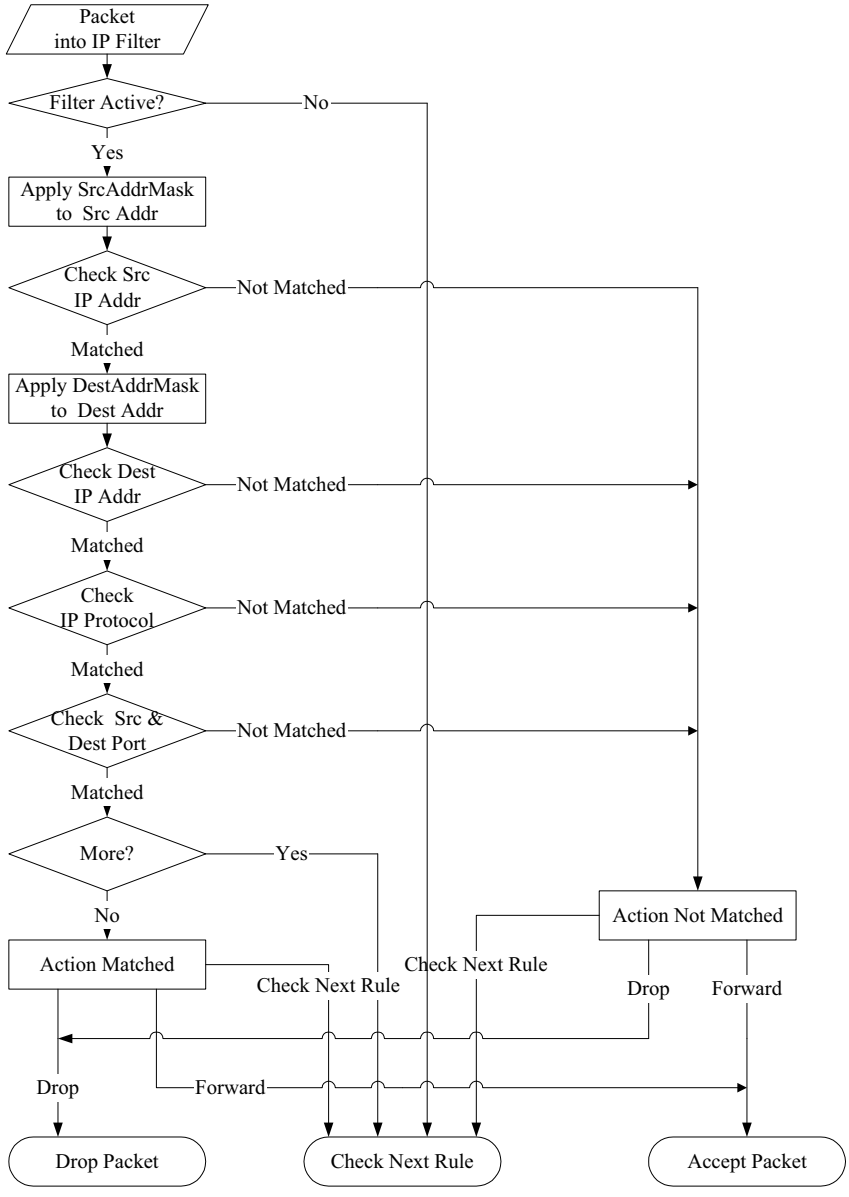


Рис. 31-12 Реализация фильтра IP

31.4.2 Правило общего фильтра

В данном разделе описывается конфигурирование правила общего фильтра. Общие фильтры служат для фильтрации пакетов, не относящихся к IP. Для пакетов IP проще использовать непосредственно правила для IP.

В случае общих правил OMNI ADSL обращается с пакетом, как с битовым потоком, в противоположность пакетам IP. Ту часть пакета, которая подлежит проверке, определяет поле **Offset** (от 0) и поле **Length**, оба измеряемые в байтах. OMNI ADSL применяет Mask (поразрядное осуществление операции "И") к блокам данных перед операцией сравнения результата со значением Value, для которого и определяется совпадение. В полях **Mask** (маска) и **Value (**значение) задаются шестнадцатиричные числа. Следует отметить, что для представления байта потребуются две шестнадцатиричные цифры, так что если в поле Length установлено 4, значение любого данного поля будет включать 8 разрядов (напр., FFFFFFFF).

Для того чтобы сгенерировать общее правило, выберите пустой набор фильтра в меню 21.1, например 6. Выберите **Generic Filter Rule (Правило общего фильтра)** в поле **Filter Type (Тип фильтра)** и нажмите клавишу [ENTER] для вызова **Меню 21.1.6.1 – Generic Filter Rule (Правило общего фильтра)**, показанного на следующем рисунке.

```
                  Меню 21.1.6.1 - Правило общего фильтра

                 Filter #: 6,1
                 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:

Press Space Bar to Toggle.
```

Рис. 31-13 Меню 21.1.6.1 - Правило общего фильтра

В следующей таблице описываются поля в Меню правила общего фильтра.

Табл. 31-4 Меню 21.1.6.1 - Правило общего фильтра

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Filter # (Номер фильтра)	Набор фильтров и номер правила фильтра, напр., 2, 3 обозначает второй набор фильтров и третье правило фильтра второго набора.	6,1
Filter Type (Тип фильтра)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите тип правила. Параметры, указываемые для каждого типа, могут различаться. Выберите одну из следующих опций: **Generic Filter Rule (Правило общего фильтра)** или **TCP/IP Filter Rule (Правило фильтра TCP/IP)**.	**Generic Filter Rule**
Active (Активно)	Выберите **Yes** для включения или **No** для выключения правила фильтра.	**No** (по умолчанию)
Offset (Смещение)	Введите начальный байт блока данных в пакете, для которого будет производиться сравнение. Диапазон значений данного поля от 0 до 255.	0 (по умолчанию)
Length (Длина)	Введите количество байтов для блока данных в пакете, для которого будет производиться сравнение. Диапазон значений от 0 до 8.	0 (по умолчанию)
Mask (Маска)	Введите маску (в шестнадцатиричной форме) для применения к блоку данных перед сравнением.	
Value (Значение)	Введите значение (в шестнадцатиричной форме) для сравнения с блоком данных.	
More (Продолжение списка)	Если установлено **Yes**, пакет, для которого достигнуто соответствие, передается на проверку по следующему правилу фильтра, перед тем как будут выполнены какие-либо действия; в противном случае пакет обрабатывается в соответствии с полями действий. Если для **More** установлено **Yes**, то поля **Action Matched** и **Action Not Matched** будут недоступны (**N/A**).	**No** (по умолчанию)
Log (Журнал)	Выберите функцию журнальной регистрации из следующего: **None** - Пакеты не регистрируются в журнальном файле. **Action Matched** – Регистрируются только пакеты, соответствующие параметрам правила. **Action Not Matched** - Регистрируются только пакеты, не соответствующие параметрам правила. **Both** – Все пакеты регистрируются в журнальном файле.	**None**
Action	Выберите действие для пакета, соответствующего правилу.	**Check Next**

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Matched (Действие при соответствии)	Возможные варианты - **Check Next Rule** (Проверить по следующему правилу), **Forward** (Переслать) или **Drop** (Сбросить).	**Rule** (по умолчанию)
Action Not Matched (Действие при несоответствии)	Выберите действие для пакета, для которого совпадение не произошло. Возможные варианты - **Check Next Rule** (Проверить по следующему правилу), **Forward** (Переслать) или **Drop** (Сбросить).	**Check Next Rule** (по умолчанию)
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

31.5 Типы фильтров и трансляция сетевых адресов

Существует два класса правил фильтра: **Generic Filter** Device rules (Правила общего фильтра устройств) и Protocol Filter (**TCP/IP**) (Правила фильтров протокола TCP/IP). Правила общих фильтров применяются к потоку данных между LAN и WAN. Правила фильтра протоколов применяются к пакетам IP.

Если функция NAT (Network Address Translation - Трансляция сетевых адресов) включена, внутренний IP-адрес и номер порта заменяются по принципу "от соединения к соединению", что делает невозможным знание точного адреса и порта на шине. Таким образом, OMNI ADSL применяет фильтры протоколов к "исконным" IP-адресам и номерам порта перед NAT - для исходящих пакетов и после NAT для входящих пакетов. С другой стороны, общие фильтры (или фильтры устройств), применяются к необработанным пакетам, которые появляются на шине. Они применяются к точкам входа, где OMNI ADSL получает или отправляет пакеты, например, к интерфейсу. Интерфейсом может быть Ethernet или любой другой аппаратный порт. Это иллюстрирует следующий рисунок.

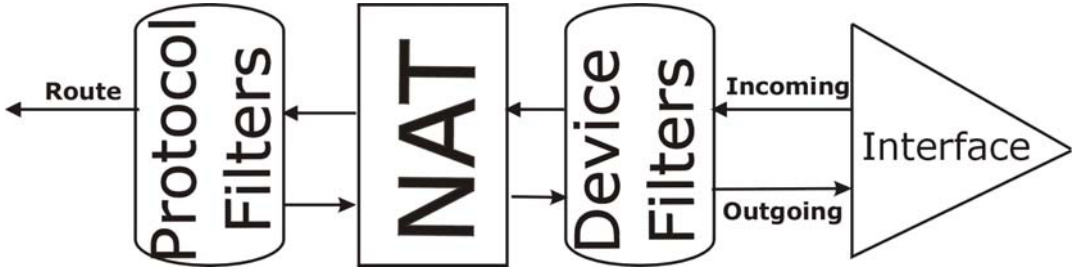


Рис. 31-14 Наборы фильтров протоколов и фильтров устройств

31.6 Пример фильтра

Рассмотрим пример, в котором блокируются попытки теледоступа к OMNI ADSL со стороны внешних пользователей.

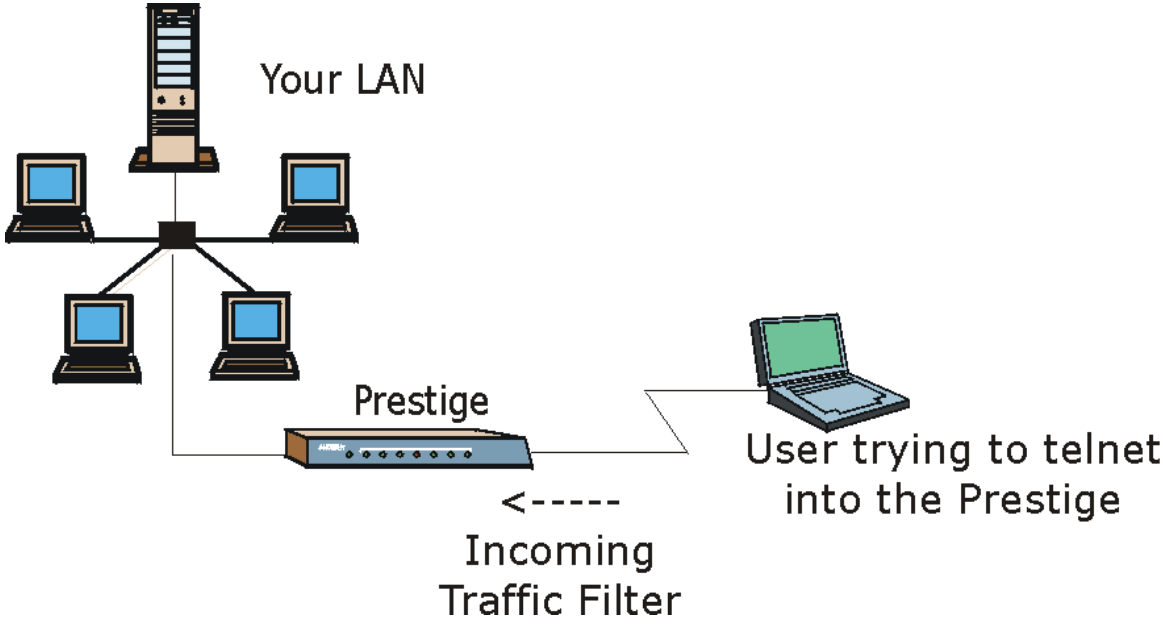


Рис. 31-15 Образец фильтра TELNET

Step 1. Введите "1" в меню 21 для вызова **Меню 21.1** — **Конфигурирование наборов фильтров**.

Step 2. Введите порядковый номер фильтра, который нужно сконфигурировать (в данном случае 6).

Step 3. Введите идентифицирующее имя или комментарий в поле **Edit Comments (Редактирование комментария)** (например, TELNET_WAN) и нажмите [ENTER].

Step 4. При появлении сообщения "Press [ENTER] to confirm or [ESC] to cancel" нажмите клавишу [ENTER] для перехода в **Меню 21.6** – **Сводка правил фильтра**.

Step 5. Введите "1" для конфигурирования первого правила фильтра. Сконфигурируйте параметры в Меню, как показано ниже.

При нажатии клавиши [ENTER] для подтверждения появляется следующая экранная форма. Следует отметить, что данный набор включает только одно правило фильтра.

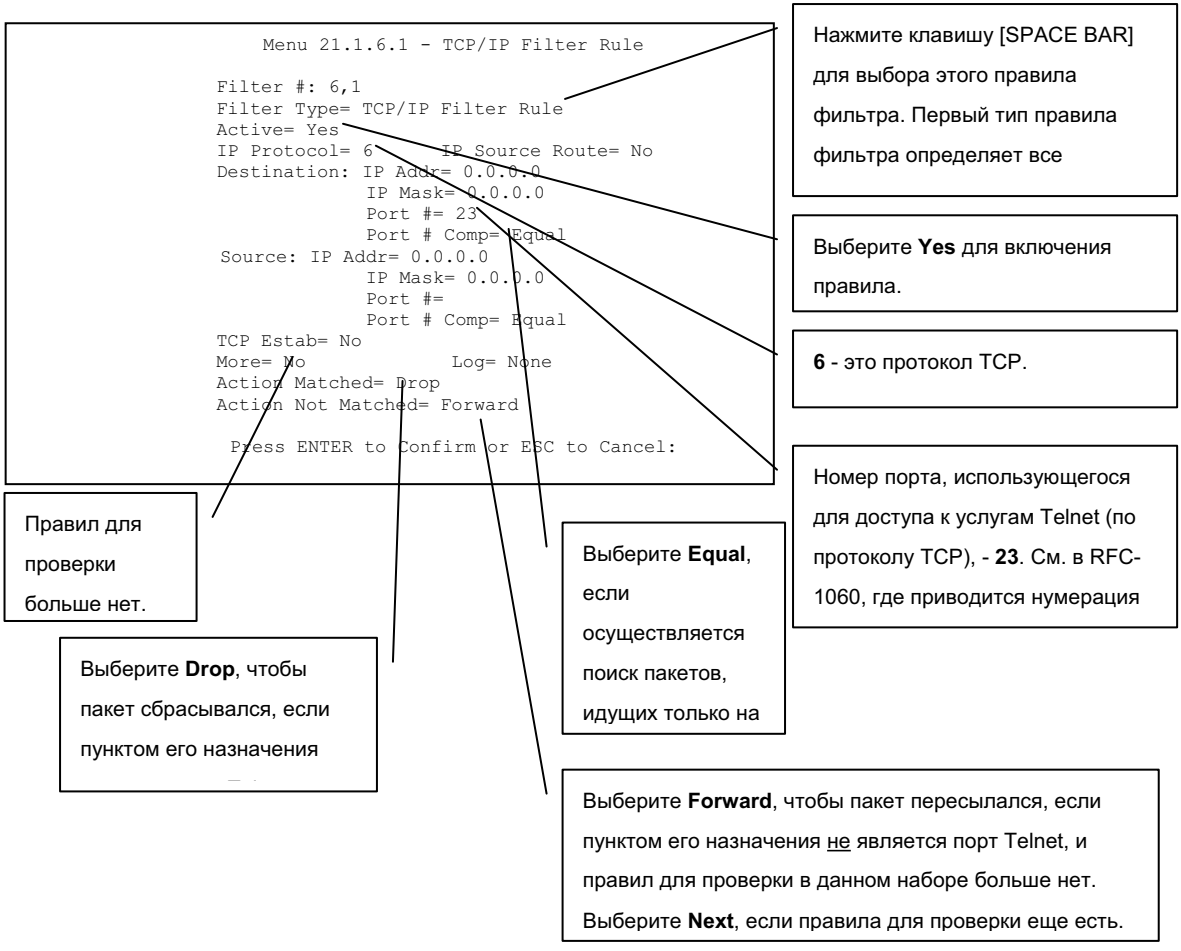


Рис. 31-16 Меню 21.1.6.1 - Образец фильтра

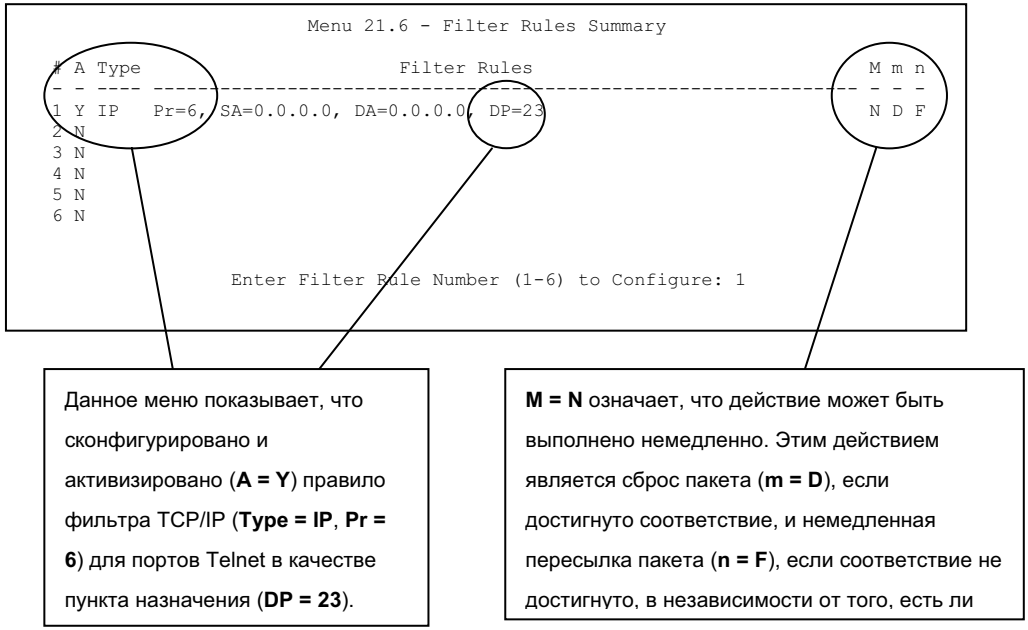


Рис. 31-17 Меню 21.1.6 - Образец сводки по правилам фильтров

После создания набора фильтров его нужно применить.

Step 1. Введите "11" в Главном меню для вызова меню 11 и наберите номер удаленного узла для редактирования.

Step 2. Перейдите к полю **Edit Filter Sets**, нажмите клавишу [SPACE BAR] для выбора **Yes**, а затем нажмите клавишу [ENTER].

Step 3. Происходит переход в Меню 11.5. Включите применение набора фильтров (напр., набора фильтров 3) в данном меню в соответствии с указаниями в следующем разделе.

31.7 Применение фильтров и заводские настройки по умолчанию

В данном разделе показано, где следует применять фильтр(-ы) после его (их) разработки. В Меню 21 изготовителем по умолчанию сконфигурированы (но не включено применение) наборы правил фильтров для фильтрации трафика.

Табл. 31-5 Таблица набора фильтров

НАБОРЫ ФИЛЬТРОВ	ОПИСАНИЕ
Input Filter Sets (Наборы входных фильтров):	Применить фильтры для входящего трафика. Можно применить фильтры протоколов или фильтры устройств. Более подробно о фильтрах см. в данной главе выше.
Output Filter Sets (Наборы выходных фильтров):	Применить фильтры для трафика, исходящего из OMNI ADSL. Можно применить фильтры протоколов или фильтры устройств. Более подробно о типах фильтров см. в данной главе выше.
Call Filter Sets (Наборы фильтров вызовов):	Применить фильтры для определения, следует ли разрешать пакету инициировать вызов.

31.7.1 Трафик Ethernet

Необходимость в фильтрации трафика Ethernet возникает редко; тем не менее, наборы фильтров могут быть полезными для блокировки отдельных пакетов, уменьшения объема трафика и предотвращения несанкционированного доступа. Перейдите в Меню 3.1 (показано ниже) и введите номер(-а) набора(-ов) фильтров, которые нужно применить, в соответствии с потребностью. Можно выбрать до четырех наборов фильтров (из двенадцати) путем ввода их номеров, разделенных запятыми, например, 2, 4, 6, 11. Набор фильтров, установленный изготовителем по умолчанию, NetBIOS_LAN, вставлен в поле **protocol filters** в составе **Input Filter** Sets в меню 3.1, с целью предотвращения генерирования вызовов на сервер DNS локальными сообщениями NetBIOS.

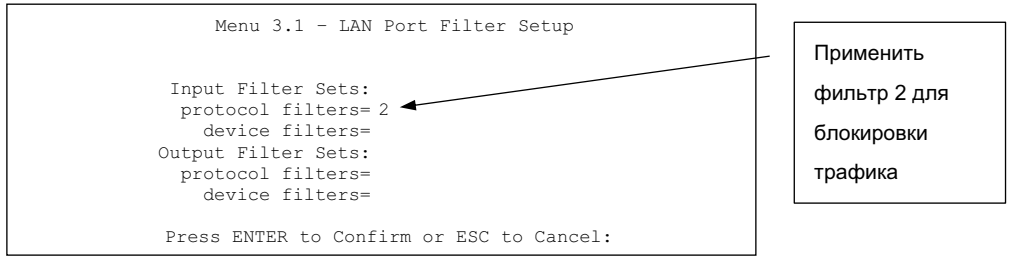


Рис. 31-18 Фильтрование трафика Ethernet

31.7.2 Фильтры для удаленного узла

Перейдите в Меню 11.5 (показано ниже) и введите номер(-а) набора(-ов) фильтров, в соответствии с необходимостью. Можно последовательно задать до четырех наборов фильтров, введя их номера через запятую. Чтобы заблокировать инициирование вызовов Интернет-провайдера локальным трафиком NetBIOS, в поле **protocol filters** под **Call Filter Sets** в меню 11.5 стоит заводской набор фильтров по умолчанию - NetBIOS_WAN.

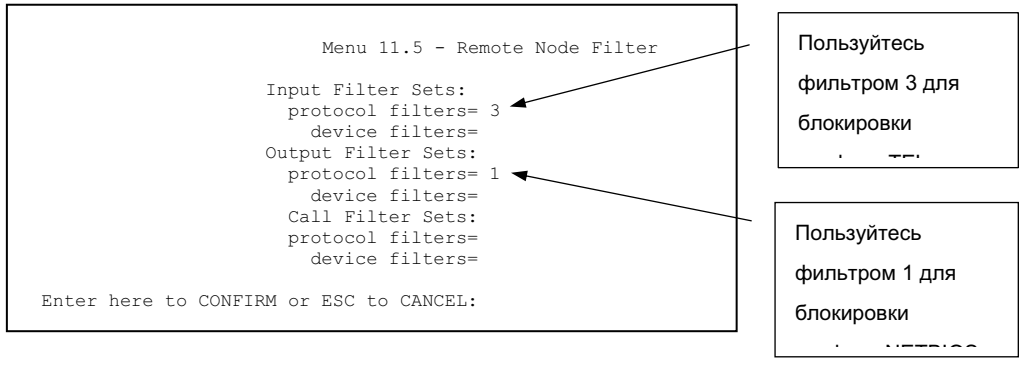


Рис. 31-19 Фильтрация трафика удаленного узла

Отметим, что наборы фильтров вызовов отображаются только если выбрана инкапсуляция PPPoA или PPPoE.

Chapter 32
Активизация межсетевого экрана

В данной главе дается информация о начале работы с межсетевым экраном OMNI ADSL. Межсетевой экран применяется в модели OMNI ADSL LAN H/HW.

32.1 Дистанционное управление и межсетевой экран

Если меню 24.11 системной консоли сконфигурировано для управления (см. главу *Remote Management (Дистанционное управление)*), а межсетевой экран включен:

- Межсетевой экран блокирует дистанционное управление из глобальной сети до тех пор, пока не будет установлено соответствующее правило его работы.
- Межсетевой экран позволяет осуществлять дистанционное управление из LAN.

32.2 Методы доступа

Наиболее полным средством конфигурации межсетевого экрана, из всех имеющихся у OMNI ADSL, является Web-конфигуратор. Поэтому рекомендуется настраивать межсетевой экран с помощью Web-конфигуратора (инструкции см. в следующих главах). Меню SMT позволяет активизировать межсетевой экран и просматривать журналы.

32.3 Активизация межсетевого экрана

В Главном меню введите "21" для перехода в **Меню 21 - Настройка фильтров и межсетевого экрана**.

Выберите опцию "2" в данном меню для вывода на экран следующего меню. Нажатием клавиши [SPACE BAR], а затем [ENTER] выберите **Yes** в поле **Active** для активизации сетевого экрана. Межсетевой экран необходимо включать для защиты от атак типа Denial of Service (DoS, отказ от обслуживания). Дополнительные правила можно задать через Web-конфигуратор.

```
                          Menu 21.2 - Firewall Setup

      The firewall protects against Denial of Service (DoS) attacks when
      it is active. The default Policy sets

          1. allow all sessions originating from the LAN to the WAN and
          2. deny all sessions originating from the WAN to the LAN

      You may define additional Policy rules or modify existing ones but
      please exercise extreme caution in doing so

          Active: ДА

          LAN-to-WAN Set Name: ACL Default Set
          WAN-to-LAN Set Name: ACL Default Set

      Please configure the Firewall function through Web Configurator.

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

Рис. 32-1 Меню 21.2 - Настройка межсетевого экрана

Для конфигурирования правил межсетевого экрана пользуйтесь Web-конфигуратором или командным процессором.

32.4 Просмотр журнала регистраций межсетевого экрана

В меню 21 введите "3" для просмотра журнала регистраций межсетевого экрана. Ниже приводится пример журнала регистрации межсетевого экрана.

```
#   Time       Packet Information                        Reason          Action
120|Jan 01 00 |From:192.168.17.1    To:192.168.17.255  |default policy  |block
   | 12:38:44 |UDP src port:00520   dest port:00520    |<2,00>          |
121|Jan 01 00 |From:192.168.1.1     To:192.168.11.33   |default policy  |forward
   | 07:39:25 |ICMP        type:00003      code:00001  |<0,00>          |


Clear Firewall Log (y/n):
```

Рис. 32-2 Пример журнала регистраций межсетевого экрана

Следующая таблица описывает поля данного меню.

Табл. 32-1 Журналы регистраций межсетевого экрана

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
# (Порядковый номер)	Порядковый номер журнальной записи. Возможен в пределах 128 записей с номерами от 0 до 127. Как только они будут использованы, заполнение журнала начинается с начала, при этом старые записи не сохраняются.	
Time (Время)	Время внесения записи в данном формате. Для правильного отображения времени Вам следует сделать настройку меню 24.10.	dd:mm:yy (дд:мм:гг), например, Jan 01 0; hh:mm:ss (чч:мм:сс), например, 00:04:28
Packet Information (Данные о пакете)	В этом поле содержатся следующие данные о пакете: IP-адреса отправителя и получателя, протокол и номера портов.	
Reason (Причина регистрации)	В этом поле указывается причина регистрации записи; т.е., соответствие или несоответствие правилу, или атака. Координаты набора и правила (<X, Y>, где X=1,2; Y=00~10), сопровождаемые кратким объяснением. Существует два набора стратегий; набор 1 (X = 1) для правил на направлении LAN - WAN и набор 2 (X = 2) для правил на направлении WAN - LAN. Y означает номер правила в наборе. Можно задавать до 10 правил в любом наборе (Y = 01 до 10). Правило под номером 00 означает правило по умолчанию.	not match <1,01> dest IP Это означает, что в данном пакете IP-адрес назначения не соответствует заданному в наборе 1 правилу 1. Другими причинами этой ситуации (кроме упомянутой выше) является несоответствие src IP (IP-адреса источника), dest port (номера порта назначения), src port (номера порта источника) и протокола.
	Регистрация атаки DoS.	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop или syn flood

Табл. 32-1 Журналы регистраций межсетевого экрана

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Action (Активно)	Пакет должен быть блокирован (т.е. просто удален), передан или ни то ни другое (**Block**, **Forward** или **None**). None означает, что данным правилом не предусмотрено никакое действие.	**Block**, **Forward** или **None**
После просмотра журнальной регистрации введите “y” для очистки или “n” для сохранения. После этого происходит возвращение в **Меню 21- Настройка фильтров и межсетевого экрана**.		

Chapter 33
Конфигурирование SNMP

В данной главе рассматривается Меню 22 - Конфигурирование SNMP.

33.1 Описание SNMP

Простой протокол сетевого управления представляет собой протокол, используемый для обмена информацией об управлении между сетевыми устройствами. SNMP является одним из элементов стека протоколов TCP/IP. OMNI ADSL поддерживает функциональные возможности агента SNMP, который позволяет отслеживать, как функционирует OMNI ADSL и управлять им через сеть. Маршрутизатор OMNI ADSL поддерживает первую и вторую версии SNMP: SNMPv1 и SNMPv2c. Следующий рисунок иллюстрирует функцию управления по протоколу SNMP. Протокол SNMP доступен только при сконфигурированном TCP/IP.

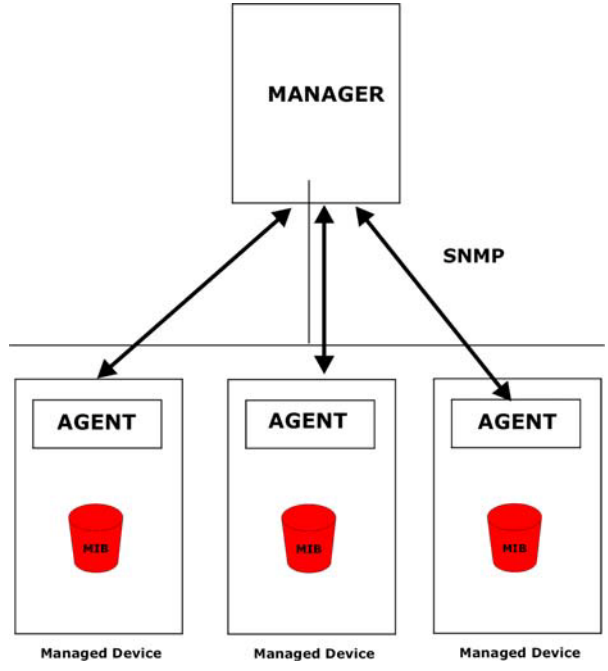


Рис. 33-1 Модель управления по протоколу SNMP

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

Агент представляет собой модуль программы управления, находящийся в управляемом устройстве (OMNI ADSL). Агент преобразует локальную информацию об управлении, получаемую от управляемого устройства, в форму, совместимую с протоколом SNMP. В качестве управляющей станции выступает консоль, с которой сетевые администраторы выполняют функции управления сетью. С нее выполняются операции по управлению и контролю управляемых устройств.

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

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

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

33.2 Поддерживаемые базы управляющей информации

OMNI ADSL поддерживает базы по протоколу RFC-1215 и MIB II, как определенные протоколом RFC-1213, также как частные базы управляющей информации ZyXEL . В основном, базы управляющей информации предназначены для того, чтобы сетевые администраторы могли собирать статистические данные и контролировать состояние и производительность сети.

33.3 Конфигурирование SNMP

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

```
                    Menu 22 - SNMP Configuration

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


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

Рис. 33-2 - Меню 22 - Конфигурирование SNMP

В следующей таблице описываются параметры конфигурирования SNMP.

Табл. 33-1 Меню 22 - Конфигурирование SNMP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
SNMP:		
Get Community (Ввод пароля Get)	Введите пароль **Get** для входящих запросов "Get" и "GetNext" от управляющей станции.	public
Set Community (Ввод пароля Set)	Введите пароль **Set** для входящих запросов "Set" от управляющей станции.	public
Trusted Host (Доверенный хост)	Если вводится доверенная хост-машина (trusted host), OMNI ADSL будет отвечать только на сообщения SNMP с данного адреса. Если оставить это поле пустым, OMNI ADSL будет отвечать на все сообщения SNMP, полученные им, независимо от их источника.	0.0.0.0
Trap (Прерывание):		
Community (Ввод пароля)	Введите пароль "Trap", посылаемый с каждым прерыванием на управляющую станцию SNMP.	public
Destination (IP-адрес назначения)	Введите IP-адрес станции, на которую должны посылаться прерывания SNMP.	0.0.0.0
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

33.4 Прерывания SNMP

OMNI ADSL должен посылать прерывания на управляющую станцию SNMP, если произошло какое-либо из следующих событий:

Табл. 33-2 Прерывания SNMP

НОМЕР ПРЕРЫВАНИЯ #	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
1	coldStart (определено в RFC-*1215*)	Прерывание посылается после загрузки (включения питания).
2	warmStart (определено в RFC-*1215*)	Прерывание посылается после загрузки (загрузки программного обеспечения).
3	linkDown (определено в RFC-*1215*)	Прерывание отправляется, если порт не подключен к сети.
4	linkUp (определено в RFC-*1215*)	Прерывание отправляется, если порт подключен к сети.
5	authenticationFailure (определено в RFC-*1215*)	Прерывание посылается на управляющую станцию при получении запросов get или set SNMP с неверным паролем.
6	whyReboot (определено в MIB ZYXEL)	Прерывание посылается с кодом причины перезапуска перед перезагрузкой, если система собирается перезапускаться ("горячий" запуск).
6a	Для преднамеренной перезагрузки:	Прерывание посылается с сообщением "System reboot by user!" (перезагрузка системы пользователем) при неслучайной перезагрузке системы (например, загрузка новых файлов, интерпретируемая команда "sys reboot" и т.д.).

В следующей таблице показано соответствие физических портов и типов инкапсуляции типам интерфейса.

Табл. 33-3 Порты и типы интерфейса

ФИЗИЧЕСКИЙ ПОРТ/ИНКАПСУЛЯЦИЯ	ТИП ИНТЕРФЕЙСА
Порты LAN	enet0
Радиопорты	enet1

ФИЗИЧЕСКИЙ ПОРТ/ИНКАПСУЛЯЦИЯ	ТИП ИНТЕРФЕЙСА
Инкапсуляция PPPoE	PPPoE
Инкапсуляция 1483	mpoa
Инкапсуляция Ethernet	Инкапсуляция ENET
PPPoA	PPP

Chapter 34
System Security (Система защиты)

В этой главе описывается, как осуществить настройку системы защиты на маршрутизаторе OMNI ADSL. Содержание данной главы относится только к моделям OMNI ADSL LAN H и OMNI ADSL LAN HW.

34.1 Описание системы защиты

В меню 23 можно сконфигурировать системный пароль, внешний сервер RADIUS и функции протокола IEEE802.1x.

34.1.1 Системный пароль

Введите "1" в Главном меню для вызова Меню **23 - Система защиты** .

Рекомендуется поменять пароль, заданный по умолчанию. Если Вы забыли пароль, заданный по умолчанию, следует восстановить файл конфигурации, заданной по умолчанию. См. раздел об изменении системного пароля в главе *Знакомство с системной консолью (SMT)* и раздел о сбросе настроек OMNI ADSL в главе *Знакомство с Web-конфигуратором*.

```
Menu 23 - System Security

    1. Change Password
    2. RADIUS Server

    4. IEEE802.1x
```

Рис. 34-1 Меню 23 - Система защиты

34.1.2 Конфигурирование внешнего сервера RADIUS

Введите "2" в **Меню 23 - Система защиты** для вызова **Меню 23.2 - Система защиты - сервер RADIUS**.

```
Меню 23 - "Система защиты"

    1. Change Password
    2. RADIUS Server

    4. IEEE802.1x
```

Рис. 34-2 Меню 23 - Система защиты

```
Menu 23.2 - System Security - RADIUS Server

 Authentication Server:
   Active= No
   Server Address= 10.11.12.13
   Port #= 1812
   Shared Secret= ********

 Accounting Server:
   Active= No
   Server Address= 10.11.12.13
   Port #= 1813
   Shared Secret= ********


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

Рис. 34-3 Меню 23.2 - Система защиты: сервер RADIUS

Следующая таблица описывает поля данного меню.

Табл. 34-1 Меню 23.2 - Система защиты: сервер RADIUS

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Authentication Server (Сервер аутентификации)		
Active (Активно)	Нажатием клавиши [SPACE BAR] выберите **Yes** и нажмите клавишу [ENTER] для включения функции аутентификации пользователя с помощью внешнего сервера аутентификации.	**No**
Server Address (Адрес сервера)	Введите IP-адрес внешнего сервера аутентификации в десятичном виде с разделительными точками.	10.11.12.13
Port # (Номер порта)	По умолчанию номер порта RADIUS-сервера аутентификации принимается равным **1812**. Не следует менять этот параметр без получения дополнительных инструкции и необходимой информации у Вашего системного администратора.	**1812**
Shared Secret (Общий ключ)	Укажите пароль (до 31 буквенно-цифровых символа), который будет использоваться как общий ключ внешним сервером аутентификации и точкой доступа. Значение ключа не может передаваться по сети. Значение ключа должно быть одинаковым для внешнего сервера аутентификации и устройства OMNI ADSL.	
Accounting Server (Сервер учета работы пользователей)		

Табл. 34-1 Меню 23.2 - Система защиты: сервер RADIUS

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Active (Активно)	Нажатием клавиши [SPACE BAR] выберите **Yes** и нажмите клавишу [ENTER] для включения функции аутентификации пользователя с помощью внешнего сервера учета работы пользователей.	**No**
Server Address (Адрес сервера)	Введите IP-адрес внешнего сервера учета работы пользователей в десятичном виде с разделительными точками.	10.11.12.13
Port # (Номер порта)	По умолчанию номер порта RADIUS-сервера учета работы пользователей принимается равным **1813**. Не следует менять этот параметр без получения дополнительных инструкции и необходимой информации у Вашего системного администратора.	**1813**
Shared Secret (Общий ключ)	Укажите пароль (до 31 буквенно-цифровых символа), который будет использоваться как общий ключ внешним сервером учета работы пользователей и точкой доступа. Значение ключа не может передаваться по сети. Значение ключа должно быть одинаковым для внешнего сервера учета работы пользователей и устройства OMNI ADSL.	
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.		

34.1.3 Протоколы IEEE802.1x

Стандарт IEEE802.1x описывает улучшенные методы защиты применительно к аутентификации беспроводных станций и управлению ключами криптографической защиты.

Выполните следующие действия для включения функции аутентификации EAP на устройстве OMNI ADSL.

Step 1. Введите в Главном меню "23" для вызова **Меню 23 – Система защиты**.

```
Menu 23 - System Security

    1. Change Password
    2. RADIUS Server

    4. IEEE802.1x
```

Рис. 34-4 Меню 23 - Система защиты

Step 2. Введите "4" для вызова **Меню 23.4 – Система защиты – IEEE802.1x**.

```
                Menu 23.4 - System Security - IEEE802.1x

    Wireless Port Control= Authentication Required
    ReAuthentication Timer (in second)= 1800
    Idle Timeout (in second)= 3600

    Authentication Databases= Local User Database Only


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

Рис. 34-5 Меню 23.4 - Система защиты: Протоколы IEEE802.1x

Следующая таблица описывает поля данного меню.

Табл. 34-2 Меню 23.4 - Система защиты: Протоколы IEEE802.1x

ПОЛЕ	ОПИСАНИЕ
Wireless Port Control (Управление радиопортом)	Нажатием клавиши [SPACE BAR] выберите режим защиты для доступа к беспроводной LAN. Выбор **No Authentication Required (Аутентификация не требуется)** разрешает доступ любого клиента к Вашей проводной сети без ввода имени пользователя и паролей. Данная установка задается по умолчанию. Выбор опции **Authentication Required (Требуется аутентификация)** означает, что клиенты для получения разрешения на доступ в проводную сеть должны указать имя пользователя и пароль. Выбор опции **No Access Allowed (Доступ закрыт)** блокирует доступ всех клиентов к проводной сети.
ReAuthentica-tion Timer (in seconds) (Таймер повторной аутентификации, в секундах)	Определяет частоту подтверждения имени пользователя и пароля для сохранения подключения к проводной сети. Эти поля будут активизированы только при выборе опции **Authentication Required** в поле **Wireless Port Control**. Введите значение временного интервала в диапазоне от 10 до 9999 (в секундах). По умолчанию значение временного интервала принимается равным **1800** секунд (30 минут).
Idle Timeout (Время простоя)	OMNI ADSL автоматически производит отключение клиента от проводной сети через определенное время . Клиенту необходимо повторно ввести имя пользователя и пароль, чтобы ему был разрешен доступ к проводной сети. Эти поля будут активизированы только при выборе опции **Authentication Required** в поле **Wireless Port Control**. По умолчанию значение временного интервала принимается равным **3600** секунд (1 час).

Табл. 34-2 Меню 23.4 - Система защиты: Протоколы IEEE802.1x

ПОЛЕ	ОПИСАНИЕ
Authentication Databases (Базы данных аутентификации)	Эти поля будут активизированы только при выборе опции **Authentication Required** в поле **Wireless Port Control**. База данных аутентификации содержит регистрационные сведения о беспроводных станциях. Локальная база данных о пользователях является встроенной базой данных устройства OMNI ADSL. RADIUS-сервер является для нее внешним. Заполните это поле для указания, какой базой данных следует пользоваться (в первую очередь) устройству OMNI ADSL для аутентификации беспроводной станции. Перед определением приоритетности, убедитесь в том, что Вы правильно подключили (в качестве первой) соответствующую базу данных. Выберите опцию **Local User Database Only (Только локальная база данных о пользователе)** для того чтобы OMNI ADSL выполнил проверку имени пользователя и пароля беспроводной станции, пользуясь только встроенной базой данных о пользователе устройства OMNI ADSL. Выберите опцию **RADIUS Only (Только RADIUS-сервер)** для того, чтобы OMNI ADSL выполнил проверку имени пользователя и пароля беспроводной станции, пользуясь только базой данных о пользователе на указанном RADIUS-сервере. Выберите опцию **Local first, then RADIUS (Вначале локальная БД, а затем БД RADIUS-сервера)** для того, чтобы OMNI ADSL при аутентификации беспроводной станции вначале выполнил проверку, пользуясь своей базой данных. Если имя пользователя в базе данных не обнаружено, то OMNI ADSL приступает к проверке по базе данных на указанном RADIUS-сервере. Выберите опцию **RADIUS first, then Local** (Вначале БД RADIUS-сервера, а затем локальная БД), чтобы OMNI ADSL при аутентификации беспроводной станции вначале выполнил проверку, пользуясь базой данных RADIUS-сервера. Если имя пользователя в базе данных RADIUS-сервера не обнаружено или пароль не совпадает с хранящимся в базе данных RADIUS-сервера, OMNI ADSL не будет обращаться для проверки к локальной базе данных пользователя и аутентификация прерывается. Если RADIUS-сервер недоступен для устройства OMNI ADSL, то OMNI ADSL выполняет проверку, пользуясь своей локальной базой данных о пользователе.
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.	

Если включена функция аутентификации пользователя, следует указать внешний сервер RADIUS или создать в OMNI ADSL локальные учетные записи пользователя для аутентификации.

34.2 Создание учетной записи пользователя в устройстве OMNI ADSL

Организация хранения сведений о настройках пользователя в ЛВС позволяет устройству OMNI ADSL выполнять аутентификацию без обращения к сети RADIUS-сервера.

Выполните следующие действия, как указано ниже, для установки настроек пользователя в устройстве OMNI ADSL.

Step 1. В главном меню введите "14" для вызова **Меню 14 - Настройка удаленного коммутируемого пользователя**.

```
                    Menu 14 - Dial-in User Setup

   1. ________      9. ________      17. ________      25. ________
   2. ________      10. ________     18. ________      26. ________
   3. ________      11. ________     19. ________      27. ________
   4. ________      12. ________     20. ________      28. ________
   5. ________      13. ________     21. ________      29. ________
   6. ________      14. ________     22. ________      30. ________
   7. ________      15. ________     23. ________      31. ________
   8. ________      16. ________     24. ________      32. ________

                      Enter Menu Selection Number:
```

Рис. 34-6 Меню 14 - Настройка удаленного коммутируемого пользователя

Step 3. Введите номер и нажмите клавишу [ENTER] для редактирования настройки пользователя.

```
                     Menu 14.1 - Edit Dial-in User

                    User Name= test
                    Active= Yes
                    Password= ********

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

Рис. 34-7 Меню 14.1 - Редактирование настройки коммутируемого пользователя

Следующая таблица описывает поля данного меню.

Табл. 34-3 Меню 14.1 - Редактирование настройки коммутируемого пользователя

ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите имя пользователя (до 31 буквенно-цифрового символа), использующееся в его настройке. Это поле чувствительно к регистру.
Active (Активно)	Нажатием клавиши [SPACE BAR] выберите **Yes** и нажмите [ENTER] для включения настройки пользователя.
Password (Пароль)	Введите пароль (до 31 символа), использующийся в настройке пользователя.
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.	

Chapter 35
Информация о системе и диагностика

В данной главе рассматривается информация о системе и средства диагностики, содержащиеся в Меню SMT с 24.1 по 24.4.

35.1 Описание сопровождения системы

Средства диагностики включают в себя функции обновления статуса системы, статуса порта, журнальной регистрации и трассировки, а также обновления системного программного обеспечения. Далее в настоящей главе эти функции описываются более подробно.

Введите "24" в Главном меню для перехода в **Меню 24 – Сопровождение системы**, показанное на следующем рисунке.

```
Menu 24 - System Maintenance


1.  System Status
2.  System Information и Console Port Speed
3.  Log и 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. 35-1 Меню 24 - Сопровождение системы

35.2 Статус системы

При выборе первого пункта - "Статус системы" - выводится информация о статусе и статистике портов, как показано ниже. Системный статус является средством, которое используется для отслеживания функционирования OMNI ADSL. В частности, в нем указывается статус телефонной линии ADSL, и количество посланных и полученных пакетов.

Для доступа к статусу системы в главном меню следует ввести "24", чтобы открыть **Меню 24** – **Сопровождение системы**. В данном меню введите "1" для выбора **. System Status (Статус системы)**. В **Меню 24.1 - System Maintenance - Status** (Сопровождение системы - статус) есть две команды. Ввод "1" вызывает сброс счетчиков; нажатием клавиши [ESC] осуществляется вызов предыдущего экрана.

```
                        Menu 24.1 - System Maintenance - Status          hh:mm:ss
                                                                  Sat. Jan. 01, 2000

 Node-Lnk    Status         TxPkts     RxPkts     Errors   Tx B/s   Rx B/s      Up Time
   1-ENET      Up              211          0          0        0        0      0:26:20
   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):

    Ethernet:                                        WAN:
      Status: 10M/Half Duplex          Tx Pkts: 53      Line Status: Up
      Collisions: 0                    Rx Pkts: 36      Upstream Speed:     0 Kbps
    CPU Load= 3.8%                                      Downstream Speed:     0 Kbps



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

Рис. 35-2 Меню 24.1 - Сопровождение системы - Статус

В следующей таблице описываются поля, содержащиеся в **Меню24.1 - Сопровождение системы** – **Статус**, которые предназначены ТОЛЬКО ДЛЯ ЧТЕНИЯ и используются исключительно в целях диагностики.

Табл. 35-1 Меню 24.1 - Сопровождение системы - Статус

ПОЛЕ	ОПИСАНИЕ
Node-Lnk	Индекс удаленного узла и тип связи. Типы связи: PPP, ENET, 1483.
Status	Статус удаленного узла.
TxPkts	Количество пакетов, переданных данному удаленному узлу.
RxPkts	Количество пакетов, принятых от данного удаленного узла.

Табл. 35-1 Меню 24.1 - Сопровождение системы - Статус

ПОЛЕ	ОПИСАНИЕ
Errors	Количество пакетов с ошибкой в рамках данного соединения.
Tx B/s	Скорость передачи в байтах в секунду.
Rx B/s	Скорость приема в байтах в секунду.
Up Time	Время, в течение которого данный канал был соединен с текущим удаленным узлом.
My WAN IP (from ISP)	IP-адрес удаленного узла Интернет-провайдера.
Ethernet	Статистика по локальной сети.
Status	Текущий статус ЛВС.
Tx Pkts	Количество пакетов, переданных в LAN.
Rx Pkts	Количество пакетов, полученных из LAN.
Collision	Количество коллизий.
WAN	Статистика по порту WAN.
Line Status	Текущий статус линии xDSL, который может быть "Up" (Включена) или "Down" (Отключена).
Upstream Speed	Скорость исходящего потока данных в кбит/с.
Downstream Speed	Скорость входящего потока данных в кбит/с.
CPU Load (Загрузка CPU)	Загрузка процессора в процентах.

35.3 Информация о системе

Для перехода в меню System Information (Информация о системе):

Step 1. Введите "24" в Главном меню для вызова **Меню 24 — Сопровождение системы**.

Step 2. Введите "2" для вызова **Меню 24.2 — Информация о системе**.

Step 3. Из данного меню существует два пути, как показано на следующем рисунке.

```
Menu 24.2 - System Information and Console Port Speed
      1. System Information
      2. Console Port Speed



            Please enter selection:
```

Рис. 35-3 Меню 24.2 - Информация о системе и скорость консольного порта

35.3.1 Информация о системе

Введите "1" в Меню 24.2 для вывода следующей экранной формы.

```
Menu 24.2.1 - Сопровождение системы - Информация

  Name:
  Routing: IP
  ZyNOS F/W Version: V3.40(IS.3) | 8/11/2003
  ADSL Chipset Vendor: Alcatel, Version  3.9.122
  Standard: Multi-Mode

  LAN
    Ethernet Address: 00:a0:c5:8d:dd:dc
    IP Address (IP-АДРЕС): 192.168.1.1
    IP Mask: 255.255.255.0
    DHCP: Server

         Press ESC or RETURN to Exit:
```

Рис. 35-4 Меню 24.2.1 - Сопровождение системы - Информация

Следующая таблица описывает поля данного меню.

Табл. 35-2 Меню 24.2.1 - Сопровождение системы - Информация

ПОЛЕ	ОПИСАНИЕ
Name (Имя)	Системное имя маршрутизатора OMNI ADSL. Данный параметр можно изменить **в Меню 1 - Настройка общих параметров**.
Routing (Маршрутизация)	Использующийся протокол маршрутизации.
ZyNOS F/W Version (Версия встроенного ПО ZyNOS)	Версия встроенного системного программного обеспечения ZyNOS (ZyXEL Network Operating System). ZyNOS является зарегистрированной торговой маркой ZyXEL Communications Corporation.

Табл. 35-2 Меню 24.2.1 - Сопровождение системы - Информация

ПОЛЕ	ОПИСАНИЕ
ADSL Chipset Vendor (Поставщик микросхемы ADSL)	Производитель микросхемы ADSL и версии DSL.
Standard (Стандарт)	Обозначает операционный протокол, используемый OMNI ADSL и DSLAM (Digital Subscriber Line Access Multiplexer/Мультиплексор доступа к цифровой абонентской линии).
LAN (ЛВС)	
Ethernet Address (Адрес Ethernet)	Это относится к MAC-адресу Ethernet (Media Access Control/Управление доступом к среде) для OMNI ADSL.
IP Address (IP-адрес)	IP-адрес OMNI ADSL в десятичном виде с разделительными точками.
IP Mask (IP-маска)	Маска подсети OMNI ADSL.
DHCP (Dynamic Host Configuration Protocol/Протокол динамического выбора конфигурации хост-машины)	Данное поле показывает настройку DHCP (None или Server) для OMNI ADSL.

35.3.2 Скорость консольного порта

С помощью **Меню 24.2.2 – Сопровождение системы – Скорость консольного порта** можно установить различную скорость для консольного порта. Устройством OMNI ADSL поддерживается скорость 9600 (по умолчанию), 19200, 38400, 57600 и 115200 бит/с. Нажатием клавиш [SPACE BAR] и [ENTER] выберите нужную скорость в меню 24.2.2, как показано на следующем рисунке.

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

Console Port Speed: 9600

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

Рис. 35-5 Меню 24.2.2 - Сопровождение системы - Изменение скорости консольного порта

При изменении скорости консольного порта OMNI ADSL, необходимо также установить параметр скорости для коммуникационной программы, использующейся для подключения к маршрутизатору OMNI ADSL.

35.4 Журнальная регистрация и трассировка

OMNI ADSL имеет две функции журнальной регистрации. Первая - это журналы регистрации ошибок и результатов трассировок, которые хранятся локально. Вторая - функция системного журнала UNIX для регистрации сообщений.

35.4.1 Просмотр журнала регистрации ошибок

Первое, куда следует заглянуть для того, чтобы разобраться в причинах сбоя - это журнал регистрации ошибок. Для просмотра локального журнала регистрации ошибок/трассировок следует выполнить описанную ниже процедуру:

Step 1. Введите "24" в Главном меню для вызова **Меню 24 — Сопровождение системы**.

Step 2. В Меню 24 введите "3" для перехода в Меню **24.3 – Сопровождение системы – Журнальная регистрация и трассировка.**

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

         1. View Error Log
         2. UNIX Syslog


                  Please enter selection:
```

Рис. 35-6 Меню 24.3 - Сопровождение системы: Журнальная регистрация и трассировка

Step 3. В **Меню 24.3 - Сопровождение системы - Журнальная регистрация и трассировка** выберите первую опцию. Появится системный журнал регистрации ошибок.

По завершении показа журнала OMNI ADSL можно воспользоваться опцией очистки журнала. Примеры типичных сообщений об ошибках и информационных сообщений приведены на следующем рисунке.

```
   1 Sat Jan 01 00:00:02 2000 PP09 -WARN  SNMP TRAP 3: link up
   2 Sat Jan 01 00:00:02 2000 PP0f -WARN  Last errorlog repeat 1 Times
   3 Sat Jan 01 00:00:02 2000 PP0f  INFO  LAN promiscuous mode <0>
   4 Sat Jan 01 00:00:02 2000 PP0f  INFO  LAN promiscuous mode <1>
   5 Sat Jan 01 00:00:02 2000 PP00  INFO  Starting Connectivity Monitor
   6 Sat Jan 01 00:00:02 2000 PP1a  INFO  adjtime task pause 1 day
   7 Sat Jan 01 00:00:02 2000 PP1b  INFO  monitoring WAN connectivity
   8 Sat Jan 01 00:00:02 2000 PP1b  INFO  conn-mon change
   9 Sat Jan 01 00:00:22 2000 PP0a  WARN  MPOA Link Down
  10 Sat Jan 01 00:03:41 2000 PP13  INFO  SMT Password pass
Clear Error Log (y/n):
```

Рис. 35-7 Примеры информационных сообщений и сообщений об ошибке

35.4.2 Системный журнал и учет

OMNI ADSL использует функцию системного журнала UNIX для регистрации CDR (Журнал регистрации вызовов) и системных сообщений на сервере системного журнала. Параметры системного журнала и учета можно сконфигурировать в **Меню 24.3.2 – Сопровождение системы – Системный журнал UNIX**, как показано ниже.

```
                Menu 24.3.2 - System Maintenance - UNIX Syslog

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

                      Types: (Типы:)
                        CDR= No
                        Packet Triggered= No
                        Filter log= No
                        PPP log= No

                        Firewall log= No
                        VPN Log= No

                   Press ENTER to Confirm or ESC to Cancel:

 Press Space Bar to Toggle
```

Рис. 35-8 Меню 24.3.2 - Сопровождение системы - Системный журнал и учет

Чтобы активизировать системный журнал необходимо сконфигурировать параметры системного журнала UNIX, описанные в следующей таблице, а затем выбрать то, что требуется регистрировать.

Табл. 35-3 Меню 24.3.2 - Сопровождение системы - Системный журнал и учет

ПАРАМЕТР	ОПИСАНИЕ
UNIX Syslog (Системный журнал UNIX):	
Active (Активно)	Для включения/отключения системного журнала пользуйтесь клавишами [SPACE BAR] и [ENTER].
Syslog IP Address (IP-адрес системного журнала)	Введите IP-адрес сервера системного журнала.
Log Facility (Функция журнала)	Пользуясь клавишами [SPACE BAR] и [ENTER] выберите одну из следующих семи доступных опций. Функция журнальной регистрации дает возможность регистрировать сообщения в различных файлах на сервере. (См. руководство по UNIX).
Types (Типы):	
CDR	Если установлено **Yes**, CDR (Журнал регистрации вызовов) регистрирует любое использование телефонной линии для передачи данных.
Packet Triggered	Если в поле установлено **Yes**, первые 48 байт или октетов, а также тип

Табл. 35-3 Меню 24.3.2 - Сопровождение системы - Системный журнал и учет

ПАРАМЕТР	ОПИСАНИЕ
	протокола пакета, инициировавшего вызов, посылаются на сервер системного журнала UNIX.
Filter Log	Фильтры не регистрируются в журнале, если это поле установлено в **No**. Фильтры, поле Log Filter у которых установлено в **Yes** регистрируются, когда это поле установлено в **Yes**.
PPP Log	Если в поле установлено **Yes**, регистрируются события PPP.
Firewall Log	Если установлено **Yes**, OMNI ADSL посылает журнал брандмауэра на сервер системного журнала.
VPN Log	Если установлено **Yes**, OMNI ADSL посылает журнал VPN на сервер системного журнала.
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.	

На следующем рисунке представлены примеры четырех типов сообщений системного журнала, посланных OMNI ADSL:

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 xxxxx (L2TP, xxxxx = Remote Call ID)
C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxx (= connected speed) xxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
2 - Packet Triggered
SdcmdSyslogSend (SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,

Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
3 - Filter Log
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m), drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol (“TCP”, ”UDP”, ”ICMP”)
spo: Source port
dpo: Destination port
Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP spo=0208 dpo=0208]} S03>R01mF Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF
4 - PPP Log
sdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing

35.5 Диагностика

Функция диагностики позволяет тестировать различные аспекты функционирования OMNI ADSL для определения надежности его работы. С помощью Меню 24.4 можно выбрать различные диагностические тесты для оценки работоспособности системы, как показано на следующем рисунке.

Для доступа к функциям диагностики следует выполнить описанную ниже процедуру.

Step 1. В Главном меню введите "24" для перехода в **Меню 24 – Сопровождение системы**.

Step 2. В данном меню введите "4" для вывода **Меню 24.4 - Сопровождение системы - Диагностика** , показанного ниже.

```
                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
```

Рис. 35-9 Меню 24.4 - Сопровождение системы - Диагностика

В следующей таблице описываются диагностические тесты для OMNI ADSL и соединений, доступные в Меню 24.4.

Табл. 35-4 Меню 24.4 - Сопровождение системы - Диагностика

ПОЛЕ	ОПИСАНИЕ
Reset xDSL (Перезапуск xDSL)	Повторно инициализирует соединение xDSL с телефонной компанией.
Ping Host (Эхо-тестирование связи с хостом)	Производит эхо-тестирование хост-машины для определения работоспособности соединений и протокола TCP/IP в обеих системах.
Reboot System (Перезагрузка системы)	Перезагрузить OMNI ADSL.
Command Mode (Командный режим)	Введите режим для осуществления диагностики OMNI ADSL с помощью определенного набора команд.
Host IP Address (IP-адрес хоста)	Если для эхо-тестирования хост-машины введено "12", введите адрес компьютера, который нужно проверить эхо-тестированием.

Chapter 36
Работа с файлом конфигурации и встроенным программным обеспечением

В данной главе рассматривается резервное сохранение и восстановление существующего файла конфигурации, а также загрузка нового файла конфигурации и встроенного программного обеспечения.

36.1 Значение имен файлов

Файл конфигурации (часто называемый "romfile" или "rom-0") содержит заводские настройки по умолчанию в следующих меню: Пароль, Настройка DHCP, настройка TCP/IP и т. д. Файл конфигурации, предоставляемый ZyXEL, имеет расширение "rom". После того, как в настройки OMNI ADSL внесены изменения, их можно сохранить в файле с любым именем.

Файл ZyNOS (ZyXEL Network Operating System, иногда называемый также файлом "ras") содержит встроенное программное обеспечение системы и имеет расширение "bin". Во многих клиентах FTP и TFTP имена файлов аналогичны указанным ниже.

Пользуйтесь только специальным микропрограммным обеспечением, предназначенным для Вашей модели маршрутизатора OMNI ADSL. См. предупредительную наклейку в нижней части устройства OMNI ADSL.

```
ftp> put firmware.bin ras
```
Это пример сеанса FTP, демонстрирующий передачу файла " firmware.bin" с компьютера на OMNI ADSL.

```
ftp> get rom-0 config.cfg
```
Это пример сеанса FTP, демонстрирующий сохранение текущей конфигурации в файле “config.cfg” компьютера.

Если клиент [T]FTP не позволяет использовать различные имена для исходного и целевого файла, может возникнуть необходимость в их переименовании, так как OMNI ADSL распознает только "rom-0" и "ras". Убедитесь, что у Вас остались неизмененные копии обоих файлов, так как они могут потребоваться в дальнейшем.

Следующая таблица представляет собой сводку по именам файлов. Следует отметить, что внутреннее имя файла относится к имени файла на OMNI ADSL, а внешнее имя файла относится к имени файла вне OMNI ADSL, то есть на компьютере, в локальной сети или на FTP-сайте, таким образом, имена (но не расширения) могут различаться. После загрузки нового встроенного программного обеспечения см. поле **ZyNOS F/W Version** в **Меню 24.2.1 - Сопровождение системы - Информация**, чтобы убедиться, что загружена правильная версия встроенного программного обеспечения. Введите команду AT после нажатия "Y" в ответ на предложение перейти в режим отладки в меню SMT.

Табл. 36-1 Значение имен файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл конфигурации	Rom-0	Это имя файла конфигурации OMNI ADSL. При загрузке файла rom-0 происходит замена всей файловой системы ПЗУ, включая конфигурацию OMNI ADSL, данные, относящиеся к системе (включая пароль по умолчанию), журнал регистрации ошибок и журнал регистрации результатов трассировки.	*.rom
Встроенное программное обеспечение	Ras	Это базовое имя для встроенного программного обеспечения ZyNOS на OMNI ADSL.	*.bin

36.2 Резервное сохранение конфигурации

OMNI ADSL отображает различные сообщения с разъяснениями существующих путей резервного сохранения, восстановления и загрузки файлов в Меню 24.5, 24.6, 24.7.1 и 24.7.2. Выбор зависит от того, что используется для подключения - консольный порт или Telnet.

Опция 5 **Меню 24 - Сопровождение системы** позволяет сохранять текущую конфигурацию OMNI ADSL на компьютере. Резервирование настоятельно рекомендуется после того, как получена работающая конфигурация OMNI ADSL. Более предпочтительным способом сохранения текущей конфигурации является FTP вследствие его высокой скорости. Кроме того, можно производить резервное сохранение и восстановление конфигурации через консольный порт с помощью Меню 24. Подходит любая коммуникационная программа, поддерживающая работу в режиме терминала, однако для загрузки/выгрузки программного обеспечения следует 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 OMNI ADSL на компьютер, а "выгрузка" - с компьютера на OMNI ADSL.

36.2.1 Резервное сохранение конфигурации

Следует выполнить указания, приведенные в следующем экране.

```
                    Menu 24.5 - Backup Configuration

 To transfer the configuration file to your computer, follow the procedure
 below:

   1. Launch the FTP client on your computer.
   2. Type "open" and the IP address of your system. Then type "root" and
      SMT password as requested.
   3. Locate the 'rom-0' file.
   4. Type 'get rom-0' to back up the current system configuration to your
      computer.

 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 user manual.

                              Press ENTER to Exit:
```

Рис. 36-1 Telnet в Меню 24.5

36.2.2 Использование команд FTP из командной строки

Step 1. Запустите клиент FTP на своем компьютере.

Step 2. Введите "open", а затем через пробел - IP-адрес OMNI ADSL.

Step 3. При появлении запроса имени пользователя нажмите клавишу [ENTER].

Step 4. Введите пароль (пароль по умолчанию "1234").

Step 5. Введите "bin" для установки двоичного режима передачи.

Step 6. Использовать "get" для передачи файлов с OMNI ADSL на компьютер, напр., "get rom-0 config.rom" передает файл конфигурации с OMNI ADSL на компьютер и переименовывает его в "config.rom". Более подробно пояснения по именам файлов см. в данной главе выше.

Step 7. Введите "quit" для выхода из режима FTP.

36.2.3 Пример использования команд FTP из командной строки

```
331 Enter PASS command
Пароль:
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
```

Рис. 36-2 Пример сеанса FTP

36.2.4 Клиенты FTP на базе GUI

В следующей таблице описываются некоторые параметры клиентов FTP на базе GUI.

Табл. 36-2 Общие команды для клиентов FTP на базе GUI

КОМАНДА	ОПИСАНИЕ
Host Address (Адрес хоста)	Введите адрес хост-сервера.
Login Type (Тип регистрации)	Анонимная. В этом случае серверу автоматически назначается идентификатор пользователя и пароль для анонимного доступа. Анонимная регистрация возможна только, если эта опция включена Интернет-провайдером или администратором услуг. Обычная. Для выполнения регистрации требуется уникальный идентификатор пользователя и пароль.
Transfer Type (Тип передачи)	При загрузке конфигурации или файла микропрограммного обеспечения необходимо использовать двоичный режим. Передача файлов либо в режиме ASCII (форма открытого текста), либо в двоичном режиме.
Initial Remote Directory (Исходный удаленный каталог)	Определите удаленный каталог по умолчанию (путь).
Initial Local Directory (Исходный локальный каталог)	Определите локальный каталог по умолчанию (путь).

36.2.5 Случаи, когда TFTP и FTP не будет работать через глобальную сеть

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

1. Отключена функция сервиса Telnet в Меню 24.11.
2. Применен фильтр в меню 3.1 (ЛВС) или в меню 11.5 (глобальная сеть) для блокировки услуги Telnet.
3. IP-адрес в поле **Secured Client IP (Защищенный клиент IP)** в Меню 24.11 не соответствует клиенту IP. В этом случае OMNI ADSL немедленно прерывает сеанс связи Telnet.
4. Осуществляется сеанс связи с системным терминалом.

36.2.6 Резервное сохранение конфигурации с помощью TFTP

OMNI ADSL поддерживает загрузку/выгрузку микропрограммного обеспечения и файла конфигурации с использованием протокола TFTP (упрощенного протокола передачи файлов) через LAN. Данный протокол также может применяться (хотя и не рекомендуется) при работе через WAN.

Для использования TFTP Ваш компьютер должен иметь клиенты Telnet и TFTP. Для сохранения файла конфигурации следует выполнить описанную ниже процедуру:

Step 1. Подключиться к OMNI ADSL через Telnet и зарегистрироваться. Так как проверка защиты в TFTP не предусмотрена, OMNI ADSL регистрирует IP-адрес клиента Telnet и принимает запросы TFTP только с этого адреса.

Step 2. Перевести системный терминал в режим командного процессора (CI) путем ввода "8" в **Меню 24** – **Сопровождение системы**.

Step 3. Ввести команду "sys stdio 0" для запрета отключения по тайм-ауту системного терминала, чтобы передача при помощи TFTP не была прервана. Ввести команду "sys stdio 5" чтобы восстановить пятиминутный интервал тайм-аута системного терминала (по умолчанию) по окончании передачи файла.

Step 4. Запустить клиента TFTP на компьютере и подключиться к OMNI ADSL. Перед началом передачи данных установить двоичный режим передачи.

Step 5. Для передачи файлов с OMNI ADSL на компьютер и обратно следует использовать клиента TFTP (см. в приведенном ниже примере). Для файла конфигурации используется имя "rom-0" (rom-ноль, а не заглавная "O").

Следует помнить, что перед началом и в процессе передачи данных по TFTP должно быть установлено Telnet-соединение, а системный терминал должен находиться в CI-режиме. Для получения подробной информации по командам TFTP (см. следующий пример) следует обратиться к документации по имеющимся клиентским программам TFTP. В операционной системе UNIX

используется команда "get" для передачи с OMNI ADSL на компьютер и "binary" - для установки двоичного режима передачи.

36.2.7 Пример команды TFTP

Ниже приведен пример команды TFTP:

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

где "i" обозначает двоичный режим передачи (этот режим используется при передаче двоичных файлов), "host" - IP-адрес OMNI ADSL, "get" осуществляет передачу файла с OMNI ADSL (rom-0 - имя файла конфигурации OMNI ADSL) на компьютер и переименование его в config.rom.

36.2.8 Клиенты TFTP на базе GUI

В следующей таблице описываются некоторые параметры клиентов TFTP на базе GUI.

Табл. 36-3 Общие команды для клиентов TFTP на базе GUI

КОМАНДА	ОПИСАНИЕ
Host (Хост-машина)	Введите IP-адрес OMNI ADSL. IP-адрес OMNI ADSL по умолчанию при поставке - 192.168.1.1.
Send/Fetch (Передать/Принять)	Нажмите "Send" для загрузки файла на OMNI ADSL и "Fetch" для резервного сохранения файла на компьютере.
Local File (Локальный файл)	Введите путь и имя файла встроенного программного обеспечения (расширение *.bin) или файла конфигурации (расширение *.rom) на ПК.
Remote File (Удаленный файл)	Имя файла на OMNI ADSL. Для файла встроенного программного обеспечения используется имя "ras", а для файла конфигурации - "rom-0".
Binary (Двоичный режим)	Передать файл в двоичном режиме.
Abort (Стоп)	Остановить передачу файла.

Для получения более подробной информации о конфигурации, блокирующей работу TFTP и FTP через глобальную сеть, см. *раздел 36.2.5*.

36.2.9 Резервное сохранение конфигурации через консольный порт (только для модели OMNI ADSL LAN H/HW)

Для резервного сохранения конфигурации через консольный порт следует выполнить описанную ниже процедуру для программы HyperTerminal. Процедура для других программ, поддерживающих работу в режиме терминала, аналогична.

Step 1. Вызовите Меню 24.5 на экран и введите "Y", как показано на следующем рисунке.

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

Рис. 36-3 Меню 24.5 - Сопровождение системы - Резервное сохранение конфигурации

Step 2. Следующий экран показывает, что загрузка по Xmodem запущена.

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

Рис. 36-4 Меню 24.5 - Сопровождение системы – Экран запуска загрузки по Xmodem

Step 3. Запустите программу HyperTerminal, щелкнув на **Transfer**, а затем на **Receive File**, как показано на следующем рисунке.

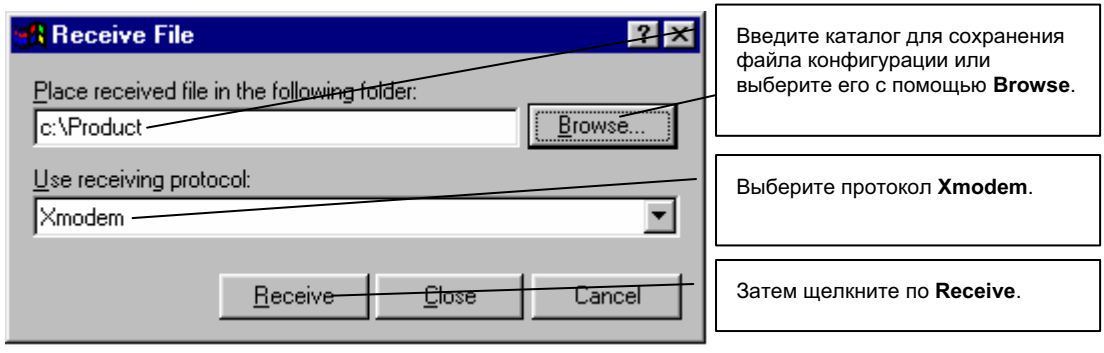


Рис. 36-5 Пример резервного сохранения конфигурации

Step 4. После успешного создания резервной конфигурации появится следующий экран. Нажмите любую клавишу для возврата в меню SMT.

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

Рис. 36-6 Экран подтверждения успешного резервного сохранения

36.3 Восстановление конфигурации

В данном разделе описывается восстановление предварительно сохраненной конфигурации. Следует помнить, что перед тем как восстановить предыдущую резервную конфигурацию, данная функция стирает текущую конфигурацию; поэтому перед началом восстановления следует сохранить резервный файл текущей конфигурации на диске.

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

ПРЕДУПРЕЖДЕНИЕ!
НЕ ПРЕРЫВАЙТЕ ПРОЦЕСС ПЕРЕДАЧИ ФАЙЛА, ТАК КАК ЭТО МОЖЕТ ПРИВЕСТИ К НЕУСТРАНИМЫМ ПОВРЕЖДЕНИЯМ OMNI ADSL.

36.3.1 Восстановление конфигурации с помощью FTP

Более подробно о резервном сохранении с помощью (T)FTP см. в предыдущих разделах по загрузке файлов через FTP и TFTP в данной главе.

```
                    Menu 24.6 - Restore Configuration

To transfer the firmware and the configuration file, follow the procedure
below:

  1. Launch the FTP client on your computer.
  2. Type "open" and the IP address of your system.  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 computer and rom-0 is the
     remote file name on the system. This restores the configuration to
     your system.
  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 restoring using TFTP (note that you must
remain on this menu to restore using TFTP), please see your user manual.

                            Press ENTER to Exit:
```

Рис. 36-7 Telnet в Меню 24.6

Step 1. Запустите клиент FTP на своем компьютере.

Step 2. Введите "open", а затем через пробел - IP-адрес OMNI ADSL.

Step 3. При появлении запроса имени пользователя нажмите клавишу [ENTER].

Step 4. Введите пароль (пароль по умолчанию "1234").

Step 5. Введите "bin" для установки двоичного режима передачи.

Step 6. Найдите файл "rom" (на своем компьютере), который нужно восстановить на OMNI ADSL.

Step 7. Используйте команду "put" для передачи файлов с компьютера на OMNI ADSL , напр., "put config.rom rom-0" передает файл конфигурации "config.rom" с компьютера на OMNI ADSL. Более подробно пояснения по именам файлов см. в данной главе выше.

Step 8. Введите "quit" для выхода из режима FTP. После успешного восстановления конфигурации OMNI ADSL автоматически перезапускается.

36.3.2 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
```

Рис. 36-8Пример восстановления конфигурации с помощью сеанса FTP

Для получения более подробной информации о конфигурации, блокирующей работу TFTP и FTP через глобальную сеть см. *раздел 36.2.5*.

36.3.3 Восстановление конфигурации через консольный порт (только для моделей OMNI ADSL LAN H/HW)

Для восстановления конфигурации через консольный порт следует выполнить описанную ниже процедуру для программы HyperTerminal. Процедура для других программ, поддерживающих работу в режиме терминала, аналогична.

Step 1. Вызовите меню 24.6 на экран и введите "Y", как показано на следующем рисунке.

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

Рис. 36-9 Сопровождение системы - Восстановление конфигурации

Step 2. Следующий экран показывает, что загрузка по Xmodem запущена.

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

Рис. 36-10Сопровождение системы — Экран запуска загрузки по Xmodem

Step 3. Запустите программу HyperTerminal, щелкнув на **Transfer**, а затем на **Send File**, как показано на следующем рисунке.

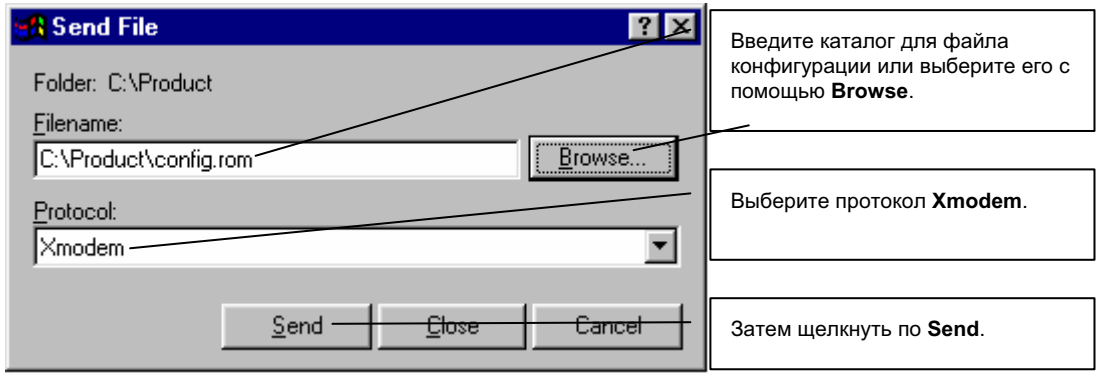


Рис. 36-11 Пример восстановления конфигурации

Step 4. После успешного восстановления конфигурации появится следующий экран. Нажмите любую клавишу для перезапуска OMNI ADSL и возвращения в меню SMT.

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

Рис. 36-12 Экран подтверждения успешного восстановления конфигурации

36.4 Загрузка встроенного программного обеспеченияи файла конфигурации

В данном разделе рассматривается загрузка файла конфигурации и встроенного программного обеспечения. Файл конфигурации можно загрузить, выполнив процедуру, описанную в предыдущем разделе *Восстановление конфигурации* или указания в **Меню 24.7.2 - Сопровождение системы - Загрузка системного файла конфигурации** (для консольного порта).

ПРЕДУПРЕЖДЕНИЕ!
НЕ ПРЕРЫВАТЬ ПРОЦЕСС ПЕРЕДАЧИ ФАЙЛА, ТАК КАК ЭТО МОЖЕТ ПРИВЕСТИ К НЕУСТРАНИМЫМ ПОВРЕЖДЕНИЯМ OMNI ADSL.

36.4.1 Загрузка встроенного программного обеспечения

FTP является более предпочтительным методом для загрузки файлов конфигурации и встроенного программного обеспечения. Чтобы использовать эту функцию, компьютер должен располагать клиентом FTP.

При подключении к OMNI ADSL через Telnet появляются следующие экраны для загрузки файла конфигурации и встроенного программного обеспечения при помощи FTP.

```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.
                            Press ENTER to Exit:
```

Рис. 36-13 Telnet в Меню 24.7.1 - Загрузка встроенного системного микропрограммного обеспечения

36.4.2 Загрузка файла конфигурации

При входе в меню 24.7.2 через Telnet появляется следующий экран.

```
      Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

                              Press ENTER to Exit:
```

Рис. 36-14 Telnet в Меню 24.7.2 - Сопровождение системы

Для загрузки файлов конфигурации и встроенного программного обеспечения следует выполнить описанные ниже действия:

36.4.3 Пример использования команды загрузки файлов через FTP из подсказки DOS

Step 1. Запустите клиент FTP на своем компьютере.

Step 2. Введите "open", а затем через пробел - IP-адрес OMNI ADSL.

Step 3. При появлении запроса имени пользователя нажмите клавишу [ENTER].

Step 4. Введите пароль (пароль по умолчанию "1234").

Step 5. Введите "bin" для установки двоичного режима передачи.

Step 6. Используйте "put" для передачи файлов с компьютера на OMNI ADSL, напр., "put firmware.bin ras" передает файл встроенного программного обеспечения (firmware.bin) с компьютера на OMNI ADSL и переименовывает его в "ras". Аналогичным образом "put config.rom rom-0" передает файл конфигурации (config.rom) с компьютера на OMNI ADSL и переименовывает его в "rom-0". Точно так же "get rom-0 config.rom" передает файл конфигурации с OMNI ADSL на компьютер и переименовывает его в "config.rom". Более подробно пояснения по именам файлов см. в данной главе выше.

Step 7. Введите "quit" для выхода из режима FTP.

После успешной загрузки файла происходит автоматический перезапуск OMNI ADSL.

36.4.4 Пример загрузки встроенного программного обеспечения с помощью сеанса FTP

```
331 Enter PASS command
Пароль:
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
```

Рис. 36-15 Пример загрузки встроенного программного обеспечения с помощью сеанса FTP

Другие команды (для клиентов FTP на базе GUI) были перечислены в данной главе ранее.

Для получения более подробной информации о конфигурации, блокирующей работу TFTP и FTP через глобальную сеть см. *раздел 36.2.5*.

36.4.5 Загрузка файлов через TFTP

OMNI ADSL также поддерживает загрузку файлов микропрограммного обеспечения с использованием протокола TFTP (упрощенного протокола передачи файлов) через LAN. Данный протокол может использоваться (хотя это и не рекомендуется) и при передаче через WAN.

Для использования TFTP компьютер должен иметь клиенты Telnet и TFTP. Для передачи встроенного программного обеспечения и файла конфигурации следует выполнить описанные ниже действия.

Step 1. Подключиться к OMNI ADSL через Telnet и зарегистрироваться. Так как проверка защиты в TFTP не предусмотрена, OMNI ADSL регистрирует IP-адрес клиента Telnet и принимает запросы TFTP только с этого адреса.

Step 2. Перевести системный терминал в режим командного процессора (CI), введя "8" в **Меню 24 – Сопровождение системы**.

Step 3. Ввести команду "sys stdio 0" для запрета отключения по тайм-ауту системного терминала, чтобы передача при помощи TFTP не была прервана. Ввести команду "sys stdio 5" чтобы восстановить пятиминутный интервал тайм-аута системного терминала (по умолчанию) по окончании передачи файла.

Step 4. Запустить клиента TFTP на компьютере и подключиться к OMNI ADSL. Перед началом передачи данных установить двоичный режим передачи.

Step 5. Для передачи файлов с OMNI ADSL на компьютер и обратно следует использовать клиента TFTP (см. в приведенном ниже примере). Имя файла встроенного программного обеспечения - "ras".

Следует помнить, что перед началом и в процессе передачи данных по TFTP должно быть установлено Telnet-соединение, а OMNI ADSL должен находиться в режиме командного процессора. Для получения подробной информации по командам TFTP (см. следующий пример) следует обратиться к документации по имеющимся клиентским программам TFTP. В операционной системе UNIX используется команда "get" для передачи с OMNI ADSL на компьютер, "put" - для передачи в обратном направлении и "binary" - для установки двоичного режима передачи.

36.4.6 Пример команды загрузки через TFTP

Ниже приведен 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 OMNI ADSL, "put" осуществляет передачу файла с компьютера (firmware.bin – имя файла программного обеспечения на компьютере) на удаленный хост (ras - имя файла программного обеспечения на OMNI ADSL).

Команды для клиентов TFTP на базе GUI были перечислены в данной главе ранее.

36.4.7 Загрузка конфигурации через консольный порт (только для моделей OMNI ADSL LAN H/HW)

Более предпочтительными методами загрузки встроенного программного обеспечения в OMNI ADSL являются FTP и TFTP. Однако, если сеть не работает, загрузка файлов возможна только с помощью прямого соединения с OMNI ADSL через консольный порт. В обычных условиях загрузка файлов через консольный порт не рекомендуется, так как через FTP и TFTP это делается гораздо быстрее. Подходит любая коммуникационная программа, поддерживающая работу в режиме терминала, однако для загрузки/выгрузки лучше использовать протокол Xmodem.

36.4.8 Загрузка файла конфигурации через консольный порт (только для моделей OMNI ADSL LAN H/HW)

Step 1. Выберите "1" в **Меню 24.7 - Сопровождение системы - Загрузка встроенного программного обеспечения** для вывода **Меню 24.7.1 - Сопровождение системы - Загрузка встроенного системного программного обеспечения**, а затем выполнить указания, приведенные в следующем экране.

```
              Menu 24.7.1 - System Maintenance - Upload System Firmware


          To upload system firmware:
          1. Enter "y" at the prompt below to go into debug mode.
          2. Enter "atur" after "Enter Debug Mode" message.
          3. Wait for "Starting XMODEM upload" message before activating
             Xmodem upload on your terminal.
          4. After successful firmware upload, enter "atgo" to restart the
             OMNI ADSL.

          Warning: Proceeding with the upload will erase the current system
          firmware.
                           Do You Wish To Proceed:(Y/N)
```

Рис. 36-16 Вид Меню 24.7.1 при использовании консольного порта

Step 2. После появления сообщения "Starting XMODEM upload" необходимо активизировать протокол Xmodem. Выполните процедуру для программы HyperTerminal, описанную выше. Процедура для других программ, поддерживающих работу в режиме терминала, аналогична.

36.4.9 Пример загрузки встроенного программного обеспечения по Xmodem с помощью программы HyperTerminal

Щелкните по **Transfer (Передача)**, а затем по **Send File (Отправить файл)**, чтобы вызвать следующий экран.

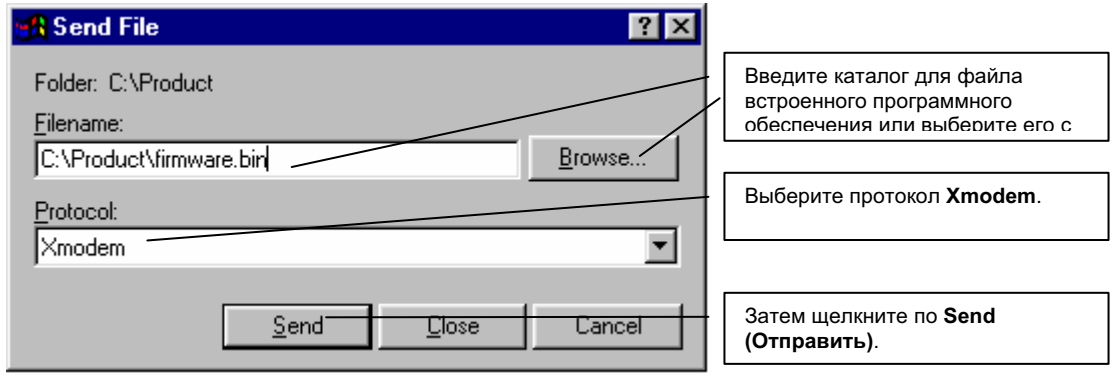


Рис. 36-17 Пример загрузки по Xmodem

После завершения процесса загрузки файла конфигурации следует перезапустить OMNI ADSL, введя команду "atgo".

36.4.10 Загрузка файла конфигурации через консольный порт

Step 1. Выберите "2" в **Меню 24.7 - Сопровождение системы - Загрузка встроенного программного обеспечения** для вывода **Меню 24.7.2 - Сопровождение системы - Загрузка системного файла конфигурации**. Далее необходимо выполнить указания, приведенные в следующем экране.

```
        Menu 24.7.2 - System Maintenance - Upload System Configuration File


        To upload system configuration file:
        1. Enter "y" at the prompt below to go into debug mode.
        2. Enter "atlc" after "Enter Debug Mode" message.
        3. Wait for "Starting XMODEM upload" message before activating
           Xmodem upload on your terminal.
        4. After successful firmware upload, enter "atgo" to restart the
           system.

        Warning:
        1. Proceeding with the upload will erase the current router
           configuration file.
        2. The system's console port speed (Menu 24.2.2) may change
           when it is restarted; please adjust your terminal's speed
           accordingly. The password may change (menu 23), also.
        3. When uploading the DEFAULT configuration file, the console
           port speed will be reset to 9600 bps and the password to
           "1234".
                        Do You Wish To Proceed:(Y/N)
```

Рис. 36-18 Вид Меню 24.7.2 при использовании консольного порта

Step 2. После появления сообщения "Starting XMODEM upload" необходимо активизировать протокол Xmodem. Выполните процедуру для программы HyperTerminal, описанную выше. Процедура для других программ, поддерживающих работу в режиме терминала, аналогична.

Step 3. Введите "atgo" для перезапуска OMNI ADSL.

36.4.11 Пример загрузки файла конфигурации по Xmodem с помощью программы HyperTerminal

Щелкните по **Transfer (Передача)**, а затем по **Send File (Отправить файл)**, чтобы вызвать следующий экран.

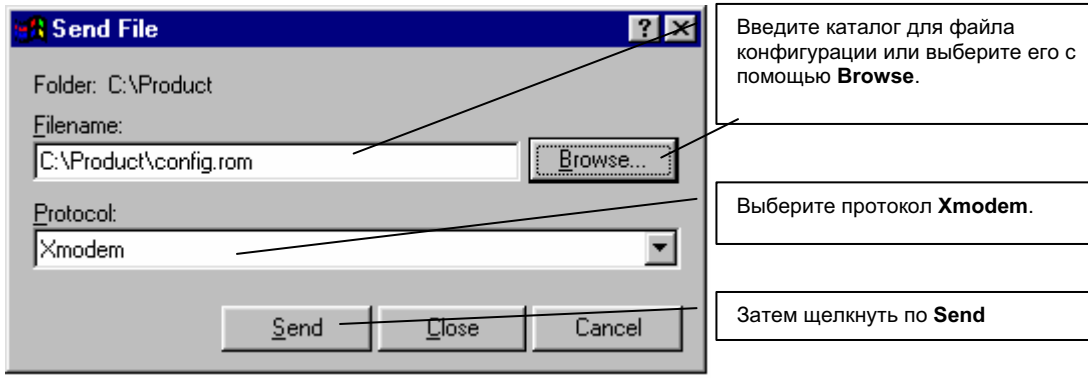


Рис. 36-19 Пример загрузки по Xmodem

После завершения процесса загрузки файла конфигурации следует перезапустить OMNI ADSL, введя команду "atgo".

Chapter 37
Сопровождение системы

В этой главе приводятся описания меню SMT с 24.8 по 24.10.

37.1 Описание режима командного процессора

Командный процессор (CI) является частью основного встроенного программного обеспечения системы. CI обладает практически всеми теми же функциями, что и SMT, а, кроме того, некоторыми функциями настройки низкого уровня и диагностики. Войти в режим командного процессора из SMT можно, выбрав меню 24.8. Более подробную информацию по командам CI можно найти на компакт-диске, входящем в комплект поставки или на Web-сайте zyxel.com. Введите "8" в **Меню 24 - Сопровождение системы**. Список доступных команд можно получить, введя `help` или `?` в командной строке. Для возврата к Главному меню SMT по окончании работы наберите "exit".

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information и Console Port Speed
3.  Log и 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 37-1 Командный режим в Меню 24

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             poe             wlan            ip
ipsec           ppp             bridge          hdap
bm              radius          8021x
ras>
```

Рис. 37-2 Доступные команды

37.2 Поддержка управления вызовами

Функция поддержки управления вызовами выполняется только при выборе режима **Encapsulation** - **PPPoE** в Меню 4 или Меню 11.1.

Функция бюджетирования позволяет устанавливать лимит на общее время исходящих вызовов OMNI ADSL за определенный интервал времени. Если общая продолжительность исходящих вызовов превысит установленный предел, текущий вызов будет сброшен, а все последующие исходящие вызовы будут заблокированы.

Для доступа в меню управления вызовами выберите "9" в меню 24 для перехода в **Меню 24.9 - Сопровождение системы - Управление вызовами**, как показано на следующем рисунке.

```
                Menu 24.9 - System Maintenance - Call Control

                   1.  Budget Management



                        Enter Menu Selection Number:
```

Рис. 37-3 Меню 24.9 - Сопровождение системы: Управление вызовами

37.2.1 Бюджетирование

В меню 24.9.1 выводится бюджетная статистика исходящих вызовов. Введите "1" в **Меню 24.9 - Сопровождение системы - Управление вызовами** для перехода к следующему меню.

```
                    Menu 24.9.1 - Budget Management

  Remote Node        Connection Time/Total Budget      Elapsed Time/Total Period
1. MyISP                      No Budget                       No Budget
2.--------                       ---                             ---
3.--------                       ---                             ---
4.--------                       ---                             ---
5.--------                       ---                             ---
6.--------                       ---                             ---
7.--------                       ---                             ---
8.--------                       ---                             ---

                      Reset Node (0 to update screen):
```

Рис. 37-4 Меню 24.9.1 - Бюджетирование

Общий бюджет - это лимит, устанавливаемый для суммарного времени исходящих вызовов удаленного узла. Превышение данного лимита приводит к сбрасыванию вызова и блокированию всех последующих исходящих вызовов данного удаленного узла. По завершении бюджетируемого времени бюджет сбрасывается. По умолчанию для бюджета установлено 0 минут 0 часов, т.е. бюджетирование выключено. Введя в данном меню индекс удаленного узла, можно сбросить суммарное время соединения. Для обновления экрана нажмите "0". Если выбрана инкапсуляция PPPoE, то параметры бюджета и периодичности его сброса для удаленного узла устанавливаются в Меню 11.1.

Табл. 37-1 Меню 24.9.1 - Бюджетирование

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Remote Node (Удаленный узел)	Введите индекс удаленного узла (в данном случае один)	1
Connection Time/Total Budget (Время соединения/Общий бюджет)	Общее истекшее время соединения в пределах выделенного бюджета, установленного в меню 11.1.	5/10 означает, что прошло 5 минут из выделенных 10 минут.
Elapsed Time/Total Period (Время работы/Общая продолжительность периода)	Период - это временной цикл (в часах), после которого происходит сброс выделенного бюджета (см. меню 11.1.) Использованное время - это время, использованное в пределах периода.	0.5/1 означает, что прошло 30 минут из промежутка времени в 1 час.
Введите "0" для обновления экрана или нажмите клавишу [ESC] для возврата к предыдущему экрану.		

37.3 Установка времени и даты

OMNI ADSL осуществляет хранение даты и времени. В нем имеется программная процедура для установки времени вручную или получения значения текущего времени и даты от внешнего сервера при включении устройства OMNI ADSL. В меню 24.10 можно произвести обновление настроек даты и времени OMNI ADSL. При этом реальное время отображается в журналах регистрации ошибок OMNI ADSL.

В Главном меню введите "24" для перехода в **Меню 24 - Сопровождение системы**, показанное ниже.

```
                Menu 24 - System Maintenance

               1.  System Status
               2.  System Information
               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. 37-5 Меню 24 - Сопровождение системы

Введите "10" для перехода в **Меню 24.10 - Сопровождение системы - Установка времени и даты** для обновления настроек времени и даты OMNI ADSL, как показано на следующем экране.

```
          Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= None
Time Server Address= N/A

Current Time:                          00 : 00 : 00
New Time (hh:mm:ss):                   11 : 23: 16

Current Date:                          2000 - 01 - 01
New Date (yyyy-mm-dd):                 2001 - 03 - 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:
```

Рис. 37-6 Меню 24.10 - Сопровождение системы : - Установка времени и даты

Табл. 37-2 Меню 24.10 - Сопровождение системы - Установка времени и даты

ПОЛЕ	ОПИСАНИЕ
Use Time Server when Bootup (Использование сервера времени при перезагрузке)	Укажите сервисный протокол, посылаемый сервером времени при включении OMNI ADSL. Серверы могут поддерживать не все протоколы, поэтому необходимо обратиться к Интернет-провайдеру/сетевому администратору или методом подбора найти работающий протокол. Основное различие между ними - формат. Формат **Daytime (RFC 867)** - это формат вида день/месяц/год/часовой пояс сервера. Формат **Time (RFC-868)** представляет собой 4-байтовое целое число, означающее количество секунд, прошедшее с момента времени 0:0:0 1 января 1970 года. Формат **NTP (RFC-1305)** такой же, как и **Time (RFC-868)**. **None**. - задано по умолчанию. Введите время вручную.
Time Server Address (Адрес сервера времени)	Введите IP-адрес или имя домена Вашего сервера времени. Если Вы не располагаете точной информацией, следует обратиться к Интернет-провайдеру или системному администратору.
Current Time (Текущее время)	Обновленное время появляется в этом поле только при следующем заходе в это меню.
New Time (Новое время)	Введите новое время суток в формате часа, минут и секунд.
Current Date (Текущая дата)	В данном поле показана текущая дата (обновляется только при повторном входе в меню).
New Date (Новая дата)	Введите новую дату в формате "месяц, день, год".
Time Zone (Часовой пояс)	Нажатием клавиш [SPACE BAR] и [ENTER] установите значение расхождения часовых поясов между Вашим часовым поясом и Гринвичским временем (GMT).
Daylight Saving (Летнее время)	Если в Вашей стране принято летнее время, выберите **Yes**.
Start Date (Дата перехода)	Если вы пользуетесь летним временем, введите дату и месяц перехода на летнее время.
End Date (Дата обратного перехода)	Если вы пользуетесь летним временем, введите дату и месяц окончания периода летнего времени.

ПОЛЕ	ОПИСАНИЕ
После заполнения полей меню и получения сообщения “Press ENTER to Confirm or ESC to Cancel“, нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для ее отмены.	

37.3.1 Сброс времени

OMNI ADSL сбрасывает установленное время только в трех случаях:

i. При выходе из меню 24.10 после внесения изменений.

ii. При запуске OMNI ADSL, при условии, что в меню 24.10 задан сервер времени.

iii. Через 24 часа после запуска.

Chapter 38
Дистанционное управление

В этой главе описывается режим дистанционного управления из меню SMT 24.11. Функция дистанционного управления доступна не для всех моделей.

38.1 Описание дистанционного управления

Функция дистанционного управления позволяет определить порядок доступа к ресурсам сети: с какого компьютера, к каким услугам/протоколам и через какой интерфейс (если их несколько) устройства OMNI ADSL.

38.2 Настройка дистанционного управления

Чтобы отключить функцию дистанционного управления для данной услуги, выберите **Disable** в соответствующем поле **Server Access**.

Введите "11" в меню 24 для вызова **Меню 24.11 – Работа в режиме дистанционного управления**.

38.2.1 Настройка дистанционного управления

Возможны следующие режимы дистанционного управления OMNI ADSL:

только через Интернет (**WAN only**), только через ЛВС **(LAN only)**, **ALL** - через LAN и WAN или **Disable** (Отключено).

- WAN only (Internet)
- ALL (LAN and WAN)
- LAN only
- Disable (Neither)

Если функция дистанционного управления включена, но одновременно применяется фильтр блокировки услуги, Вы не сможете осуществлять дистанционное управление ею.

Введите "11" в меню 24 для вызова **Меню 24.11 — Работа в режиме дистанционного управления** (показано ниже).

```
                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:
```

Рис. 38-1 Меню 24.11- Работа в режиме дистанционного управления

Следующая таблица описывает поля данного меню.

Табл. 38-1 Меню 24.11 - Работа в режиме дистанционного управления

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Telnet Server FTP Server Web Server (Серверы Telnet, FTP и Web)	Каждая из этих надписей (только для чтения) указывает вид сервиса, позволяющий дистанционно управлять устройством OMNI ADSL.	
Server Port (Порт сервера)	В данном поле отображается номер порта доступа к сервису для выполнения дистанционного управления. Номер порта доступа к этому сервису, если нужно можно изменить, но для выполнения дистанционного управления необходимо пользоваться тем же самым номером порта доступа к данному виду сервиса.	23
Server Access (Сервер доступа)	Выберите интерфейс доступа (если он есть) нажатием клавиши [SPACE BAR]. Возможные варианты: **LAN only**, **WAN only**, **ALL** или **Disable**. По умолчанию принято - **LAN only**.	**LAN only**
Secured Client IP (Надежный IP-клиент)	Заданное по умолчанию значение 0.0.0.0 позволяет любому клиенту пользоваться этим сервисом для дистанционного управления устройством OMNI ADSL. Введите какой-либо IP-адрес для ограничения доступа только клиенту, имеющему IP-адрес, совпадающий с указанным.	0.0.0.0
После заполнения полей меню и получения сообщения "Press ENTER to Confirm or ESC to Cancel", нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для ее отмены.		

38.2.2 Ограничения дистанционного управления

Дистанционное управление через локальную или глобальную сеть невозможно в следующих случаях:

1. Если применен фильтр в меню 3.1 (локальная сеть) или меню в 11.5 (глобальная сеть) для блокировки соединений Telnet, FTP или Web.
2. Данная функция отключена в меню 24.11.
3. IP-адрес в поле **Secured Client IP** (меню 24.11) не совпадает с IP-адресом клиента. В этом случае OMNI ADSL немедленно прекращает сеанс связи Telnet.
4. При совпадении сеансов дистанционного управления одного типа (Web, FTP или Telnet). Одновременно нельзя осуществлять два и более сеанса удаленного управления одного и того же типа.
5. Сеанс удаленного управления Web осуществляется одновременно с сеансом Telnet. При установлении Web-соединения сеанс связи Telnet сбрасывается; Telnet-соединение не установится при уже существующем Web-соединении.

38.3 Дистанционное управление и трансляция сетевых адресов

Когда функция NAT включена:

- при управлении из глобальной сети следует использовать IP-адрес устройства OMNI ADSL в глобальной сети;
- при управлении из локальной сети следует использовать IP-адрес OMNI ADSL в локальной сети.

38.4 Системная задержка

Время системной задержки для соединений Telnet/Web/FTP составляет пять минут (300 секунд). В OMNI ADSL автоматически происходит выход из системы, если в течение этого срока не происходит никаких действий, за исключением непрерывного обновления статуса в меню 24.1 или изменения `sys stdio` в командной строке.

Chapter 39
Маршрутизация на базе стратегии IP

В данной главе рассматривается настройка и применение стратегий IP, используемых для маршрутизации.

39.1 Описание маршрутизации на базе стратегии IP

Как правило, маршрутизация основывается только на адресе назначения, который указывает самый короткий путь для пересылки пакета. Маршрутизация на базе стратегии IP (IPPR) предоставляет возможность игнорировать схему маршрутизации, заданную по умолчанию, и изменить процесс пересылки пакета на базе стратегии, определенной сетевым администратором. Маршрутизация на базе стратегии применяется к входящим пакетам, рассылаемым по интерфейсу, и осуществляется перед обычной маршрутизацией.

39.2 Преимущества маршрутизации на базе стратегии IP

- Маршрутизация в зависимости от источника - Сетевые администраторы могут использовать маршрутизацию на базе IP-стратегии для пропуска трафика от различных пользователей через различные каналы.
- Качество услуги (QoS) – Организации могут дифференцировать трафик путем определения очередности в IP-заголовке или TOS (Type of Service/Тип услуги) для периферии сети с целью активизации функции назначения приоритетов трафика.
- Сокращение расходов - IPPR позволяет организациям использовать дорогостоящие каналы с высокой пропускной способностью для интерактивного трафика, а дешевые каналы - для пакетного трафика.
- Разделение нагрузки - Сетевые администраторы могут использовать IPPR для распределения трафика на несколько путей.

39.3 Стратегия маршрутизации

Отдельные стратегии маршрутизации используются как часть единого процесса IPPR. Стратегия определяет критерии соответствия и действие, которое должно быть выполнено, если пакет отвечает этим критериям. Действие выполняется только, если достигнуто соответствие всем критериям. Критериями могут быть адрес и порт источника, протокол IP (ICMP, UDP, TCP и т.д.), адрес и порт назначения, TOS и очередность (поля в IP-заголовке), а также длина. Критерий длины может быть

включен для дифференциации интерактивного трафика и трафика массивов данных. Интерактивные приложения, напр., telnet, обычно ориентированы на короткие пакеты, тогда как трафик массивов данных, напр., передача файлов, - на крупные.

Действия, которые могут быть выполнены, включают:

- маршрутизацию пакета к тому или иному шлюзу (следовательно, выходному интерфейсу)
- настройку полей TOS и очередности в IP-заголовке.

По характеру и реализации IPPR аналогична существующей функции фильтрации пакетов RAS. Стратегии группируются по наборам, каждый из которых состоит из родственных стратегий. Перед тем, как применить стратегии к интерфейсу или удаленному узлу, пользователь должен определить их так же, как фильтры. Всего может быть 12 наборов стратегий по шесть стратегий в каждом.

39.4 Настройка стратегии маршрутизации IP

В меню 25 показаны все задаваемые стратегии.

```
                Menu 25 - IP Routing Policy Setup

Policy                                  Policy
Set #          Name                     Set #          Name
------  -----------------               ------  -----------------
  1      test                             7      _________________
  2      _________________                8      _________________
  3      _________________                9      _________________
  4      _________________               10      _________________
  5      _________________               11      _________________
  6      _________________               12      _________________


            Enter Policy Set Number to Configure= 0

            Edit Name= N/A

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

Рис. 39-1 Меню 25 - Настройка стратегии маршрутизации IP

Для настройки стратегии маршрутизации следует выполнить описанную ниже процедуру:

Step 1. Введите "25" в Главном меню для перехода в **Меню 25 – Настройка стратегии маршрутизации IP**.

Step 2. Введите индекс набора стратегий, который нужно сконфигурировать, для перехода в **Меню 25.1 – Настройка стратегии маршрутизации IP**.

Меню 25.1 содержит сводку по набору стратегий, включая критерии и действие для отдельной стратегии, а также информацию, активна стратегия или нет. Каждая стратегия состоит из двух строк. Первая часть - это критерии входящего пакета, а вторая - действие. Разделитель "|", стоящий между двумя частями, означает, что действие выполняется при соответствии пакета критериям, а разделитель "=" - при несоответствии.

```
                    Menu 25.1 - IP Routing Policy Setup

  # A                          Criteria/Action
  - - ------------------------------------------------------------------------
  1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
      SP=20-25,DP=20-25,P=6,T=NM,PR=0              |GW=192.168.1.1,T=MT,PR=0
  2 N _____________________________________________________________________
      _____________________________________________________________________
  3 N _____________________________________________________________________
      _____________________________________________________________________
  4 N _____________________________________________________________________
      _____________________________________________________________________
  5 N _____________________________________________________________________
      _____________________________________________________________________
  6 N _____________________________________________________________________
      _____________________________________________________________________

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

Рис. 39-2 Меню 25.1 - Настройка стратегии маршрутизации IP

Табл. 39-1 Меню 25.1 - Настройка стратегии маршрутизации IP

СОКРАЩЕНИЕ		ЗНАЧЕНИЕ
Criterion	SA	IP-адрес источника
	SP	Порт источника
	DA	IP-адрес назначения
	DP	Порт назначения
	p	Номер протокола сетевого уровня 4 (TCP=6,UDP=17…)
	T	Тип услуги входящего пакета
	Pr	Очередность входящего пакета
Action	GW	IP-адрес шлюза
	T	Тип исходящей услуги
	p	Очередность исходящего пакета
Service	NM	Обычный

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
MD	Минимальная задержка
MT	Максимальная пропускная способность
MR	Максимальная надежность
MC	Минимальная стоимость

Введите число в диапазоне от 1 до 6 для вызова **Меню 25.1.1 – Стратегия маршрутизации IP** (см. следующий рисунок). Данное меню позволяет конфигурировать правила стратегии.

```
                                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= N/A
            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:

Press Space Bar to Toggle.
```

Рис. 39-3 Меню 25.1.1 - Стратегия маршрутизации IP

Следующая таблица описывает поля данного меню.

Табл. 39-2 Меню 25.1.1 - Стратегия маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
Policy Set Name (Имя набора стратегий)	Имя набора стратегий, присвоенное в **Меню 25 – Настройка стратегии маршрутизации IP**.
Active (Активно)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите **Yes** (для активации) или No (для дезактивации) стратегии. Неактивные стратегии обозначаются в Меню 25 SMT знаком минуса "–".
Criteria (Критерии):	

Табл. 39-2 Меню 25.1.1 - Стратегия маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
IP Protocol (Протокол IP)	Номер протокола сетевого уровня 4, например: **UDP**, **TCP**, **ICMP**, и т.д.
Type of Service (Тип услуги)	Определить приоритеты для входящего сетевого трафика путем выбора между **Don't Care (Все равно)**, **Normal (Обычно)**, **Min Delay (Минимальная задержка)**, **Max Thruput (Максимальная пропускная способность), Min Cost (Минимальная стоимость)** или **Max Reliable (Максимальная надежность)**.
Precedence (Очередность)	Значение очередности входящего пакета. Нажатием клавиш [SPACE BAR] и [ENTER] выберите значение в диапазоне от **0** до **7** или **Don't Care (Все равно)**.
Packet Length (Длина пакета)	Введите длину входящих пакетов (в байтах). Операторы в поле **Len Comp** (следующее поле) применяются к пакетам этой длины.
Len Comp (Определение длины пакета)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите одну из следующих опций: **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	Диапазон IP-адресов источника с начала до конца.
port start / end	Диапазон номеров портов источника с начала до конца; доступно только при TCP/UDP.
Destination (Назначение):	
addr start / end	Диапазон IP-адресов назначения с начала до конца.
port start / end	Диапазон номеров портов назначения с начала до конца; доступно только при TCP/UDP.
Action (Действие)	Определяет, должно ли выполняться действие при соответствии **Matched** или несоответствии **Not Matched** пакета критериям.
Gateway addr (Адрес шлюза)	Определяет адрес выходного шлюза. Шлюз должен находиться в той же подсети, что и OMNI ADSL, если он находится в LAN, в противном случае шлюзом должен быть IP-адрес удаленного узла. В качестве шлюза по умолчанию задано 0.0.0.0.
Type of Service (Тип услуг)	Установить новое значение TOS для исходящего пакета. Определить приоритеты для входящего сетевого трафика путем выбора между **No Change** (Без изменений), **Normal** (Обычно), **Min Delay** (Минимальная задержка), **Max Thruput** (Максимальная пропускная способность), **Max**

Табл. 39-2 Меню 25.1.1 - Стратегия маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
	Reliable (Максимальная надежность) или **Min Cost** (Минимальная стоимость).
Precedence (Очередность)	Установить новое значение очередности для исходящего пакета. Значения могут быть от **0** до **7** или **No Change** (Без изменений).
Log (Журнал)	Нажатием клавиш [SPACE BAR] и [ENTER] выберите **Yes** для внесения в системный журнал записи после выполнения стратегии.
По завершении работы в этом меню при появлении сообщения "Press [ENTER] to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены и возврата к предыдущему экрану.	

39.5 Применение стратегии IP

В данном разделе рассматривается применение стратегий IP после их создания.

39.5.1 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 выбрать до четырех наборов стратегий IP (из 12), введя их номера через запятую, напр., 2, 4, 7, 9.

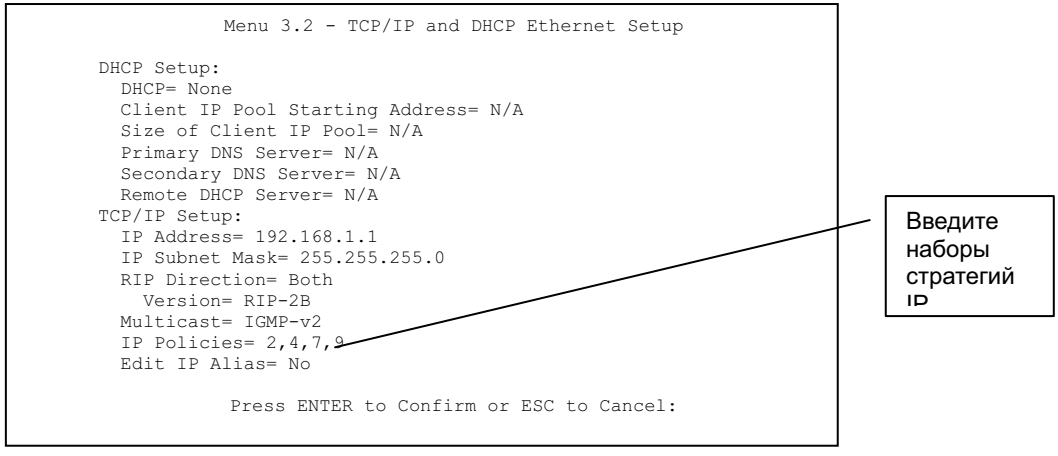


Рис. 39-4 Меню 3.2 - Настройка TCP/IP и DHCP для Ethernet

Войдите в Меню 11.3 (показано ниже) и введите номер(-а) набора(-ов) стратегий маршрутизации IP в соответствии с необходимостью. Можно последовательно задать до четырех наборов стратегий, введя их номера через запятую.

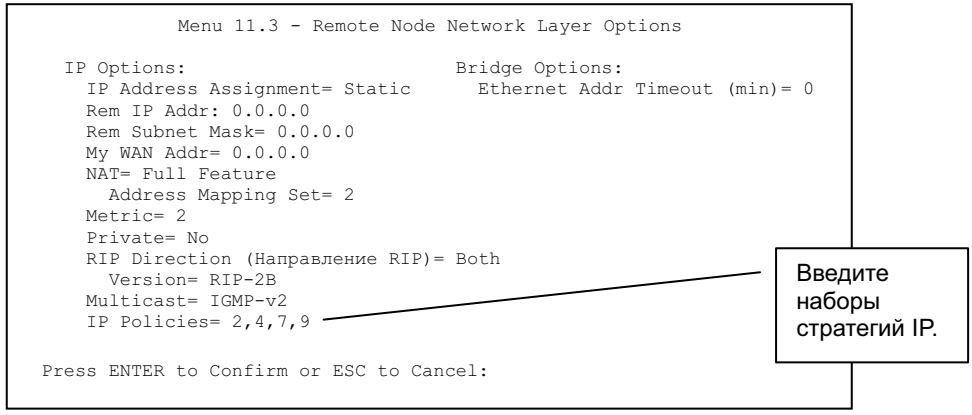


Рис. 39-5 Меню 11.3 - Опции сетевого уровня для удаленного узла

39.6 Пример маршрутизации на базе стратегии IP

Если сеть одновременно имеет соединения с Интернетом и удаленным узлом, можно маршрутизировать Web-пакеты в Интернет, используя одну стратегию, а FTP-пакеты в удаленную сеть, используя другую стратегию. См. следующий рисунок.

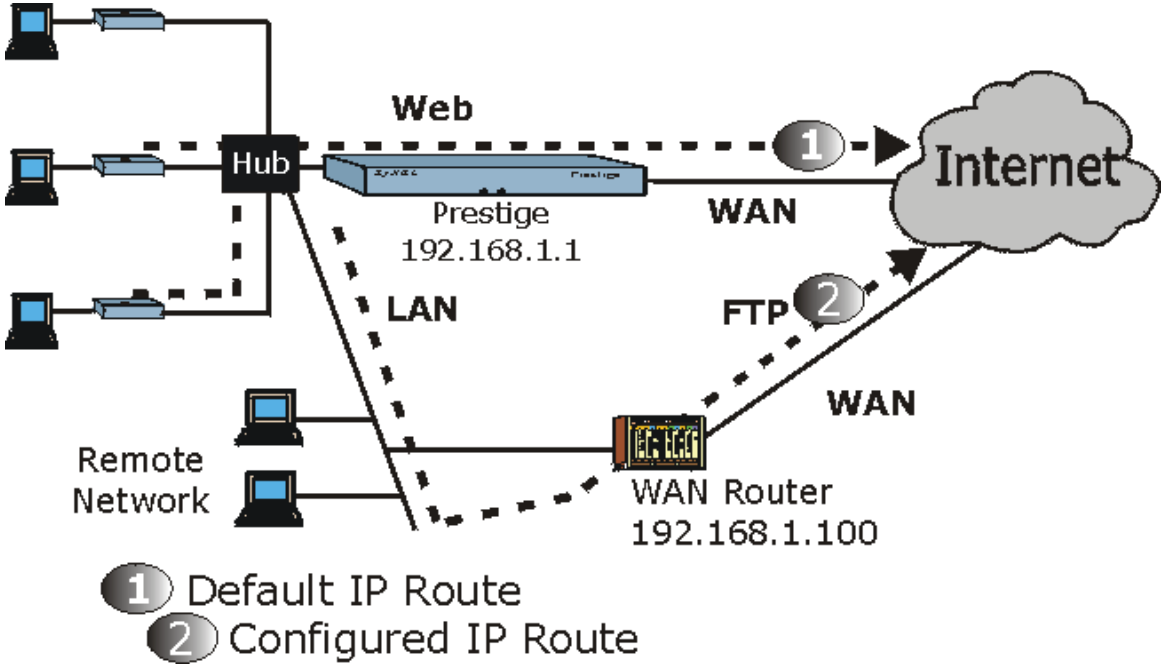


Рис. 396 Пример маршрутизации на базе стратегии IP

Для маршрутизации Web-пакетов, приходящих от клиентов с IP-адресами от 192.168.1.33 до 192.168.1.64, в Интернет через порт WAN OMNI ADSL, следует выполнить описанные ниже действия.

Step 1. Создать набор стратегий маршрутизации в Меню 25.

Step 2. Создать правило для этого набора в **Меню 25.1.1 - Стратегия маршрутизации IP**, как показано ниже.

```
                        Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set1
          Active= Yes
          Criteria (Критерии):
            IP Protocol    = 6
            Type of Service= Don't Care          Packet length= 10
            Precedence     = Don't Care            Len Comp= N/A
            Source: (Источник)
                addr start= 192.168.1.2      end= 192.168.1.64
                Port Start= 0                End= N/A
            Destination: (Адресат:)
              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:
Press Space Bar to Toggle.
```

Рис. 39-7 Пример маршрутизации на базе стратегии IP

Step 3. Войти в **Меню 25.1 - Настройка стратегии маршрутизации IP** и проверить, добавлено ли правило.

Step 4. Создать еще один набор стратегий маршрутизации в Меню 25.

Step 5. Создать правило в Меню 25.1 для этого набора, предназначенного для маршрутизации пакетов из любой хост-машины (IP=0.0.0.0 обозначает любую хост-машину) с протоколом TCP и доступом к порту FTP через другой шлюз (192.168.1.100).

```
                                  Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set2

          Active= Yes
          Criteria (Критерии):
            IP Protocol    = 6
            Type of Service= Don't Care             Packet length= 10
            Precedence     = Don't Care               Len Comp= N/A
            Source (Источник):
              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:
Press Space Bar to Toggle.
```

Рис. 39-8- Пример маршрутизации на базе стратегии IP

Step 6. Войти в **Меню 25.1 - Настройка стратегии маршрутизации IP** и проверить, добавлено ли правило.

Step 7. Применить оба набора стратегий в Меню 3.2, как показано ниже.

```
                    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:

  Press Space Bar to Toggle.
```

Рис. 39-9 Пример применения стратегии IP

Chapter 40
Составление плана вызовов

Функция составления плана вызовов (применяется только для инкапсуляции PPPoA или PPPoE) позволяет назначить время и продолжительность вызова удаленного узла.

40.1 Описание составления плана вызовов

Функция составления плана вызовов позволяет OMNI ADSL управлять удаленным узлом и определять, когда следует направлять вызов на удаленный узел и какой должна быть продолжительность вызова. Данная функция аналогична программе-планировщику видеомагнитофона (возможность назначения промежутка времени, в течение которого производится запись на видеомагнитофон). В **Меню 11.1 - Настройки пользователя для удаленного узла** можно назначить до четырех наборов планов. Находясь в Главном меню, введите "26" для доступа к **Меню 26 - Настройка планов**, показанному ниже.

```
                        Menu 26 - Schedule Setup

 Schedule                                Schedule
  Set #          Name                     Set #          Name (Имя)
 ------   -----------------              ------      ------------------
    1          AlwaysOn                     7          _______________
    2      _______________                  8          _______________
    3      _______________                  9          _______________
    4      _______________                 10          _______________
    5      _______________                 11          _______________
    6      _______________                 12          _______________

                    Enter Schedule Set Number to Configure=

                    Edit Name=

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

Рис. 40-1 Меню 26 - Настройка планов

Наборы с более низкими номерами имеют приоритет над наборами с более высокими номерами, благодаря чему исключаются конфликты при составлении планов. Напр., 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 OMNI ADSL по умолчанию сначала применяет наборы с более низкими номерами. Набор 2 будет иметь приоритет над наборами 3 и 4 и так далее.

Для одного удаленного узла можно разработать до 12 наборов планов, однако применить не больше четырех.

Для удаления набора плана введите его номер в поле Edit Name (Редактирование имени) **и нажмите клавиши** [SPACE BAR] **и** [ENTER] **(или удалить).**

Для настройки набора планов выберите набор из меню 26 (1-12) и нажмите клавишу [ENTER] для вызова **Меню 26.1 — Настройка набора планов**, показанного ниже.

```
                          Меню 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:
      Press Space Bar to Toggle
```

Рис. 40-2 Меню 26.1 - Настройка набора планов

Если соединение уже установлено, OMNI ADSL не сбрасывает его. Если соединение сбрасывается вручную или завершается, невозможно послать вызов на удаленный узел до истечения времени, указанного в поле **Duration (Продолжительность)**.

Табл. 40-1 Меню 26.1 - Настройка набора планов

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Active (Активно)	Нажатие клавиши [SPACE BAR] позволяет выбрать**Yes** или **No**. Выберите **Yes** и нажмите [ENTER] для активации набора планов.	**Yes**
Start Date (Начальная дата)	Введите дату начала действия набора в формате "год-месяц-день". Допускаются даты начиная с текущего дня и до 5 февраля 2036 года.	2000-01-01

Табл. 40-1 Меню 26.1 - Настройка набора планов

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
How Often (Как часто)	Возобновлять данный набор планов еженедельно или выполнить только один раз? Нажатием клавиш [SPACE BAR] и [ENTER] выберите одну из следующих опций: **Once (Однократно)** или **Weekly (Еженедельно)**. Эти варианта взаимно исключают друг друга. Если выберите **Once**, все поля дней недели будут недоступны (**N/A**). **Once** означает, что план автоматически удаляется после истечения времени его выполнения.	**Once (Однократно)**
Once (Однократно): Date (Дата)	Если в предыдущем поле **How Often**выбрано **Once**, введите в данное поле дату выполнения набора в формате год-месяц-день.	2000-01-01
Weekday (День недели): Day (День)	Если в поле **How Often** выбрано **Weekly**, задайте день (дни) выполнения (и возобновления) плана переключением в соответствующем поле (полях) и нажатием клавиши [SPACE BAR] для выбора **Yes**, а затем нажмите [ENTER].	**Yes** **No** **N/A**
Start Time (Начальное время)	Введите время начала действия набора в формате "час-минута".	09:00
Duration (Продолжительность)	Введите максимальное время разрешенного соединения в формате "час-минута".	08:00

Табл. 40-1 Меню 26.1 - Настройка набора планов

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Action (Активно)	**Forced On** (Продолжать) означает, что соединение поддерживается в независимости от наличия вызова-запроса на линии и сохраняется в течение времени, заданного в поле **Duration**. **Forced Down** (Отменить) означает, что соединение блокируется в независимости от наличия вызова-запроса на линии. **Enable Dial-On-Demand** (Включить набор по запросу) означает, что данный план допускает вызов-запрос на линии. **Disable Dial-On-Demand** (Отключить набор по запросу) означает, что данный план не допускает вызов-запрос на линии.	**Forced On**
После заполнения полей данного меню на запрос “Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для сохранения конфигурации или - клавишу [ESC] для ее отмены и возвращения к предыдущему экрану.		

После конфигурирования набора планов их нужно применить к требуемому удаленному узлу (узлам). Наберите в **Главном меню** "11", а затем введите индекс требуемого удаленного узла. Пользуясь клавишей [SPACE BAR] в поле **Encapsulation (Инкапсуляция)** , выберите тип **PPPoE** или **PPPoA** и нажмите клавишу [ENTER] для того чтобы он стал доступным (см. ниже).

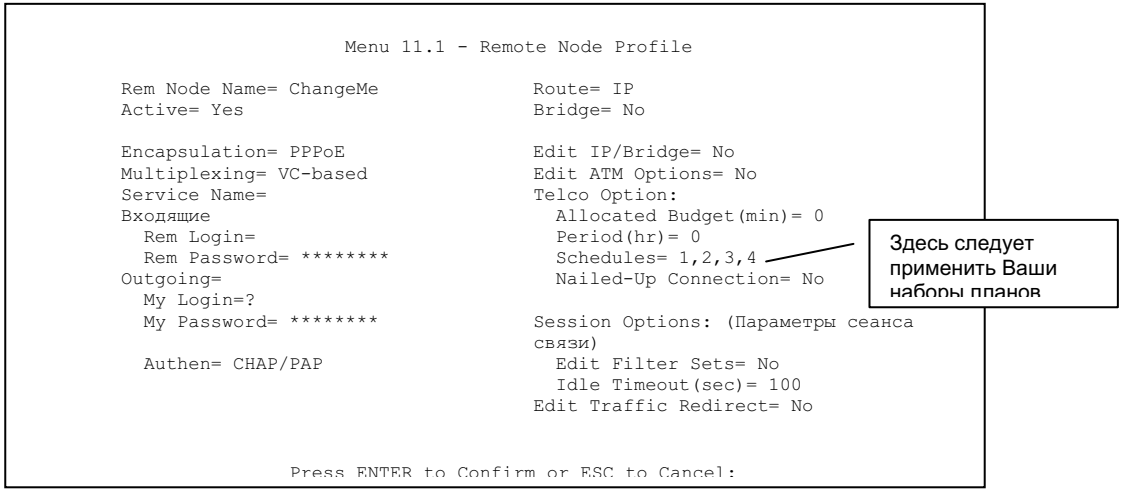


Рис. 40-3 Применение одного или нескольких наборов планов для удаленного узла (PPPoE)

Для одного удаленного узла можно применить до четырех наборов планов, введя их номера через запятую. Порядок выполнения наборов можно менять по своему усмотрению.

Part XI:

Системная консоль: VPN/IPSec (виртуальная частная сеть по протоколу IPSec) и Internal SPTGEN (внутренний генератор таблицы системных параметров)

В данной части описывается конфигурирование VPN/IPSec (виртуальной частной сети по протоколу IPSec) для обеспечения надежной связи и Internal SPTGEN (внутренний генератор таблицы системных параметров) маршрутизатора OMNI ADSL.

См. разделы данного руководства, посвященные описанию Web-конфигуратора, содержащие необходимую информацию о технических параметрах, задаваемых с его помощью и с помощью системной консоли.

Chapter 41
Настройка VPN/IPSec

В данной главе описываются меню SMT виртуальной частной сети.

41.1 Описание VPN/IPSec

Главное SMT-меню настройки VPN/IPSec содержит следующие основные подменю:

1. В подменю 27.1 задаются стратегии VPN, включая стратегии безопасности, IP-адреса конечных пунктов, IP-адрес удаленного маршрутизатора и управление ключами.
2. **Меню 27.2 - SA Monitor** (Монитор соглашений по безопасности) позволяет управлять (обновлять или разрывать) SA-соединениями.

Описание структуры меню VPN.

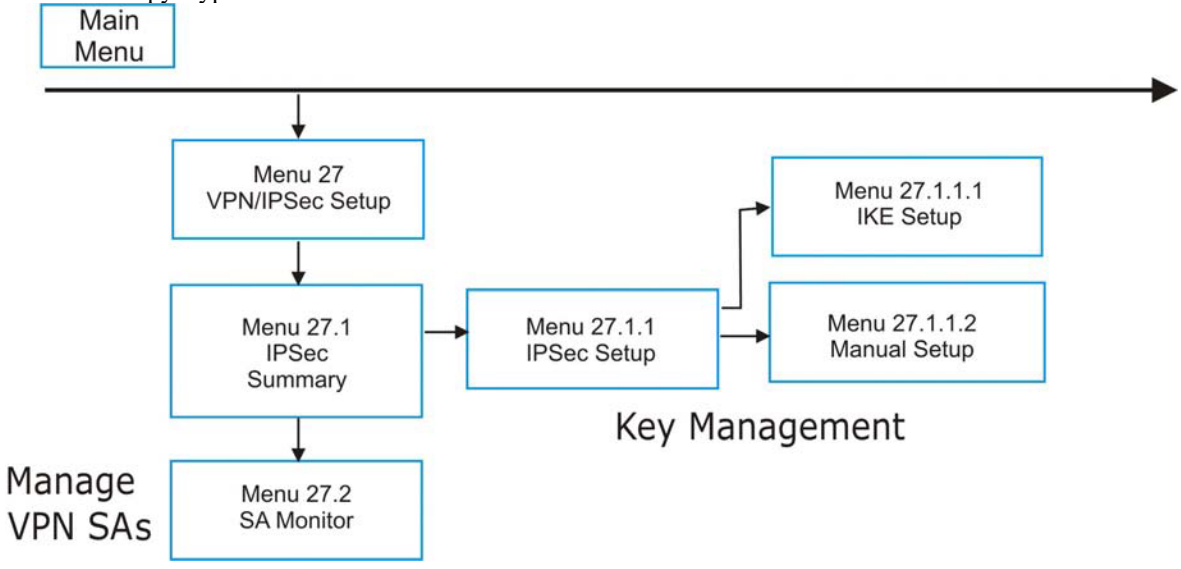


Рис. 41-1 Структура меню SMT VPN

В Главном меню введите "27" для вывода первого меню VPN, представленного ниже.

```
                    Menu 27 - VPN/IPSec Setup

              1. IPSec Summary
              2. SA Monitor
              3. View IPSec Log


                    Enter Menu Selection Number:
```

Рис. 41-2 Меню 27 — Настройка VPN/IPSec

41.2 Экран сводки IPSec

В меню 27 наберите "1" и нажмите клавишу [ENTER] для перехода в **Меню 27.1 — Сводка по IPSec**. Это информационное меню (только для чтения) о правилах (туннелях) конкретного применения IPSec. Редактировать или создавать правила IPSec можно в соответствующих подменю, выбрав указатель интересующего правила.

```
                              Menu 27.1 - IPSec Summary

#        Name      A   Local Addr Start      - Addr End / Mask     Encap     IPSec Algorithm
         Key Mgt       Remote Addr Start     - Addr End / Mask               Secure GW Addr
---      --------  -   ------------------    ------------------    ------    ------------------
001      Taiwan    Y   192.168.1.35          192.168.1.38          Tunnel    ESP DES MD5
         IKE           172.16.2.40           172.16.2.46                     193.81.13.2
002      zw50      N   1.1.1.1               1.1.1.1               Tunnel    AH SHA1
         IKE           4.4.4.4               255.255.0.0                     zw50test.zyxel.
003      China     N   192.168.1.40          192.168.1.42          Tunnel    ESP DES MD5
         IKE           N/A                   N/A                             0.0.0.0
004

005


              Select Command= None                              Select Rule= N/A
                        Press ENTER to Confirm or ESC to Cancel:
```

Рис. 41-3 Меню 27.1 — Сводка по IPSec

Следующая таблица описывает поля данного меню.

Табл. 41-1 Меню 27.1 — Сводка по IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
# (Индекс)	Индекс стратегии VPN.	1
Name (Имя)	В этом поле указывается уникальное идентификационное имя данного правила VPN. Имя может содержать до 32 символов, но в поле отображается не более десяти.	Taiwan
A (Активно)	**Y** в этом поле означает, что данное правило VPN активно.	**Y**
Local Addr Start (Первый локальный IP-адрес)	Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **Single**, то в это поле вводится статический IP-адрес в локальной сети за OMNI ADSL. Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **Range**, то в это поле вводится первый IP-адрес (статический) из набора компьютеров в локальной сети за OMNI ADSL. Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **SUBNET**, то в это поле вводится статический IP-адрес в локальной сети за OMNI ADSL.	192.168.1.35
Addr End / Mask (Последний IP-адрес/Маска подсети)	Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **Single**, то в этом поле указывается тот же IP-адрес (статический), что и в поле **Local Addr Start**. Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **Range**, то в это поле вводится последний IP-адрес (статический) из набора компьютеров в локальной сети за OMNI ADSL. Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **SUBNET**, то в это поле вводится маска подсети в локальной сети за OMNI ADSL.	192.168.1.38
Encap	В этом поле указывается **Tunnel (Туннельный)** или **Trunsport (Транспортный)** режим. Описание обоих режимов см. выше. Если появляются символы **???**, необходимо завершить конфигурирование стратегии VPN в меню 27.1.1.1 или 27.1.1.2.	**Tunnel**

Табл. 41-1 Меню 27.1 — Сводка по IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
IPSec Algorithm (Алгоритм шифрования)	В этом поле отображаются протоколы защиты данных, использующиеся для соединения SA. Протокол **ESP** обеспечивает конфиденциальность и целостность данных шифрованием и инкапсуляцией в пакеты IP. В состав методов защиты входят: 56-битовый алгоритм **DES** и 168-битовый алгоритм **3DES**. Признак **NULL** указывает на туннель без шифрования. Протокол **AH** (Authentication Header/Аутентифицирующий заголовок) обеспечивает надежность целостности и аутентификации путем включения аутентифицирующих данных в IP-пакеты. Эта информация определяется в зависимости от содержания заголовка и полей данных в IP-пакете. Это позволяет получить дополнительный уровень защиты. Для протокола **AH** можно выбрать алгоритм **MD5** (по умолчанию - 128 бит) и **SHA - 1**(160 бит)**.** Как **AH**, так и **ESP** повышают требования к объему обработки данных в OMNI ADSL и увеличивают время ожидания связи (задержку). Если появляются символы **???**, необходимо завершить конфигурирование стратегии VPN в меню 27.1.1.1 или 27.1.1.2.	**ESP DES MD5**
Key Mgt (Управление ключами)	В этом поле указывается тип управления ключами для соединения SA (**IKE** или **Manual (Ручное)**).	**IKE**
Remote Addr Start (Первый удаленный IP-адрес)	Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **Single**, то в это поле вводится IP-адрес (статический) в сети, находящейся за удаленным IPSec-маршрутизатором. Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **Range**, то в это поле вводится первый IP-адрес (статический) из набора компьютеров в сети, находящейся за удаленным IPSec-маршрутизатором. Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **SUBNET**, то в это поле вводится IP-адрес (статический) в сети, находящейся за удаленным IPSec-маршрутизатором. Если в поле **Secure Gateway Addr** в меню SMT 27.1.1 установлено 0.0.0.0, данное поле недоступно (**N/A.**)	172.16.2.40

Табл. 41-1 Меню 27.1 — Сводка по IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Remote Addr End (Удаленный конечный адрес)	Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **Single**, то в этом поле указывается тот же IP-адрес (статический), что и в поле **Remote Addr Start**. Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **Range**, то в это поле вводится последний IP-адрес (статический) из набора компьютеров в сети, находящейся за удаленным IPSec-маршрутизатором. Если в поле **Addr Type** в **Меню 27.1.1 - Настройка IPSec** указано **SUBNET**, то в этом поле указывается маска подсети в сети, находящейся за удаленным IPSec-маршрутизатором. Если в поле **Secure Gateway Addr** в меню SMT 27.1.1 установлено 0.0.0.0, данное поле недоступно (**N/A**)	172.16.2.46
Secure GW Addr (IP-адрес шлюза безопасности)	В этом поле указывается IP-адрес в глобальной сети или имя домена (выводятся первые 15 символов) маршрутизатора IPSec, с которым устанавливается VPN-соединение. Если в поле **Secure Gateway Addr** в меню SMT 27.1.1 установлено 0.0.0.0, в данном поле появляется **0.0.0.0**.	193.81.13.2
Select Command (Выбор команд)	С помощью клавиши [SPACE BAR] выберите одну из команд **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** или **Previous Page**, а затем нажмите [ENTER]. При выборе команды **Edit**, Delete или **Go To** необходимо в следующем поле указать правило. Для перехода к подсказке “Press ENTER to Confirm…” выберите **None** и нажмите [ENTER]. Для создания или редактирования правила выберите **Edit**. Для удаления правила выберите **Delete**. Прежде чем редактировать или удалять правило, удостоверьтесь, что Вы находитесь на нужной странице меню. После удаления одного из правил VPN следующие за ним по списку правила не сдвигаются наверх. Для перехода к странице с нужным правилом выберите команду **Go To Rule**. Для просмотра следующей или предыдущей страницы выберите **Next Page** или **Previous Page,** соответственно.	**None**
Select Rule	Введите индекс правила VPN, которое Вы хотите редактировать или удалить, а затем нажмите [ENTER].	3

Табл. 41-1 Меню 27.1 — Сводка по IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
По завершении работы в Меню при появлении сообщения "Press Enter to Confirm…" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены.		

41.3 Настройка IPSec

Выберите в поле **Select Command (Выбор команды)**опцию **Edit (Редактировать)**; введите порядковый номер правила в поле **Select Rule (Выбор правила)** и нажмите клавишу [ENTER] для редактирования настроек VPN с использованием приведенного ниже меню.

Чтобы полностью настроить и работать с VPN, необходимо также заполнить поля в меню 27.1.1.1 или 27.1.1.2..

```
                    Menu 27.1.1 - IPSec Setup

Index= 1          Name= Taiwan
Active= Yes       Keep Alive= No
Local ID type= IP       Content=
My IP Addr= 0.0.0.0
Peer ID type= IP        Content=
Secure Gateway Address= zw50test.zyxel.com.tw
Protocol= 0             DNS Server= 0.0.0.0
Local:          Addr Type= SINGLE
           IP Addr Start= 1.1.1.1           End/Subnet Mask= N/A
              Port Start= 0                 End= N/A
Remote:         Addr Type= SUBNET
           IP Addr Start= 4.4.4.4           End/Subnet Mask= 255.255.0.0
              Port Start= 0                 End= N/A
Enable Replay Detection = No
Key Management= IKE
Edit Key Management Setup= No


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

Рис. 41-4 Меню 27.1.1 — Настройка IPSec

Следующая таблица описывает поля данного меню.

Табл. 41-2 Меню 27.1.1 — Настройка IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Index	Порядковый номер правила VPN, выбранного в предыдущем меню.	**1**
Name (Имя)	Уникальное идентификационное имя данного правила VPN. Имя может содержать до 32 символов, но в **Меню 27.1 - Сводка по IPSec** отображаются только первые 10.	Taiwan
Active (Активно)	Клавишей [SPACE BAR] выберите **Yes** или **No**. Чтобы активизировать туннель VPN, выберите **Yes** и нажмите [ENTER]. Данное поле определяет применение правила VPN до того, как пакет покинет брандмауэр.	**Yes**
Keep Alive (Поддержание соединения активным)	Нажатием клавиши [SPACE BAR] выберите одну из двух опций: **Yes** или **No**. Выберите **Yes** и нажмите клавишу [ENTER], что обеспечивает автоматическое выполнение OMNI ADSL повторной инициализации соединения SA по истечении времени жизни SA, даже при отсутствии трафика. Удаленный маршрутизатор IPSec также должен иметь включенной функцию поддержания соединения для ее выполнения.	**No**

Табл. 41-2 Меню 27.1.1 — Настройка IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Local ID type (Тип идентификации)	Нажатием клавиши [SPACE BAR] выберите **IP**, **DNS**, или **E-mail** и нажмите клавишу [ENTER]. Выберите опцию **IP** для идентификации данного устройства OMNI ADSL по его IP-адресу. Выберите опцию **DNS** для идентификации данного устройства OMNI ADSL по его доменному имени. Выберите опцию **E-mail** для идентификации данного устройства OMNI ADSL по его E-Mail адресу.	
Content (Содержание)	Если в поле **Local ID Type**выбрана опция **IP**, введите IP-адрес компьютера или оставьте это поле незаполненным для того, чтобы устройство OMNI ADSL могло автоматически использовать собственный IP-адрес. Если в поле **Local ID Type** выбрана опция **DNS**, введите значение доменного имени (до 31 символа) для идентификации данного устройства OMNI ADSL. Если в поле **Local ID Type** выбрана опция **E-mail**, введите любой E-Mail адрес (до 31 символа) для идентификации данного устройства OMNI ADSL. Имя домена или E-Mail адрес, набранные в поле **Content**, используются только для идентификации и не являются фактическими.	
My IP Addr (IP-адрес OMNI ADSL)	Введите IP-адрес OMNI ADSL. Если в этом поле оставить значение 0.0.0.0, то при открытии туннеля VPN OMNI ADSL будет использовать свой текущий IP-адрес в глобальной сети (статический или динамический). При изменении IP-адреса туннель VPN необходимо перестроить.	0.0.0.0
Peer ID type (Тип идентификации)	Нажатием клавиши [SPACE BAR] выберите **IP**, **DNS**, или **E-mail** и нажмите клавишу [ENTER]. Выберите опцию **IP** для идентификации удаленного маршрутизатора IPSec по его IP-адресу. Выберите опцию **DNS** для идентификации удаленного маршрутизатора IPSec по его доменному имени. Выберите опцию **E-mail** для идентификации удаленного маршрутизатора по его E-Mail адресу.	

Табл. 41-2 Меню 27.1.1 — Настройка IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Content (Содержание)	При выборе в поле **Peer ID Type** опции **IP** , введите IP-адрес компьютера, с которым будет устанавливаться соединение VPN, или оставьте его незаполненным, для того чтобы OMNI ADSL автоматически пользовался адресом из поля **Secure Gateway Address**. Если в поле **Peer ID Type** выбрана опция **DNS**, введите значение доменного имени (до 31 символа) для идентификации удаленного маршрутизатора IPSec . Если в поле **Peer ID Type** выбрана опция **E-mail**, введите любой E-Mail адрес (до 31 символа) для идентификации маршрутизатора IPSec. Имя домена или E-Mail адрес, набранные в поле **Content**, используются только для идентификации и не являются фактическими. Имя домена также должно отличаться от IP-адреса удаленного маршрутизатора или набранного ниже в поле **Secure Gateway Address**.	
Secure Gateway Address (IP-адрес шлюза безопасности)	В этом поле указывается IP-адрес в глобальной сети или имя домена (до 31 символа) маршрутизатора IPSec, с которым устанавливается VPN-соединение. Если удаленный маршрутизатор IPSec имеет динамический IP-адрес в глобальной сети, в данном поле необходимо выставить 0.0.0.0 (в поле **Key Management** должно быть указано **IKE**, см. далее).	Zw50test.com.tw
Protocol (Протокол)	Введите "1" для ICMP, "6" - для TCP, "17" - для UDP, и т.д.. "0" - установлен по умолчанию и означает "любой протокол".	0
DNS Server (Сервер DNS)	Если имеется частный сервер DNS, обслуживающий VPN, введите здесь его IP-адрес. OMNI ADSL назначает этот дополнительный сервер DNS клиентам DHCP устройства OMNI ADSL, имеющим IP-адрес в диапазоне локальных адресов, установленном правилом IPSec. Сервер DNS помогает клиентам VPN отыскать другие компьютеры и серверы VPN по их (частным) доменным именам.	

Табл. 41-2 Меню 27.1.1 — Настройка IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Local (Локальный)	Локальные IP-адреса должны быть статическими и соответствовать заданным IP-адресам удаленного маршрутизатора IPSec. Два активных соединения SA не могут иметь один и тот же локальный и удаленный IP-адрес (адреса) одновременно. Два активных соединения SA могут иметь один и тот же локальный или удаленный IP-адрес, но не оба сразу. Можно сконфигурировать несколько соединений SA между одинаковыми локальным и удаленным IP-адресами, но при этом активным в любой момент времени может быть только одно из них.	
Addr Type (Тип IP-адреса)	С помощью клавиши [SPACE BAR] выберите **SINGLE**, **RANGE** или **SUBNET** и нажмите [ENTER]. Для единичного IP-адреса выберите **SINGLE**. Для нескольких адресов подряд выберите **RANGE**. Чтобы указать в качестве IP-адресов в сети значение маски подсети, выберите **SUBNET**.	**SINGLE**
IP Addr Start (Первый IP-адрес)	Если в поле **Addr Type** указано **Single**, введите в данном поле статический IP-адрес локальной сети, расположенной за устройством Perstige. Если в поле **Addr Type** указано **Range**, введите в данном поле первый IP-адрес (статический) одного из компьютеров в локальной сети, расположенной за OMNI ADSL. Если в поле **Addr Type** указано **SUBNET**, то в данном поле отображается IP-адрес (статический) в локальной сети, расположенной за OMNI ADSL.	192.168.1.35
End/Subnet Mask (Последний IP-адрес/Маска посети)	Если в поле **Addr Type** указано **Single**, данное поле недоступно (**N/A**). Если в поле **Addr Type** указано **Range**, введите в данном поле последний IP-адрес (статический) одного из компьютеров в локальной сети, расположенной за OMNI ADSL. Если в поле **Addr Type** указано **SUBNET**, то в данном поле отображается маска подсети для локальной сети, расположенной за OMNI ADSL.	192.168.1.38

Табл. 41-2 Меню 27.1.1 — Настройка IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Port Start (Первый номер порта)	"0" устанавливается по умолчанию и означает любой порт. Введите номер порта (от 0 до 65535). Невозможно создать туннель VPN, если Вы пытаетесь установить соединение, пользуясь неправильным номером порта или номером, не принадлежащим указанному выше диапазону значений. Ниже приведены некоторые известные номера портов: 21 - FTP; 53 - DNS; 23 - Telnet; 80 - HTTP; 25 - SMTP; 110 - POP3	0
End (Последний номер порта)	Укажите в данном поле номер порта, замыкающий диапазон портов. Это значение должно быть больше заданного в предыдущем поле. Если в поле **Port Start** задано "0", данное поле недоступно (**N/A**).	N/A
Remote (Удаленный IP-адрес)	Удаленные IP-адреса должны быть статическими и соответствовать заданным локальным IP-адресам удаленного маршрутизатора IPSec. Если в поле **Secure Gateway Address** задано 0.0.0.0, данные поля недоступны (**N/A**). Два активных соединения SA не могут иметь один и тот же локальный и удаленный IP-адрес (адреса) одновременно. Два активных соединения SA могут иметь один и тот же локальный или удаленный IP-адрес, но не оба сразу. Можно сконфигурировать несколько соединений SA между одинаковыми локальным и удаленным IP-адресами, но при этом активным в любой момент времени может быть только одно из них.	
Addr Type (Тип IP-адреса)	С помощью клавиши [SPACE BAR] выберите **SINGLE**, **RANGE** или **SUBNET** и нажмите [ENTER]. Для единичного IP-адреса выберите **SINGLE**. Для нескольких адресов подряд выберите **RANGE**. Чтобы указать в качестве IP-адресов в сети значение маски подсети, выберите **SUBNET**.	**SUBNET**

Табл. 41-2 Меню 27.1.1 — Настройка IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
IP Addr Start (Первый IP-адрес)	Если в поле **Addr Type** указано **Single**, введите в данном поле статический IP-адрес в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Addr Type** указано **Range**, введите в данном поле первый IP-адрес (статический) одного из компьютеров в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Addr Type** указано **SUBNET**, введите в данном поле IP-адрес (статический) в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Secure Gateway Address** установлено 0.0.0.0, данное поле недоступно (**N/A**)	4.4.4.4
End/Subnet Mask (Последний IP-адрес/Маска подсети)	Если в поле **Addr Type** указано **Single**, данное поле недоступно (**N/A**). Если в поле **Addr Type** указано **Range**, введите в данном поле последний IP-адрес (статический) одного из компьютеров в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Addr Type** указано **SUBNET**, введите в данном поле значение маски подсети в сети, расположенной за удаленным маршрутизатором IPSec. Если в поле **Secure Gateway Address** установлено 0.0.0.0, данное поле недоступно (**N/A**)	255.255.0.0
Port Start (Первый номер порта)	"0" устанавливается по умолчанию и означает любой порт. Введите номер порта (от 0 до 65535). Если кто-то за удаленным маршрутизатором IPSec попытается установить связь, пользуясь неправильным номером порта или не соответствующим указанному выше диапазону, то он не сможет создать туннель VPN. Ниже приведены некоторые известные номера портов: 21 - FTP; 53 - DNS; 23 - Telnet; 80 - HTTP; 25 - SMTP; 110 - POP3.	0
End (Последний номер порта)	Укажите в данном поле номер порта, замыкающий диапазон портов. Это значение должно быть больше заданного в предыдущем поле. Если в поле **Port Start** задано "0", данное поле недоступно (**N/A**).	

Табл. 41-2 Меню 27.1.1 — Настройка IPSec

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Enable Replay Detection (Включение распознавания повторов)	Поскольку создание VPN ведет к увеличению интенсивности обработки, система становится более уязвима для атак "Отказ от обслуживания" (DoS). Получатель пакета, использующий протокол IPSec, может обнаружить, что такой пакет уже передавался, и отказаться от приема дублирующего пакета, обеспечивая тем самым защиту от атак, пользующихся механизмом повторной передачи. Выбор **Yes** в данном поле активизирует эту функцию. Нажатием клавиши [SPACE BAR] выберите **Yes** или **No**. Чтобы включить функцию защиты от повторов выберите **Yes** и нажмите клавишу [ENTER].	**No**
Key Management (Управление ключами)	С помощью клавиши [SPACE BAR] выберите в данном поле **IKE** или **Manual,** а затем нажмите [ENTER]. **Ручное** управление ключами может быть полезно для поиска и устранения неисправностей в случае, если возникают какие-либо проблемы при использовании **IKE**.	**IKE**
Edit Key Management Setup (Настройка ручного управления ключами)	Для конфигурирования настроек управления ключами смените с помощью клавиши [SPACE BAR] установленное по умолчанию **No** на **Yes**, а затем нажмите [ENTER] для перехода в меню управления ключами (описано далее). Если в поле **Key Management** установлено **IKE**, произойдет переход в **Меню 27.1.1.1 – Настройка IKE**. Если в поле **Key Management** установлено **Manual**, произойдет переход в **Меню 27.1.1.2 – Настройка ручного управления ключами**.	**No**
По завершении работы в Меню при появлении сообщения "Press Enter to Confirm…" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены.		

41.4 IKE Setup

Для работы в этом меню поле **Key Management (Управление ключами)** в **Меню 27.1.1 – Настройка IPSec** должно быть установлено **IKE**. Установите курсор в поле **Edit Key Management Setup (Настройка управления ключами)** в **Меню 27.1.1 – Настройка IPSec**; нажатием клавиши [SPACE BAR] выберите **Yes**, а затем нажмите [ENTER] для перехода в **Меню 27.1.1.1 – Настройка IKE**.

```
                    Menu 27.1.1.1 - IKE Setup

          Phase 1
            Negotiation Mode= Main
            PSK= 123456789
            Encryption Algorithm= DES
            Authentication Algorithm= SHA1
            SA Life Time (Seconds)= 28800
            Key Group= DH1

          Phase 2
            Active Protocol  = ESP
            Encryption Algorithm  = DES
            Authentication Algorithm  = SHA1
            SA Life Time (Seconds)= 28800
            Encapsulation  = Tunnel
            Perfect Forward Secrecy (PFS)= None


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

Рис. 41-5 Меню — Настройка IKE

Следующая таблица описывает поля данного меню.

Табл. 41-3 Меню 27.1.1.1 - Настройка IKE

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Phase 1		
Negotiation Mode (Режим согласования)	С помощью клавиши [SPACE BAR] выберите **Main** или **Aggressive,** а затем нажмите [ENTER]. Описание обоих режимов см. выше. Для нескольких соединений SA через безопасный шлюз должен быть установлен один и тот же режим согласования.	**Main**
PSK (Pre-Shared Key) (Предварительно согласованные ключи)	Шлюзы OMNI ADSL аутентифицируют сеанс обмена ключами в VPN путем сравнения предварительно согласованных ключей. Предварительно согласованные ключи лучше всего подходят для небольших сетей с количеством узлов менее десяти. укажите в данном поле свой предварительно согласованный ключ; можно ввести до 31 символа. Допускаются любые символы, включая пробелы, однако пробелы в конце строки удаляются. Обоими конечными устройствами туннеля VPN должен использоваться один и тот же предварительно согласованный ключ. Если таковой не используется, вы получите пакет “PYLD_MALFORMED” (уведомление о наличии искажения).	

Табл. 41-3 Меню 27.1.1.1 - Настройка IKE

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Encryption Algorithm (Алгоритм шифрования)	При использовании стандарта **DES** как отправляющая, так и принимающая сторона должны знать один и тот же секретный ключ, с помощью которого осуществляется шифрование и дешифрование сообщений, а также генерация и проверка аутентификационного кода сообщений. Алгоритм шифрования **DES** в OMNI ADSL использует 56-битовый ключ. Алгоритм Triple DES (**3DES**) - это разновидность DES, использующая 168-битный ключ. Как следствие, алгоритм **3DES** надежнее протокола **DES**. Однако он также требует большей производительности системы, что отражается в увеличении времени ожидания и в уменьшении пропускной способности. С помощью клавиши [SPACE BAR] выберите **3DES** или **DES,** и затем нажмите [ENTER].	**DES**
Authentication Algorithm (Алгоритм аутентификации)	Для аутентификации пакетных данных используются алгоритмы хэширования **MD5** (Message Digest 5 (Дайджест сообщения 5)) и **SHA1** (Secure Hash Algorithm (Алгоритм безопасного хэширования)). Алгоритм **SHA1** в целом более надежен, чем **MD5**, но несколько медленнее. С помощью клавиши [SPACE BAR] выберите **SHA1** или **MD5,** и затем нажмите [ENTER].	**SHA1**
SA Life Time (Seconds) (Время жизни SA, в сек)	В этом поле необходимо указать время, которое должно пройти до того, как согласование безопасного соединения по обмену ключами начнется заново. Можно задать значение в пределах от 60 до 3000000 секунд (почти 35 дней). Малое время **SA Life Time** повышает безопасность, так как шлюзам VPN приходится чаще обновлять шифрующие и аутентифицирующие ключи. Однако при обновлении согласования по созданию туннеля VPN все пользователи, имеющие в этот момент доступ к удаленным ресурсам, будут временно отключены.	28800 (по умолчанию)
Key Group (Группа ключей)	Необходимо выбрать группу ключей для первой фазы обмена ключами. **DH1** (по умолчанию) означает группу Диффи-Хеллмана 1: 768-битное случайное число. **DH2** означает группу Диффи-Хеллмана 2: 1024-битное случайное число.	**DH1**
Phase 2 (Фаза 2)		
Active Protocol (Активный протокол)	С помощью клавиши [SPACE BAR] выберите **ESP** или **AH,** и затем нажмите [ENTER]. Описание обоих протоколов см. выше.	**ESP**

Табл. 41-3 Меню 27.1.1.1 - Настройка IKE

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Encryption Algorithm (Алгоритм шифрования)	Нажатием клавиши [SPACE BAR] выберите **NULL**, **3DES** или **DES**, а затем нажмите клавишу [ENTER]. Для настройки туннеля без шифрования выберите **NULL**.	**DES**
Authentication Algorithm (Алгоритм аутентификации)	С помощью клавиши [SPACE BAR] выберите **SHA1** или **MD5,** и затем нажмите [ENTER].	**MD5**
SA Life Time (Seconds) (Время жизни SA, в сек)	В этом поле необходимо указать время, которое должно пройти до того, как согласование безопасного соединения по обмену ключами начнется заново. Можно задать значение в пределах от 60 до 3000000 секунд (почти 35 дней).	28800 (по умолчанию)
Encapsulation (Инкапсуляция)	С помощью клавиши [SPACE BAR] выберите режим **Tunnel** (Туннельный) или **Transport** (Транспортный), а затем нажмите [ENTER]. Описание обоих режимов см. выше.	**Tunnel**
Perfect Forward Secrecy (PFS) (Совершенная прямая секретность)	Во второй фазе создания SA-соединения для IPSec функция Perfect Forward Secrecy (PFS) по умолчанию отключена (**None**). Это позволяет увеличить скорость создания IPSec, однако снижает безопасность. Нажатием клавиши [SPACE BAR] выберите одну из опций: **DH1** или **DH2** для включения режима PFS. **DH1** означает группу Диффи-Хеллмана 1: 768-битовое случайное число. **DH2** означает группу Диффи-Хеллмана 2: 1024-битовое (1 Кб) случайное число (более безопасно, но работает медленнее).	**None**
По завершении работы в Меню при появлении сообщения "Press Enter to Confirm…" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены.		

41.5 Настройка ручного управления ключами

Работа в **Меню 27.1.1.2 – Настройка ручного управления ключами** возможна только если в поле **Key Management** в **Меню 27.1.1 – Настройка IPSec** установлено **Manual**. Ручное управление ключами может быть полезно в случае, если возникают какие-либо проблемы при использовании управления **IKE**.

41.5.1 Active Protocol

В этом поле задается комбинация режимов и протоколов обеспечения безопасности, использующихся VPN. См. раздел руководства с описанием работы Web-конфигуратора с VPN для получения дополнительной информации об этих параметрах.

Табл. 41-4 Активный протокол: инкапсуляция и протокол обеспечения безопасности

MODE	ПРОТОКОЛ БЕЗОПАСНОСТИ
Tunnel (Туннельный)	ESP
Transport (Транспортный)	AH

41.5.2 Индекс параметра безопасности (Security Parameter Index, SPI)

Для работы в данном меню следует переместить курсор в поле **Edit Manual Setup** в **Меню 27.1.1 – Настройка IPSec**, нажатием клавиши [SPACE BAR] установите **Yes**, а затем нажмите [ENTER] для перехода в **Меню 27.1.1.2 – Настройка ручного управления ключами**.

```
          Menu 27.1.1.2 - Manual Setup
Active Protocol= ESP Tunnel

ESP Setup
  SPI (Decimal)=
  Encryption Algorithm= DES
    Key1=
    Key2= N/A
    Key3= N/A
  Authentication Algorithm= MD5
    Key= N/A

AH Setup
  SPI (Decimal)= N/A
  Authentication Algorithm= N/A
    Key=

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

Рис. 41-6 Меню 27.1.1.2 - Настройка ручного управления ключами

Следующая таблица описывает поля данного меню.

Табл. 41-5 Меню 27.1.1.2 - Настройка ручного управления ключами

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Active Protocol (Активный протокол)	С помощью клавиши [SPACE BAR] выберите **ESP Tunnel**, **ESP Transport**, **AH Tunnel** или **AH Transport**, а затем нажмите [ENTER]. Если выбран вариант с **ESP**, поля **AH Setup** - недоступны (**N/A**)	**ESP Tunnel**

Табл. 41-5 Меню 27.1.1.2 - Настройка ручного управления ключами

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
ESP Setup (Установка ESP)	Если в качестве **активного протокола** выбран **AH**, поля **настройки ESP** - недоступны (**N/A)**.	
SPI (Decimal) (SPI (десятичный))	Введите значение десятичного числа в диапазоне от 1 до 999999 для задания SPI (индекса параметров безопасности).	1234
Encryption Algorithm (Алгоритм шифрования)	Нажатием клавиши [SPACE BAR] выберите **NULL**, **3DES** или **DES**, а затем нажмите клавишу [ENTER]. Заполните поле **Key1** (ниже) при выборе опции **DES** и поля **Key1** - **Key3** при выборе **3DES**. Для настройки туннеля без шифрования выберите **NULL**. При выборе **NULL** шифровальные ключи не указываются.	**DES**
Key1 (Ключ 1)	Введите уникальный ключ из восьми символов. Допускаются любые символы, включая пробелы, однако пробелы в конце строки удаляются. Если выбрано **DES**, заполнить поле **Key1**, если **3DES** - заполнить поля **Key1** - **Key3**.	89abcde
Key2 (Ключ 2)	Введите уникальный ключ из восьми символов. Допускаются любые символы, включая пробелы, однако пробелы в конце строки удаляются.	
Key3 (Ключ 3)	Введите уникальный ключ из восьми символов. Допускаются любые символы, включая пробелы, однако пробелы в конце строки удаляются.	
Authentication Algorithm (Алгоритм аутентификации)	С помощью клавиши [SPACE BAR] выберите **MD5** или **SHA1,** а затем нажмите [ENTER].	**MD5**
Key (Ключ)	Введите ключ аутентификации, который при необходимости будет использовать IPSec. Ключ должен быть уникальным. Введите 16 символов в случае аутентификации по алгоритму **MD5** и 20 - для **SHA-1**. Допускаются любые символы, включая пробелы, однако пробелы в конце строки удаляются.	123456789abcde
AH Setup (Установка AH)	Если в качестве **активного протокола** выбран **ESP**, поля **настройки AH** недоступны (**N/A)**.	
SPI (Decimal) (SPI (десятичный))	Введите значение десятичного числа в диапазоне от 1 до 999999 для задания SPI (индекса параметров безопасности).	**N/A**

Табл. 41-5 Меню 27.1.1.2 - Настройка ручного управления ключами

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Authentication Algorithm (Алгоритм аутентификации)	С помощью клавиши [SPACE BAR] выберите **MD5** или **SHA1,** а затем нажмите [ENTER].	**N/A**
Key (Ключ)	Введите ключ аутентификации, который при необходимости будет использовать IPSec. Ключ должен быть уникальным. Введите 16 символов в случае аутентификации по алгоритму **MD5** и 20 - для **SHA-1**. Допускаются любые символы, включая пробелы, однако пробелы в конце строки удаляются.	**N/A**
По завершении работы в Меню при появлении сообщения "Press Enter to Confirm…" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены.		

Chapter 42
Диспетчер соединений SA

В данной главе даются указания по управлению аспектами безопасности с помощью диспетчера соединений SA в меню SMT 27.2.

42.1 Описание диспетчера соединений SA

Security Association (SA - Соглашение по безопасности) - это набор настроек по защите для конкретного туннеля VPN. В этом меню (см. ниже) отображаются активные соединения VPN.

При наличии исходящего трафика и отсутствии входящего соединение SA автоматически прекращается через две минуты. При отсутствии входящего или исходящего трафика туннель находится в состоянии "ожидания" и не отключается до истечения установленного периода существования соединения SA. См. *Руководство пользователя к Web-конфигуратору* в части функции поддержания соединения активным для выполнения обновления согласования безопасного соединения OMNI ADSL по истечении времени жизни соединения, даже при отсутствии трафика.

42.2 Работа с диспетчером соединений SA

1. Вывод на экран списка активных соединений VPN осуществляется с помощью функции **Refresh**.
2. Отключение активных соединений осуществляется с помощью функции **Disconnect**.

В **Меню 27 - Настройка VPN/IPSec** наберите "2" и нажмите клавишу [ENTER] для перехода в **Меню 27.2 - Диспетчер соединений SA**.

```
                              Menu 27.2 - SA Monitor

 #                      Name                        Encap.      IPSec ALgorithm
---    --------------------------------        ---------     ----------------
001        Taiwan : 3.3.3.1 - 3.3.3.3.100          Tunnel      ESP DES MD5
002
003
004
005
006
007
008
009
010

                      Select Command= Refresh
                      Select Connection= N/A

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

Рис. 42-1 Меню 27.2 - Диспетчер соединений SA

Следующая таблица описывает поля данного меню.

Табл. 42-1 Меню 27.2 - Диспетчер соединений SA

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
# (Индекс)	Индекс соединения "соглашение по безопасности".	
Name (Имя)	В этом поле указывается уникальное идентификационное имя данной стратегии VPN. Это имя является уникальным для каждого соединения, в котором IP адресом безопасного шлюза является открытый статический IP-адрес. Если IP-адрес безопасного шлюза равен 0.0.0.0 (см. предыдущую главу), в различных соединениях может применяться одно правило VPN. В этом случае за именем следует удаленный IP-адрес, указанный в **Меню 27.1.1. – Настройка IPSec**. Отдельные соединения, использующие одно и то же правило VPN, могут быть прерваны, при этом другие соединения по данному правилу остаются активными.	**Taiwan**
Encap.	В этом поле указывается **Tunnel (Туннельный)** или **Transport (Транспортный)** режим. Описание режимов см. выше.	**Tunnel**
IPSec ALgorithm (Алгоритм шифрования)	В этом поле отображаются протоколы защиты данных, использующиеся для соединения SA. Протокол **ESP** обеспечивает конфиденциальность и целостность данных шифрованием и инкапсуляцией в пакеты IP. В состав методов защиты входят: 56-битовый алгоритм **DES** и 168-битовый алгоритм **3DES**. Признак **NULL** указывает на туннель без шифрования.	**ESP DES MD5**

Табл. 42-1 Меню 27.2 - Диспетчер соединений SA

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
	Входящие данные SA могут содержать **AH** в дополнение к **ESP**. Аутентифицирующий заголовок обеспечивают высокую целостность данных и аутентификацию путем включения аутентифицирующей информации в пакеты IP. Эта информация определяется в зависимости от содержания заголовка и полей данных в IP-пакете. Это позволяет получить дополнительный уровень защиты. Для протокола **AH** можно выбрать алгоритм **MD5** (по умолчанию - 128 бит) и **SHA -1**(160 бит). Как **AH**, так и **ESP** выдвигают возрастающие требования к обработке данных в OMNI ADSL и времени ожидания связи (задержки).	
Select Command (Выбор команд)	С помощью клавиши [SPACE BAR] выберите одну из команд **Refresh**, **Disconnect**, **None**, **Next Page** или **Previous Page**, а затем нажмите [ENTER]. При выборе команды **Disconnect** необходимо в следующем поле указать соединение. **Refresh** выводит на экран список текущих активных соединений VPN. Команда **None** перемещает к подсказке “Press ENTER to Confirm…”. Для просмотра следующей или предыдущей страницы выберите **Next Page** или **Previous Page,** соответственно.	**Refresh**
Select Connection (Выбор соединения)	Введите индекс соединения VPN, которое хотите разъединить, а затем нажмите [ENTER].	**1**
По завершении работы в Меню при появлении сообщения "Press Enter to Confirm…" нажмите клавишу [ENTER] для сохранения конфигурации, или в любой момент нажмите клавишу [ESC] для отмены.		

42.3 Просмотр журнала регистрации событий IPSec

Для просмотра журнала регистрации событий IPSec и IKE наберите "3" в меню 27 и нажмите [ENTER], при этом на экран выводится журнал регистраций IPSec, показанный ниже. На следующем рисунке показан типичный журнал регистрации событий инициатора VPN-соединения.

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:02:22    Send Main Mode request to <192.168.100.101>
 002    01 Jan 08:02:22    Send:<SA>
 003    01 Jan 08:02:22    Recv:<SA>
 004    01 Jan 08:02:24    Send:<KE><NONCE>
 005    01 Jan 08:02:24    Recv:<KE><NONCE>
 006    01 Jan 08:02:26    Send:<ID><HASH>
 007    01 Jan 08:02:26    Recv:<ID><HASH>
 008    01 Jan 08:02:26    Phase 1 IKE SA process done
 009    01 Jan 08:02:26    Start Phase 2: Quick Mode
 010    01 Jan 08:02:26    Send:<HASH><SA><NONCE><ID><ID>
 011    01 Jan 08:02:26    Recv:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:02:26    Send:<HASH>
 Clear IPSec Log (y/n):
```

Рис. 42-2 Примерный журнал регистрации IPSec инициатора VPN-соединения

42.3.1 Журнал регистраций IPSec отвечающей стороны VPN-соединения

На следующем рисунке показан типичный журнал регистрации событий отвечающей стороны VPN-соединения.

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:08:07    Recv Main Mode request from <192.168.100.100>
 002    01 Jan 08:08:07    Recv:<SA>
 003    01 Jan 08:08:08    Send:<SA>
 004    01 Jan 08:08:08    Recv:<KE><NONCE>
 005    01 Jan 08:08:10    Send:<KE><NONCE>
 006    01 Jan 08:08:10    Recv:<ID><HASH>
 007    01 Jan 08:08:10    Send:<ID><HASH>
 008    01 Jan 08:08:10    Phase 1 IKE SA process done
 009    01 Jan 08:08:10    Recv:<HASH><SA><NONCE><ID><ID>
 010    01 Jan 08:08:10    Start Phase 2: Quick Mode
 011    01 Jan 08:08:10    Send:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:08:10    Recv:<HASH>
 Clear IPSec Log (y/n):
```

Схема 42-1 Образец журнала регистраций IPSec отвечающей стороны VPN-соединения

Эти журналы могут быть полезны при поиске и устранении неисправностей; так как в них выводятся порядковые номер журнальных записей, время и дата создания их создания и содержание записей.

Два восклицательных знака (!!) означают сообщение об ошибке или предупреждение.

Chapter 43
Внутренний генератор таблицы системных параметров (Internal SPTGEN)

43.1 Описание внутреннего генератора таблицы системных параметров

Внутренний SPTGEN (System Parameter Table Generator - генератор таблицы системных параметров) представляет собой текстовый файл конфигурации, полезный и эффективный для одновременного конфигурирования нескольких устройств OMNI ADSL. Внутренний SPTGEN позволяет одновременно сконфигурировать, сохранить и загрузить несколько меню с использованием одного текстового файла конфигурации, в котором предъявляются требования к работе и конфигурированию отдельных меню системной консоли для каждого маршрутизатора OMNI ADSL.

43.2 Формат текстового файла конфигурации

Все текстовые файлы внутреннего SPTGEN преобразуются в следующий формат:

<field identification number (номер поля идентификации) = field name (имя поля) = parameter values allowed (допустимые значения входных параметров)= input>,

где <input> подтверждает соответствие <parameter values allowed (допустимым значениям параметра)>.

На приведенном ниже рисунке демонстрируется образец текстового файла внутреннего SPTGEN.

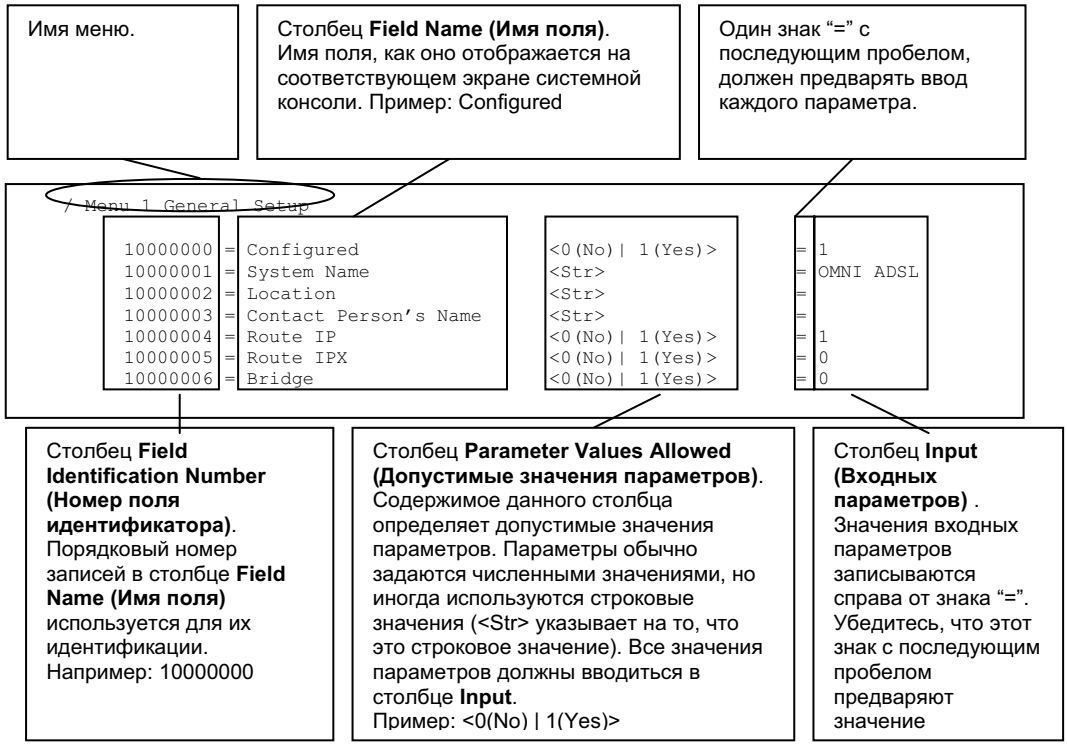


Рис. 43-1 Формат текстового файла конфигурации: Описание столбцов

НЕ изменяйте и не удаляйте содержимое полей, за исключением значений параметров в столбце Input**.**

Другие образцы текстовых файлов см. в *Приложении: Образцы экранов внутреннего SPTGEN*.

43.2.1 Внутренний SPTGEN - Модификация файлов - Основные положения

- Каждый параметр предваряется знаком “=” и следующим за ним пробелом.
- Некоторые параметры зависят от других. Например, при отключении поля **Configured** в меню 1 (см. *Рис. 43-1*) происходит отключение всех полей данного меню.
- Если ввести недопустимое значение параметра в столбце **Input**, OMNI ADSL не сохранит конфигурацию, а в командной строке будет отображаться **Field Identification Number (Номер поля идентификации)**. *Рис. 43-2*, приведенный ниже, является примером того, что отображается

на экране OMNI ADSL, если ввести значение, отличное от “0” или “1”, в столбце **Input** в поле записи с **Field Identification Number (Номером поля идентификации)** 1000000 (см. *Рис. 43-1*).

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Рис. 43-2 Ввод недопустимых значений параметров: пример записи в командной строке

На экране OMNI ADSL при вводе *допустимых* значений параметров отобразится следующее.

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Рис. 43-3 Ввод допустимых значений параметров: Пример записи в командной строке

43.3 Пример загрузки внутреннего SPTGEN через FTP

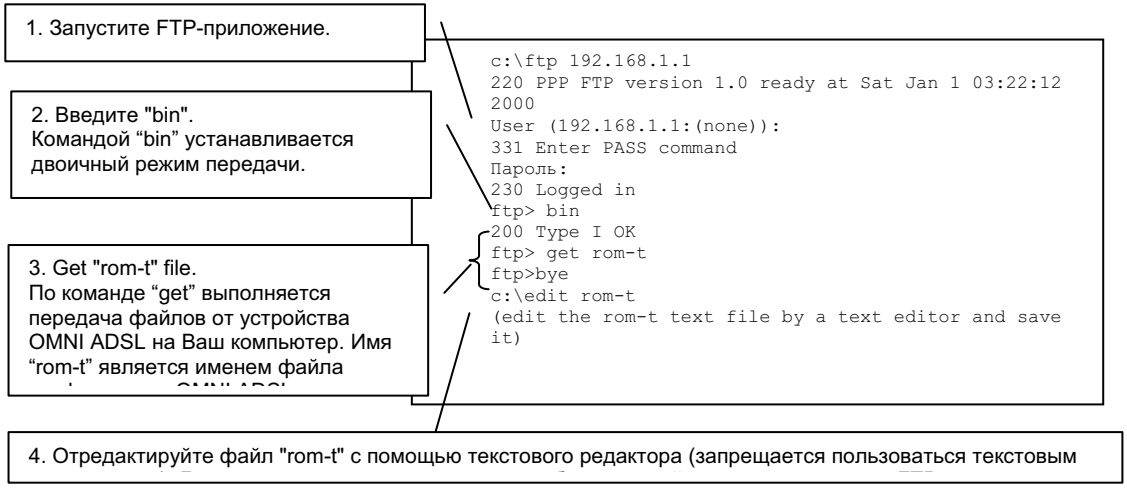


Рис. 43-4 Пример выгрузки внутреннего SPTGEN через FTP

Файл “rom-t” при сохранении его на Вашем компьютере необходимо переименовать, но он должен именоваться “rom-t” во время его загрузки в OMNI ADSL.

43.4 Пример выгрузки внутреннего SPTGEN через FTP

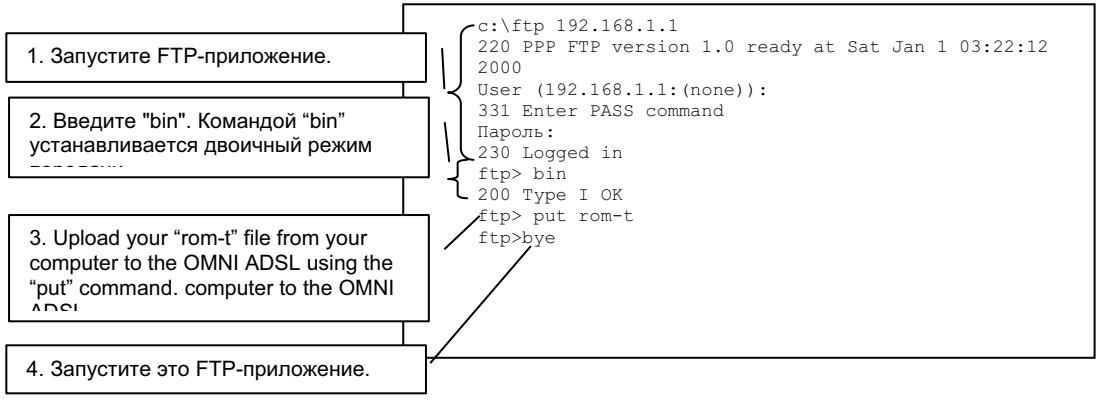


Рис. 43-5 Пример загрузки внутреннего SPTGEN через FTP

Part XII:

Приложения и алфавитный указатель

В этой части освещаются вопросы поиска и устранения неисправностей, приводится дополнительная информация и алфавитный указатель основных терминов.

Appendix A
Устранение неисправностей

В данной главе рассматриваются потенциальные проблемы и способы их устранения.

A.1 Использование светодиодов для диагностики неисправностей

Светодиоды являются полезным инструментом поиска возможных причин неисправностей.

A.1.1 Светодиод питания

Не загорается светодиод **PWR (Питание)** на передней панели.

Схема A-1 Поиск и устранение неисправностей с помощью светодиода питания

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Убедитесь, что адаптер питания OMNI ADSL подсоединен к OMNI ADSL и к соответствующему источнику питания. Обязательно пользуйтесь адаптером питания.
2	Проверьте включение OMNI ADSL и источника питания, убедитесь в том, что напряжение OMNI ADSL соответствует необходимому.
3	Выключите и снова включите OMNI ADSL.
4	Если проблема не исчезла, возможно, имеет место аппаратная неисправность. В этом случае следует связаться с продавцом.

A.1.2 Светодиод LAN

Не загорается светодиод LAN **(ЛВС)** на передней панели.

Схема A-2 Поиск и устранение неисправностей с помощью светодиода LAN

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Проверьте разъемы кабельного соединения Ethernet в устройстве OMNI ADSL, и в компьютере или концентраторе.
2	Проверьте кабель Ethernet на отсутствие дефектов.

Схема A-2 Поиск и устранение неисправностей с помощью светодиода LAN

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
3	Убедитесь в том, что компьютерная карта Ethernet работает надлежащим образом.
4	Если эти действия не помогут в устранении неисправности, обратитесь за помощью к региональному дистрибьютору.

A.1.3 Светодиод DSL

Не загорается светодиод DSL **(Цифровой абонентской линии)** на передней панели.

Схема A-3 Поиск и устранение неисправностей DSL с помощью светодиода

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Проверьте состояние телефонных проводов и разъемов порта DSL устройства OMNI ADSL и телефонной розетки.
2	Убедитесь в том, что телефонная компания проверила телефонную линию и выполнила ее настройку для сервиса DSL.
3	Сбросьте линию ADSL для повторной инициализации канала связи с концентратором DSLAM. Для получения дополнительной информации см. раздел *Сопровождение* (Web-конфигуратор) или главу "Информация о системе и диагностика (SMT)".
4	Если эти действия не помогут в устранении неисправности, обратитесь за помощью к региональному дистрибьютору.

A.2 Консольный порт

Отсутствует доступ к OMNI ADSL через консольный порт.

Схема A-4 Поиск и устранение неисправностей консольного порта

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Убедитесь в том, что OMNI ADSL подключен к последовательному порту компьютера.

Схема A-4 Поиск и устранение неисправностей консольного порта

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ	
2	Убедитесь в том, что коммуникационная программа правильно сконфигурирована. Программное обеспечение для работы в режиме терминала должно быть сконфигурировано следующим образом:	Эмуляция терминала VT100. Скорость по умолчанию, установленная изготовителем - 9600 бит/с. В случае, если скорость изменилась, попробуйте установить другие значения скорости. Без четности, 8 бит данных, 1 стоп-бит, поток данных установлен на None.
3	Убедитесь в том, что Вы ввели правильный пароль. По умолчанию установлен пароль 1234. Если Вы забыли имя пользователя или пароль, см. *раздел A.5*.	

A.3 Telnet

Отсутствует подключение к OMNI ADSL через Telnet.

Схема A-5 Поиск и устранение неисправностей при подключении через Telnet

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Проверьте порт LAN и другие соединения с Ethernet.
2	Убедитесь в том, что Вы пользуетесь правильным IP-адресом устройства OMNI ADSL. Проверьте IP-адрес OMNI ADSL.
3	Проверьте связь компьютера с OMNI ADSL эхо-тестированием. Если связь с OMNI ADSL не устанавливается, следует проверить IP-адреса, настроенные в устройстве OMNI ADSL и компьютере. Убедитесь, что компьютер настроен на получение динамического IP-адреса. Если же Вы хотите, чтобы компьютер использовал статический IP-адрес, он должен находиться в той же подсети, что и OMNI ADSL.
4	Убедитесь в том, что Вы ввели правильный пароль. По умолчанию установлен пароль 1234. Если Вы забыли имя пользователя или пароль, см. *раздел A.5*.
5	Если эти действия не решают проблему, обратитесь к поставщику.

A.4 Web-конфигуратор

Отсутствует доступ к Web-конфигуратору.

Схема A-6 Поиск и устранение неисправностей Web-конфигуратора

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Убедитесь в том, что Вы пользуетесь правильным IP-адресом устройства OMNI ADSL. Проверьте IP-адрес OMNI ADSL.
2	Убедитесь, что в этот момент не идет сеанс связи через системную консоль.
3	Убедитесь в том, что включена функция доступа к услугам Web. Если Вы пользуетесь защищенным клиентским IP-адресом, то он должен совпадать с IP-адресом Вашего компьютера. См. главу о дистанционном управлении для получения подробной информации.
4	Для доступа к WAN необходимо сконфигурировать функцию дистанционного управления, что разрешает доступ к серверу из WAN (или всем пользователям).
5	Для доступа к LAN IP-адреса Вашего компьютера и устройства OMNI ADSL должны принадлежать одной подсети.
6	В случае изменения IP-адреса OMNI ADSL в LAN, следует ввести новый адрес как URL.
7	Удалите все фильтры в меню SMT 3.1 (LAN) или в меню 11.5 (WAN), блокирующие доступ к услугам Web.
8	См. также *раздел A.9*.

Неправильное отображение Web-конфигуратора.

Схема A-7 Поиск и устранение неисправностей отображения интернет-браузера

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Убедитесь в том, что Вы пользуетесь браузером Internet Explorer 5.0 или его более поздними версиями.
2	Удалите временные web-файлы и загрузитесь повторно. В Internet Explorer щелкните по **Tools (Инструменты)**, **Internet Options (Опции Интернет)**, а затем щелкните по кнопке **Delete Files ... (Удалить файлы)**. После появления окна **Delete Files (Удалить файлы)** выберите **Delete all offline content (Удалить все содержание offline)** и щелкните по **OK**. (Действия могут отличаться в зависимости от версий использующегося интернет-браузера.)

A.5 Регистрация имени пользователя и пароля

Я забыл мое зарегистрированное имя пользователя и/или пароль.

Схема A-8 Поиск и устранение неисправностей при регистрации имени пользователя и пароля

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Если Вы изменили пароль и забыли его, следует загрузить файл конфигурации, заданный по умолчанию. При этом будут уничтожены настройки пользователя и восстановлены заводские настройки по умолчанию, включая пароль.
2	Нажмите кнопку перезапуска **RESET** и держите ее в течение пяти секунд, а затем отпустите. Если светодиод **SYS** начинает мигать, это означает, что настройки восстановлены, и происходит перезапуск OMNI ADSL. *Или* см. раздел *Resetting the OMNI ADSL (Сброс настроек OMNI ADSL)* для загрузки файла конфигурации через консольный порт.
3	Имя пользователя, заданное по умолчанию, - “admin”. По умолчанию установлен пароль 1234. Поля **Password** и **Username** чувствительны к выбору регистра. Убедитесь, что Вы ввели правильный пароль и имя пользователя в нужном регистре.
4	Настоятельно рекомендуется изменить имя пользователя и пароль, заданные по умолчанию. Убедитесь в том, что имя пользователя и пароль хранятся в безопасном месте.

A.6 Интерфейс локальной сети

Отсутствует доступ к устройству OMNI ADSL из LAN или не выполняется эхо-тестирование компьютеров LAN.

Схема A-9 Поиск и устранение неисправностей интерфейса LAN

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Проверьте светодиоды Ethernet на передней панели. Если порт подключен к компьютеру или концентратору, светодиод LAN должен гореть. Если не горят оба светодиода 10M/100M на передней панели, см. *раздел A.1.2*.
2	Убедитесь, что IP-адрес и маска подсети OMNI ADSL находятся в одной подсети с компьютерами локальной сети.

A.7 Интерфейс глобальной сети

Не удается произвести инициализацию соединения ADSL.

Схема A-10 Поиск и устранение неисправностей соединения ADSL

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Проверьте кабельные соединения между портом ADSL и стенной розеткой. Светодиод DSL на передней панели OMNI ADSL должен гореть.
2	Проверьте, чтобы VPI, VCI, тип инкапсуляции и тип мультиплексирования были идентичны предоставленным телефонной компанией и Интернет-провайдером.
3	Перезапустите OMNI ADSL. Если проблемы сохраняются, следует проверить настройки VPI, VCI, типа инкапсуляции и типа мультиплексирования в телефонной компании и у Интернет-провайдера.

Не удается получить от Интернет-провайдера IP-адрес в глобальной сети.

Схема A-11 Поиск и устранение неисправностей интерфейса WAN

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Интернет-провайдер присваивает IP-адрес в глобальной сети после Вашей аутентификации. Аутентификация может выполняться с использованием имени пользователя и пароля, MAC-адреса или имени хоста.
2	Имя пользователя и пароль используются только при инкапсуляции PPPoE и PPoA . Убедитесь в том, что правильно установлены **Service Type (Тип сервиса)**, **User Name (Имя пользователя)** и **Password (Пароль)** (убедитесь в правильности их назначения). См. главу *"Настройка WAN",* раздел "Web-конфигуратор", или главу *"Подключение к сети Интернет"*(SMT).

A.8 Доступ в Интернет

Нет доступа в Интернет.

Схема A-12 Поиск и устранение неисправностей доступа в сеть Internet

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Убедитесь, что OMNI ADSL включен и подсоединен к сети.
2	Если не горит светодиод DSL, см. *раздел A.1.3*.
3	Проверьте правильность настроек WAN. См. главу *"Настройка WAN",* раздел "Web-конфигуратор", или главу *"Подключение к сети Интернет",* раздел "Главная системная консоль".
4	Убедитесь в том, что Вы правильно ввели имя пользователя и пароль.

Схема A-12 Поиск и устранение неисправностей доступа в сеть Internet

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
5	Для беспроводных станций: убедитесь в том, что и OMNI ADSL и беспроводная станция (и) пользуются одинаковыми идентификаторами ESSID, каналами и ключами WEP (если функция шифрования WEP является активной).

Пропадает подключение к сети Интернет.

Схема A-13 Поиск и устранение неисправностей подключения к сети Интернет

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Проверьте правила плана. См. главу *Составление плана вызовов* (SMT).
2	При использовании инкапсуляции PPPoA или PPPoE, проверьте настройки времени ожидания. См. главу *WAN* (Web-конфигуратор) или главу *Конфигурирование удаленного узла* (SMT).
3	Обратитесь за помощью к Вашему Интернет-провайдеру.

A.9 Дистанционное управление

Отсутствует дистанционное управление OMNI ADSL из LAN или WAN.

Схема A-14 Поиск и устранение неисправностей дистанционного управления

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	См. раздел *Ограничения дистанционного управления* в главе *Микропрограммное обеспечение и управление файлом конфигурации* (SMT) для ознакомления со сценариями, при которых дистанционное управление невозможно.
2	При конфигурировании из глобальной сети следует использовать IP-адрес устройства OMNI ADSL в глобальной сети. При конфигурировании из локальной сети следует использовать IP-адрес OMNI ADSL в локальной сети.
3	См. *раздел A.6* для ознакомления с инструкциями по проверке подключения к LAN. См. *раздел A.7* для ознакомления с инструкциями по проверке подключения к WAN.
4	См. также *раздел A.4*.

A.10 Подключение к удаленному узлу

Невозможно подключиться к удаленному узлу или Интернет-провайдеру.

Схема A-15 Поиск и устранение неисправностей подключения к удаленному узлу или Интернет-провайдеру

ДЕЙСТВИЯ	СПОСОБЫ УСТРАНЕНИЯ
1	Проверьте меню 4 или экран WAN и убедитесь в том, что имя пользователя и пароль введены правильно.
2	Проверьте в меню 11.1 регистрационное имя и пароль для доступа к удаленному узлу.
3	Если эти действия окажутся безрезультатными, проверьте регистрационное имя и пароль у Интернет-провайдера.

Appendix B
Организация подсетей IP

Организация адресов IP

Определение маршрута маршрутизатором основывается на сетевом номере. Маршрутизатор, отвечающий за доставку пакета данных нужному хосту назначения, пользуется идентификатором хоста.

Классы IP

IP-адрес состоит из четырех октетов (восьми битов), записанных в десятичном виде с разделительными точками, например, 192.168.1.1. IP-адреса подразделяются на различные классы. Класс адреса определяется значением его первого октета.

- Адреса класса “A” имеют 0 в крайнем левом бите. В адресе класса “A” первый октет является сетевым номером, а остальные три октета образуют идентификатор хоста.
- Адреса класса “B” имеют 1 в крайнем левом бите и 0 в следующем. Два первых октета адреса класса “B” образуют сетевой номер, а два оставшихся октета - идентификатор хоста.
- Адреса класса “C” начинаются (при отсчете слева) с 1 1 0. Первые три октета адреса класса “C” образуют сетевой номер, а последний октет является идентификатором хоста.
- Адреса класса “D” начинаются с 1 1 1 0. Адреса класса “D” используются при многоадресной рассылке. (Существуют также адреса класса “E”, зарезервированные на будущее).

Схема B-1 Классы IP-адресов

IP-АДРЕС:		ОКТЕТ 1	ОКТЕТ 2	ОКТЕТ 3	ОКТЕТ 4
Класс A	0	Сетевой номер	Идентификатор хоста	Идентификатор хоста	Идентификатор хоста
Класс B	10	Сетевой номер	Сетевой номер	Идентификатор хоста	Идентификатор хоста
Класс C	110	Сетевой номер	Сетевой номер	Сетевой номер	Идентификатор хоста

Идентификаторы хостов из одних нулей или единиц не разрешены.

Таким образом:

- Сеть класса “C” (8 хост-битов) может иметь 2^8 –2 или 254 хоста.
- Адрес класса “B” (16 хост-битов) может иметь 2^{16} –2 или 65534 хоста.

Адрес класса “A” (24 хост-битов) может иметь 2^{24} –2 хостов (приблизительно 16 млн. хостов).

Поскольку первый октет IP-адреса класса “A” должен иметь “0”, значение первого октета адреса класса “A” находится в диапазоне от 0 до 127.

Аналогично, первый октет класса “B” должен начинаться с “10”, таким образом, значение первого октета адреса класса “B” имеет допустимый диапазон от 128 до 191. Первый октет адреса класса “C” начинается с “110” и, таким образом, находится в диапазоне от 192 до 223.

Схема B-2 Допустимые диапазоны классов IP-адресов

НАБОРА ФИЛЬТРОВ	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО ОКТЕТА (ДВОИЧНЫХ)	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО ОКТЕТА (ДЕСЯТИЧНЫХ)
Класс A	от **0**0000000 до **0**1111111	от 0 до 127
Класс B	от **10**000000 до **10**111111	от 128 до 191
Класс C	от **110**00000 до **110**11111	от 192 до 223
Класс D	от **1110**0000 до **1110**1111	от 224 до 239

Маски подсети

Маски подсети применяются для определения того, какие биты являются частью сетевого номера, а какие - частью идентификатора хоста (с использованием логической операции AND). Размер маски подсети - 32 бита; каждый бит маски соответствует биту IP-адреса. Если бит маски подсети равен “1”, то соответствующий бит IP-адреса является частью сетевого номера. Если бит маски подсети равен “0”, то соответствующий бит IP-адреса является частью идентификатора хоста.

Маска подсети записывается в десятичном виде с разделительными точками, также как и IP-адреса. "Естественными" масками IP-адресов классов A, B и C являются следующие.

Схема B-3 “Естественные” маски

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Организация подсетей

При организации подсетей соглашения относительно классов IP-адреса игнорируются. Например, класс C адресов не должен иметь 24 бита для сетевого номера и 8 битов - для идентификатор хоста. С организацией подсетей некоторые биты идентификатора хоста преобразуются в биты сетевого номера. Условно маска подсети всегда состоит из непрерывной последовательности единиц, начиная с крайнего левого бита маски и последующей непрерывной последовательности нулей, общим размером 32 бита.

Поскольку маска всегда представляет собой постоянное число единиц, начиная слева, и последующей постоянной совокупности нулей в оставшихся разрядах 32-битовой маски, можно просто указать число единиц, вместо того чтобы записывать значение каждого октета. Указателем такой формы является символ “/”, за которым записывается число битов в маске после адреса.

Например, 192.1.1.0 /25 является эквивалентом записи 192.1.1.0 с маской 255.255.255.128.

В следующей таблице показаны все возможные маски подсети для класса “C” адресов с использованием обоих форм записи.

Схема B-4 Альтернативная форма записи маски подсети

МАСКА ПОДСЕТИ ДЛЯ IP-АДРЕСОВ	КОЛИЧЕСТВО ЕДИНИЧНЫХ БИТОВ МАСКИ ПОДСЕТИ	ЗНАЧЕНИЕ В БИТАХ ПОСЛЕДНЕГО ОКТЕТА
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 показанная маска является "естественной" маской класса “C”. Обычно, если маска не указана, то понимается, что будет использоваться "естественная маска".

Пример: Две подсети

Возьмем в качестве примера адрес класса “C” 192.168.1.0 с маской подсети 255.255.255.0.

	СЕТЕВОЙ НОМЕР	ИДЕНТИФИКАТОР ХОСТА
IP-адрес	192.168.1.	0
IP-адрес (двоичный)	11000000.10101000.00000001.	00000000
Маска подсети	255.255.255.	0

Маска подсети (двоичная)	11111111.11111111.11111111.	00000000

Первые три октета адреса образуют сетевой адрес (класс “C”). Вам необходимо иметь две отдельные сети.

Разделим сеть 192.168.1.0 на две подсети преобразованием одного из битов идентификатора хоста IP-адреса в бит сетевого номера. “Заимствованный” бит идентификатора хоста может быть как “0”, так и “1”, указывая, таким образом, наличие двух подсетей; 192.168.1.0 с маской 255.255.255.128 и 192.168.1.128 с маской 255.255.255.128.

На следующих схемах, выделены полужирным шрифтом и цветом (затемнением) битовые значения последнего октета, указывающие "заимствованные" биты идентификатора хоста для формирования битов сетевого идентификатора. Число "заимствованных" битов идентификатора хоста указывает, сколько Вы можете иметь подсетей. Оставшееся число битов идентификатора хоста (после “заимствования”) определяет количество хостов, которые Вы можете иметь в каждой подсети.

Схема B-5 Подсеть 1

	СЕТЕВОЙ НОМЕР	**ЗНАЧЕНИЕ В БИТАХ ПОСЛЕДНЕГО ОКТЕТА**
IP-адрес	192.168.1.	0
IP-адрес (двоичный)	11000000.10101000.00000001.	**0**0000000
Маска подсети	255.255.255.	128
Маска подсети (двоичная)	11111111.11111111.11111111.	**1**0000000
Адрес подсети: 192.168.1.0	Наименьшее значение идентификатора хоста: 192.168.1.1	
Адрес циркулярной рассылки: 192.168.1.127	Наибольшее значение идентификатора хоста: 192.168.1.126	

Схема B-6 Подсеть 2

	СЕТЕВОЙ НОМЕР	**ЗНАЧЕНИЕ В БИТАХ ПОСЛЕДНЕГО ОКТЕТА**
IP-адрес	192.168.1.	128
IP-адрес (двоичный)	11000000.10101000.00000001.	**1**0000000
Маска подсети	255.255.255.	128

Маска подсети (двоичная)	11111111.11111111.11111111.	**1**0000000
Адрес подсети: 192.168.1.128	Наименьшее значение идентификатора хоста: 192.168.1.129	
Адрес циркулярной рассылки: 192.168.1.255	Наибольшее значение идентификатора хоста: 192.168.1.254	

Оставшиеся 7 битов определяют количество хостов, которое можно иметь в каждой подсети. Идентификаторы хостов, состоящие из одних нулей представляют саму подсеть, а все идентификаторы хостов являются для нее адресами циркулярной рассылки, так что фактическое количество доступных хостов в каждой подсети для приведенного выше примера равно $2^7 – 2$ или 126 хостов в каждой подсети.

192.168.1.0 с маской 255.255.255.128 является самой подсетью, а 192.168.1.127 с маской 255.255.255.128 является назначенным адресом циркулярной рассылки в первой подсети. Однако минимальное значение IP-адреса, которое может быть назначено действующему хосту в первой подсети, равно 192.168.1.1, а максимальное - 192.168.1.126. Аналогично диапазон значений для идентификатора хоста второй подсети составляет от 192.168.1.129 до 192.168.1.254.

Пример: Четыре подсети

Приведенный выше пример иллюстрирует применение 25-битовой маски подсети для разделения адресного пространства класса “C” на две подсети. Аналогично, для того чтобы разделить адрес класса “C” на четыре подсети, необходимо “заимствовать” два бита идентификатора хоста для получения четырех возможных комбинаций: 00, 01, 10 и 11. Маска подсети состоит из 26 битов (11111111.11111111.11111111.**11**000000) или 255.255.255.192. Каждая подсеть состоит из 6 битов идентификатора хоста, что позволяет иметь 2^6-2 или 62 хоста в каждой подсети (все "0" указывают на саму подсеть, а все "1" - являются адресом циркулярной рассылки в подсети).

Схема B-7 Подсеть 1

	СЕТЕВОЙ НОМЕР	**ЗНАЧЕНИЕ В БИТАХ ПОСЛЕДНЕГО ОКТЕТА**
IP-адрес	192.168.1.	0
IP-адрес (двоичный)	11000000.10101000.00000001.	**00**000000
Маска подсети (двоичная)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.0	Наименьшее значение идентификатора хоста: 192.168.1.1	
Адрес циркулярной рассылки: 192.168.1.63	Наибольшее значение идентификатора хоста: 192.168.1.62	

Схема B-8 Подсеть 2

	СЕТЕВОЙ НОМЕР	ЗНАЧЕНИЕ В БИТАХ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	64
IP-адрес (двоичный)	11000000.10101000.00000001.	**01**000000
Маска подсети (двоичная)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.64	Наименьшее значение идентификатора хоста: 192.168.1.65	
Адрес циркулярной рассылки: 192.168.1.127	Наибольшее значение идентификатора хоста: 192.168.1.126	

Схема B-9 Подсеть 3

	СЕТЕВОЙ НОМЕР	ЗНАЧЕНИЕ В БИТАХ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	128
IP-адрес (двоичный)	11000000.10101000.00000001.	**10**000000
Маска подсети (двоичная)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.128	Наименьшее значение идентификатора хоста: 192.168.1.129	
Адрес циркулярной рассылки: 192.168.1.191	Наибольшее значение идентификатора хоста: 192.168.1.190	

Схема B-10 Подсеть 4

	СЕТЕВОЙ НОМЕР	ЗНАЧЕНИЕ В БИТАХ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	192
IP-адрес (двоичный)	11000000.10101000.00000001.	**11**000000
Маска подсети (двоичная)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.192	Наименьшее значение идентификатора хоста: 192.168.1.193	
Адрес циркулярной рассылки: 192.168.1.255	Наибольшее значение идентификатора хоста: 192.168.1.254	

Пример восьми подсетей

Аналогично, используйте 27-битовую маску для создания 8 подсетей (001, 010, 011, 100, 101, 110).

В следующей таблице показаны значения последнего октета IP-адреса класса C для каждой подсети.

Схема B-11 Восемь подсетей

SUBNET	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	АДРЕС ЦИРКУЛЯРНОЙ РАССЫЛКИ
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 планированию создания подсети класса “C”.

Схема B-12 Планирование создания подсети класса C

ЧИСЛО "ЗАИМСТВОВАННЫХ" БИТОВ ХОСТА	МАСКА ПОДСЕТИ	ЧИСЛО ПОДСЕТЕЙ	ЧИСЛО ХОСТОВ НА ПОДСЕТЬ
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

Создание подсетей из сетей классов A и B.

Маска подсетей для адресов классов “A” и “B” также определяет, какие биты являются частью сетевого номера, а какие - частью идентификатора хоста.

Адрес класса “B” имеет в идентификаторе хоста два октета, которые могут использоваться для создания подсетей, а в идентификаторе хоста адреса класса “A” - три октета (см. *Схема B-1*).

В следующей таблице приведены сводные сведения по планированию создания подсети класса “B”.

Схема B-13 Планирование создания подсети класса B

ЧИСЛО "ЗАИМСТВОВАННЫХ" БИТОВ ХОСТА	МАСКА ПОДСЕТИ	ЧИСЛО ПОДСЕТЕЙ	ЧИСЛО ХОСТОВ НА ПОДСЕТЬ
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

Appendix C
Беспроводная локальная сеть и протокол IEEE 802.11

Беспроводная локальная сеть (WLAN) обеспечивает создание гибкой коммуникационной системы передачи данных, открывающей доступ к различным видам сервиса (работа в сети Интернет, электронная почта, сетевые принтеры и т.п.) без необходимости создания дорогой инфраструктуры кабельной сети. В результате среда беспроводной LAN предоставляет возможность свободного подключения к сети в пределах зоны охвата.

Преимущества беспроводной локальной сети

1. Доступ к сетевому сервису в местах, где прокладка проводов является дорогостоящей или сложной работой, например, в зданиях, имеющих историческое значение, в зданиях, построенных с использованием асбестовых материалов, или в учебных классах.
2. Врачи и медицинские сестры могут в полном объеме получить доступ, включая доступ из комнаты больного, к сведениям о пациенте, хранящимся в КПК или в ноутбуке.
3. Обеспечивает организацию гибких рабочих групп с минимальными издержками на создание сетей переменной конфигурации.
4. Участники конференций могут получить доступ к сети в процессе передвижения с одного собрания на другое - получая доступ к последней оперативной информации, что позволяет вести обсуждение решений "на лету".
5. Обеспечивает сетевой охват в пределах студенческого городка, позволяя использовать возможности роуминга для создания простых в эксплуатации беспроводных сетей, прозрачных на всем протяжении его территории.

Протокол IEEE 802.11

Завершение в 1997 разработки стандарта протокола IEEE 802.11 для беспроводных сетей (WLANs) стало первым существенным шагом в эволюции развития технологии беспроводных сетей. Целью создания стандарта является достижение максимальной эффективности взаимодействия различных видов беспроводных сетей и представление новых возможностей и преимуществ новой технологии.

Стандарт IEEE 802.11 определяет три различных метода передачи данных для физического уровня, отвечающего за передачу данных между узлами. В двух методах используется широкий спектр сигналов высоких частот - Расширенный по принципу прямой последовательности спектр - Direct Sequence Spread Spectrum (DSSS)) и Расширенный путем скачкообразной перестройки частоты

спектр - Frequency-Hopping Spread Spectrum (FHSS) в диапазоне от 2,4 до 2,4825 ГГц - нелицензируемый частотный диапазон ISM (Industrial, Scientific and Medical - для производственных, научных и медицинских целей). В третьем методе для передачи данных используется технология инфракрасной части диапазона видимого спектра электромагнитных волн.

Специальная конфигурация беспроводной LAN

Простейшей конфигурацией беспроводных LAN является независимая беспроводная LAN, соединяющая ряд компьютеров с беспроводными узлами или беспроводными станциями (STA), совокупность которых обеспечивает базовый набор услуг и именуются Basic Service Set (BSS). В большинстве случаев основной формой беспроводной LAN является соединение ряда компьютеров с помощью адаптеров беспроводной связи. Всякий раз, когда два и более адаптера беспроводной связи находятся в одной зоне, они могут образовывать независимую сеть, которая обычно именуется специальной сетью или независимым базовым набором услуг (Independent Basic Service Set - IBSS). См. следующую схему, где приводится пример специальной беспроводной LAN.

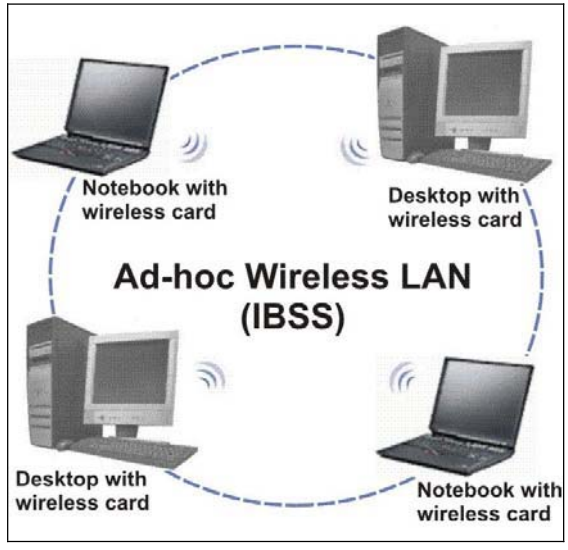


Схема C-1 Одноранговая связь в специальной сети

Инфраструктура конфигурации беспроводной LAN

В инфраструктуре беспроводных LAN несколько точек доступа (AP) связывают ее с проводной сетью, что обеспечивает эффективное использование общих сетевых ресурсов. Точки доступа не только обеспечивают связь с проводной сетью, но также служат связующим звеном для передачи

трафика беспроводной сети ближайшему окружению. Несколько точек доступа могут обеспечить охват радиосвязью в пределах всего здания или студенческого городка. Вся связь между станциями или между станцией и клиентом беспроводной сети осуществляется через точку доступа.

Расширенный набор услуг (Extended Service Set - (ESS), показанный на следующем рис., состоит из серии BSS (каждая из которых имеет в своем составе точку доступа), с перекрывающимися зонами действия, связанных друг с другом через коммутационную систему (Distribution System - DS). Хотя DS может быть создана на основе сетей различного типа, почти наверняка она относится к Ethernet LAN. Мобильные узлы могут перемещаться между точками доступа, что делает возможным полный охват территории студенческого городка.

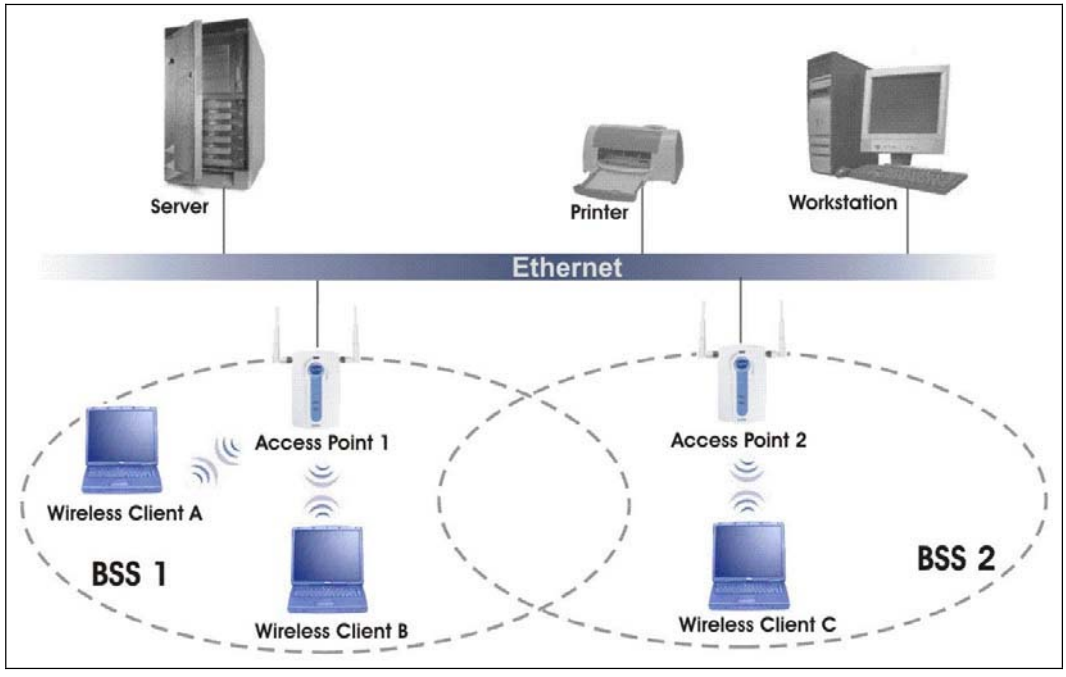


Схема C-2 ESS обеспечивает охват территории студенческого городка

Appendix D
PPPoE

Протокол PPPoE в действии

Модем ADSL передает сеанс связи PPP через Ethernet (PPP через Ethernet, RFC 2516) с Вашего ПК на постоянный виртуальный канал ATM (Permanent Virtual Circuit (PVC)), соединенный с концентратором доступа xDSL, в котором сеанс связи PPP завершается (см. следующий рисунок). Один PVC может поддерживать любое количество сеансов PPP из LAN. Протокол PPPoE обеспечивает управление и функции составления счетов, аналогично сервису с использованием протокола PPP.

Преимущества PPPoE

PPPoE дает следующие преимущества:

1. Предоставляет хорошо знакомый пользовательский интерфейс для доступа в сеть по коммутируемой линии (DUN).
2. Уменьшает нагрузку на линии связи, предоставляя виртуальные схемы на всем пути к Интернет-провайдеру для тысяч пользователей. Для GSTN (PTSN и ISDN) структура коммутации уже введена в эксплуатацию.
3. Позволяет Интернет-провайдеру использовать существующую модель соединения по коммутируемой линии для аутентификации и (по желанию) предоставления дифференцированных услуг.

Традиционная схема соединения по коммутируемой линии

На следующей схеме представлена типичная конфигурация аппаратного обеспечения, по которой ПК используют традиционный доступ в сеть по коммутируемой линии.

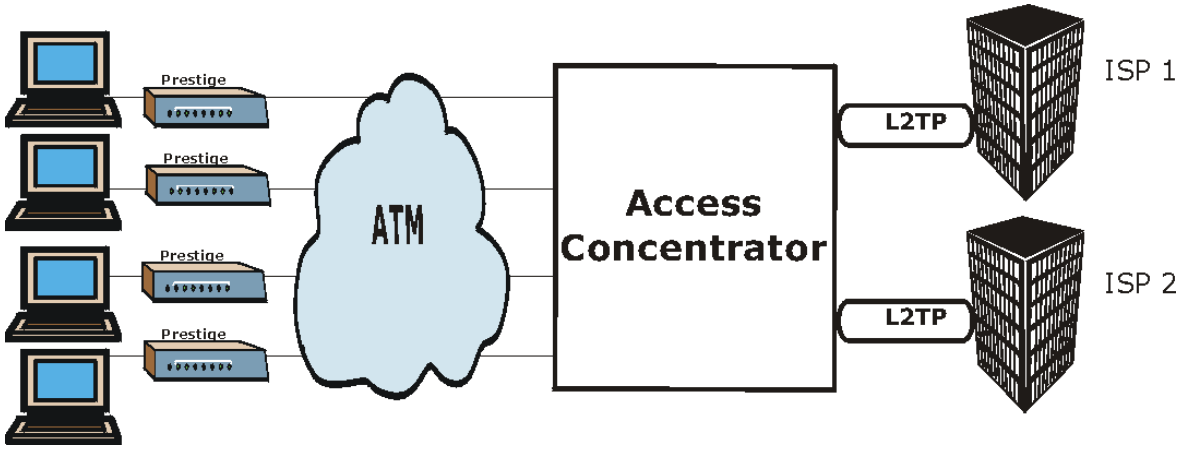


Схема D-1 Конфигурация аппаратного обеспечения для подключения одиночного ПК через маршрутизатор

Как функционирует PPPoE

Драйвер PPPoE представляет Ethernet как последовательный канал связи с ПК; через нее ПК запускает PPP, в то время как модем передает кадры Ethernet в концентратор доступа (Access Concentrator (AC)). При этом в качестве концентратора доступа, туннелирующего кадры PPP Интернет-провайдеру, выступает концентратор доступа (LAC) туннельного уровня протокола уровня 2 (L2TP). Туннель L2TP обеспечивает одновременное проведение нескольких сеансов PPP.

При наличии PPPoE виртуальный канал является эквивалентом коммутируемого соединения, и находится между модемом и концентратором доступа, находящимся на противоположном конце у Интернет-провайдера. При этом сессия PPP проводится между PC и Интернет-провайдером.

OMNI ADSL в качестве клиента PPPoE

При использовании маршрутизатора OMNI ADSL в качестве клиента PPPoE, компьютеры в LAN "видят" только Ethernet и не распознают PPPoE. Это освобождает администратора от необходимости управлять клиентами PPPoE на отдельных ПК.

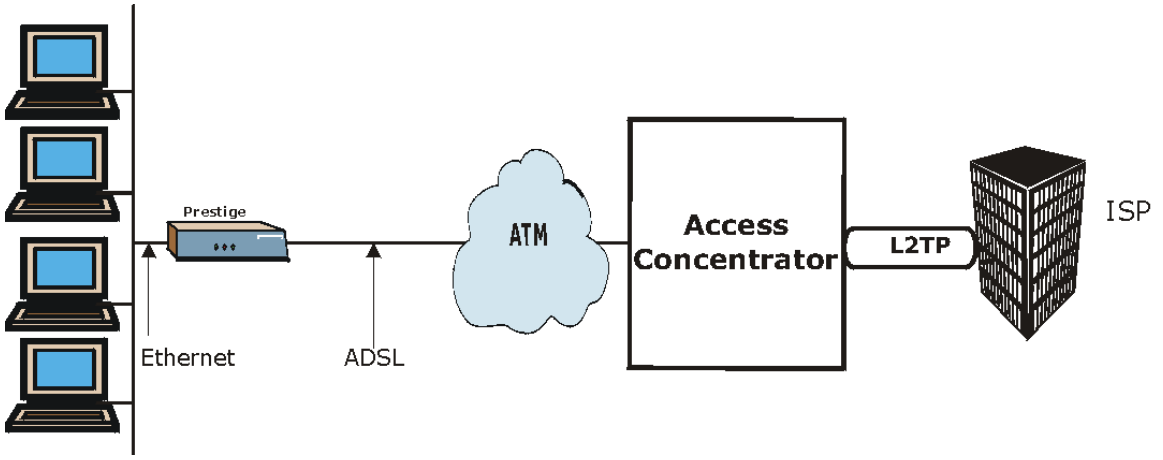


Схема D-2 OMNI ADSL в качестве клиента PPPoE

Appendix E
Топология виртуальной цепи

ATM представляет собой технологию, ориентированную на соединение, что означает создание виртуальных цепей, по которым осуществляется связь между оконечными системами. Для обозначения виртуальных цепей используются следующие термины:

- Виртуальный канал Логические соединения между коммутаторами ATM
- Виртуальный путь Набор виртуальных каналов
- Виртуальная цепь Ряд виртуальных путей между конечными точками в сети

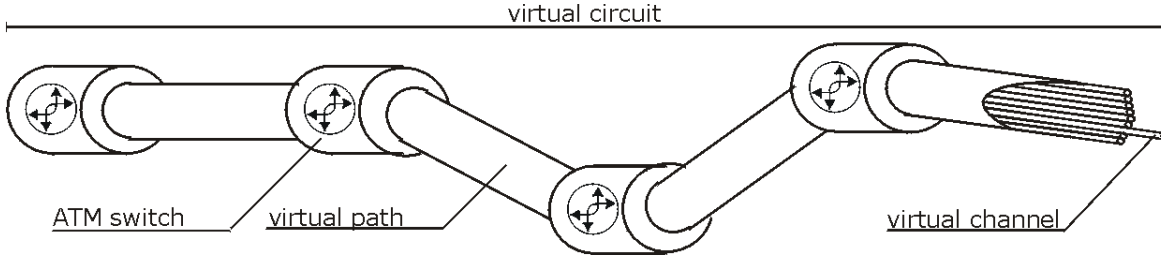


Схема E-1 Топология виртуальной цепи

Представьте, что виртуальный путь - это кабель, состоящий из нескольких проводов. Кабель соединяет две точки, при этом провода внутри кабеля создают отдельные схемы между этими двумя точками. В заголовке ячейки ATM 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 ATM. Ряд виртуальных путей образует виртуальную цепь.

Номера VPI/VCI предоставляются провайдером сетевых услуг.

Appendix F
Настройка IP-адреса компьютера

На всех компьютерах должна быть установлена адаптерная плата Ethernet 10M или 100M и TCP/IP.

Windows 95/98/Me/NT/2000, Macintosh OS 7 и более поздние операционные системы, а также все версии UNIX и LINUX содержат все программные компоненты, необходимые для инсталляции и использования TCP/IP на компьютере. Для Windows 3.1 может потребоваться дополнительный пакет прикладных программ TCP/IP другого производителя.

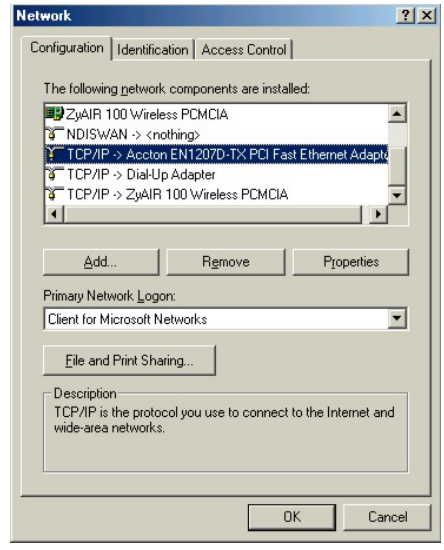
TCP/IP уже должен быть инсталлирован на компьютерах с системами Windows NT/2000/XP, Macintosh OS 7 или более поздними операционными системами.

После установки соответствующих компонентов TCP/IP осуществляется конфигурирование настроек TCP/IP для того чтобы "связаться" с сетью.

Если ввод информации об IP-адресе осуществляется вручную, вместо использования процедуры динамического назначения, убедитесь в том, что Ваш компьютер имеет IP-адреса, относящиеся к той же подсети, что и порт LAN маршрутизатора OMNI ADSL.

Windows 95/98/Me

Щелкните по **Start (Пуск)**, **Settings (Настройки)**, **Control Panel (Панель управления)** и дважды щелкните по иконке **Network (Сеть)** для вызова окна **Network (Сеть)**.



Установка компонентов

Щелкните на закладке **Configuration** в окне **Network** для вывода списка инсталлированных компонентов. Следует выбрать сетевой адаптер, протокол TCP/IP и клиента для сетей Microsoft.

Для выбора сетевого адаптера:

a. Щелкните по **Add** в окне **Network**.

b. Выберите **Adapter** и щелкните по **Add**.

c. Выберите производителя и модель сетевого адаптера и щелкните по **OK**

Для выбора TCP/IP:

a. Щелкните по **Add** в окне **Network**.

b. Выберите **Protocol** и щелкните по **Add**.

c. Выберите **Microsoft** из списка **manufactorers (производители)**.

d. Выберите **TCP/IP** из списка сетевых протоколов и щелкните по **OK**.

Для выбора клиента для сетей Microsoft:

a. Щелкните по **Add**.

b. Выберите **Client** и щелкните по **Add**.

c. Выберите **Microsoft** из списка производителей.

d. Выберите **Client for Microsoft Networks** из списка сетевых клиентов и щелкните по **OK**.

e. Перезапустите компьютер для реализации изменений.

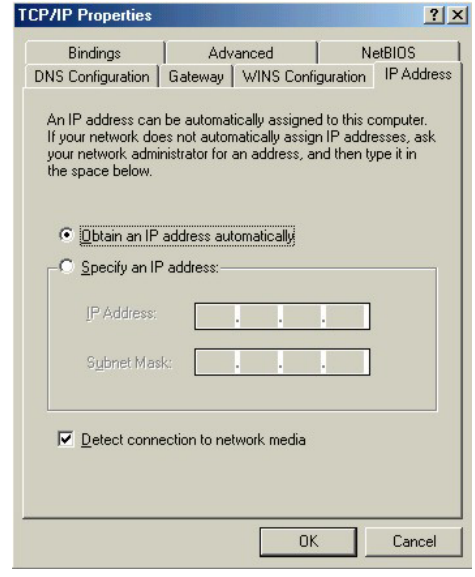
Конфигурирование

1. В окне **Network (Сеть)** щелкните по закладке **Configuration (Конфигурация),** выберите позицию TCP/IP и щелкните по **Properties (Свойства).**

2. Щелкните по закладке **IP Address**.

   Если используется динамический IP-адрес, выберите **Obtain an IP address automatically (Получить IP-адрес автоматически)**.

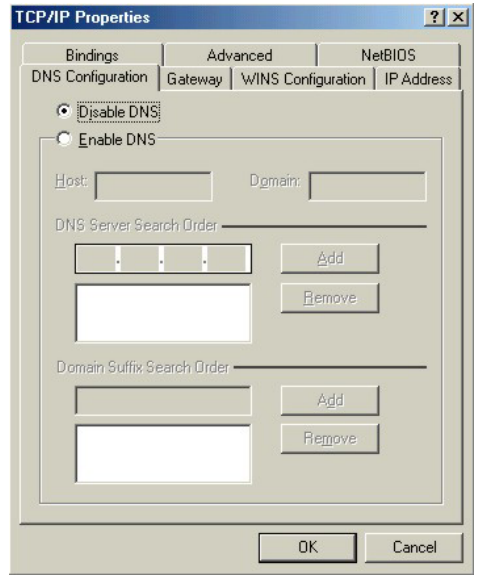
   Если используется статический IP-адрес, выберите **Specify an IP address** и введите соответствующую информацию в полях **IP Address (IP-адрес)** и **Subnet Mask (Маска подсети).**



3. Щелкните по закладке **DNS Configuration (Конфигурация DNS)**.

   Если Вы не располагаете информацией о DNS, выберите **Disable DNS**.

   Если Вы располагаете информацией о DNS, выберите **Enable DNS** и введите соответствующую информацию в указанных ниже полях (в заполнении всех полей может не быть необходимости).

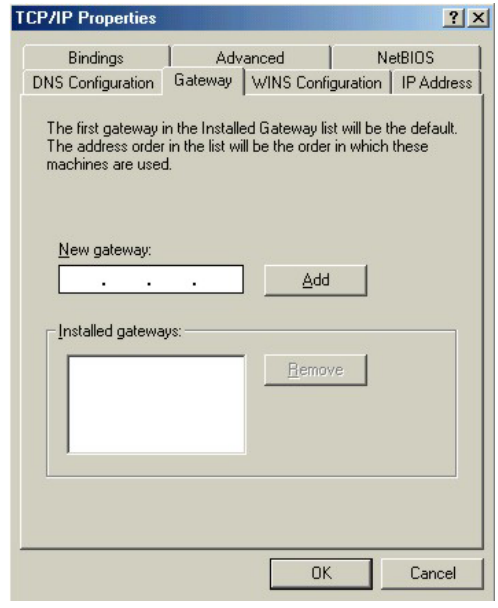


4. Щелкните по закладке **Gateway (Шлюз).**

   Если Вы не знаете IP-адрес шлюза, удалите

ранее установленные шлюзы.

Если Вы знаете IP-адрес шлюза, введите его в поле **New gateway (Новый шлюз)** и щелкните по **Add.**



5. Щелкните по кнопке **OK** для сохранения, а затем закройте окно **TCP/IP Properties (Свойства TCP/IP)**.
6. Щелкните на кнопке **OK**, чтобы закрыть окно **Network (Сеть)**. При появлении соответствующей подсказки вставьте компакт-диск с Windows.
7. Включите OMNI ADSL и перезапустите компьютер (при наличии соответствующей подсказки)

Проверка правильности настроек

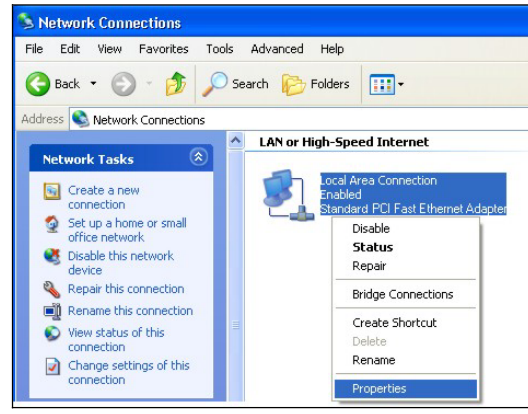
1. Щелкните по **Start**, а затем по **Run**.
2. В окне **Run** наберите "winipcfg", а затем щелкните по **OK** для вызова окна **IP Configuration (Конфигурация IP)**.
3. Выберите сетевой адаптер. При этом должен быть выведен IP-адрес и маска подсети Вашего компьютера, а также шлюз заданный по умолчанию.

Windows 2000/NT/XP

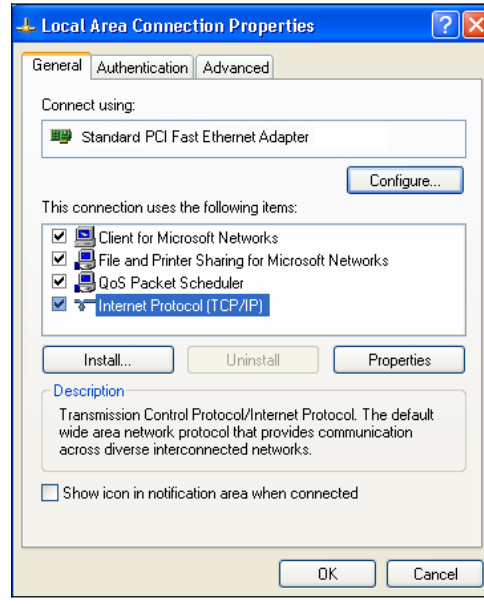
1. Для Windows XP щелкните по **Start**, **Control Panel (Панель управления)**. В Windows 2000/NT, щелкните по **Start**, **Settings (Настройки)**, **Control Panel (Панель управления)**.

2. В Windows XP щелкните по **Network Connections (Сетевые соединения)**. В Windows 2000/NT щелкните по **Network and Dial-up Connections (Сеть и коммутируемые соединения)**.

3. Щелкните правой кнопкой мыши по **Local Area Connection (Соединения ЛВС)**, а затем щелкните по **Properties (Свойства)**.



4. Выберите **Internet Protocol (TCP/IP)** (под закладкой **General (Общие)** в Win XP) и щелкните по **Properties (Свойства)**.

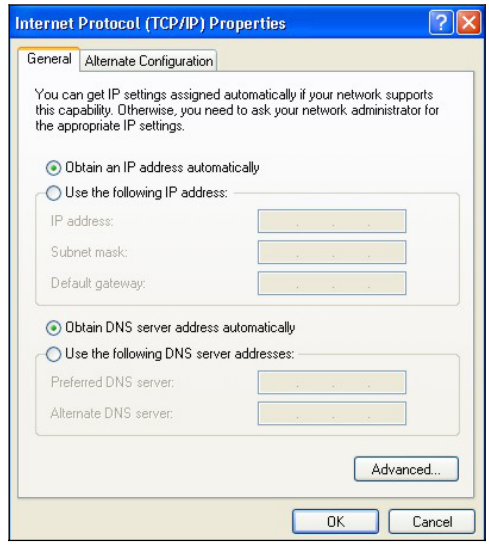


5. Откроется окно **Internet Protocol TCP/IP Properties** (закладка **General** в Windows XP).

   Если используется динамический IP-адрес, щелкните по **Obtain an IP address automatically (Получить IP-адрес автоматически)**.

   Если используется статический IP-адрес, щелкните по **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 по **Advanced (Дополнительные)**.



6. Если Вы не знаете IP-адрес шлюза, удалите все предварительно установленные шлюзы под закладкой **IP Settings (Настройки IP)** и щелкните по **OK**.

   Выполните следующие действия, если хотите сконфигурировать дополнительные IP-адреса:

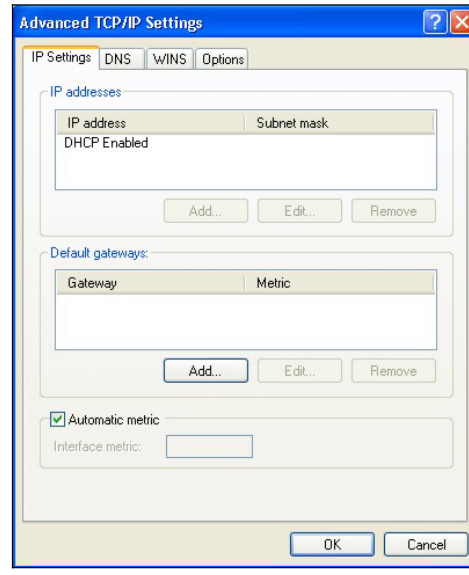
   Под закладкой **IP Settings (Настройки IP)** в IP addresses (IP-адреса) щелкните по **Add.**

   Под закладкой **TCP/IP Address** введите IP-адрес в поле **IP address** и маску подсети в поле **Subnet mask**, а затем щелкните по **Add**.

   Повторите описанные выше действия для всех IP-адресов, которые Вы хотите добавить.

   Сконфигурируйте дополнительные шлюзы по умолчанию под закладкой **IP Settings (Настройки IP)**, щелкнув по **Add (Добавить)** в **Default gateways (Шлюзы по умолчанию)**.

   В **TCP/IP Gateway Address (Адрес шлюза TCP/IP)** введите IP-адрес шлюза по умолчанию в **Gateway (Шлюз)**. Для конфигурирования в ручном режиме метрики (количество транзитных пунктов при передаче данных) отключите **Automatic metric (Автоматический ввод метрики)** и введите метрику в **Metric (Метрика)**.



Щелкните по **Add.**

Повторите описанные выше действия для всех шлюзов, которые Вы хотите добавить.

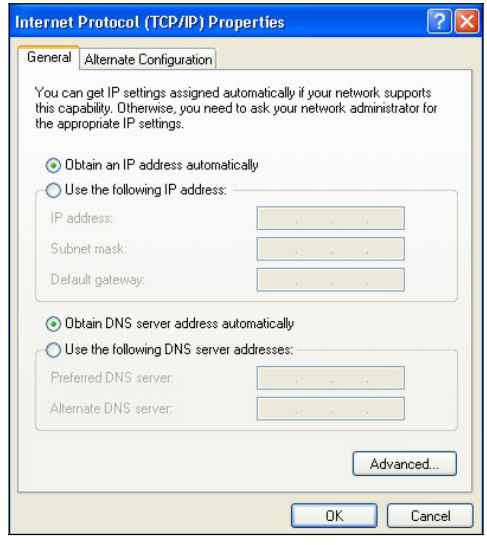
В завершение щелкните по **OK**.

7. В окне **Internet Protocol TCP/IP Properties (Свойства интернет-протокола TCP/IP)** (закладка **General (Общие)** в Windows XP):

   Щелкните по **Obtain DNS server automatically (Получить IP-адрес DNS-сервера автоматически)**, если не знаете IP-адрес(а) сервера(-ов) DNS.

   - Если IP-адрес(-а) сервера DNS известен(-ны), щелкните по **Use the following DNS server addresses (Использовать следующие адреса сервера DNS)** и введите их в полях **Preferred DNS server (Предпочтительный сервер DNS)** и **Alternate DNS server (Альтернативный сервер DNS)**.

   Если серверы DNS уже предварительно сконфигурированы, щелкните по **Advanced**, а затем по закладке **DNS** для их упорядочения.



8. Щелкните по **OK** и закройте окно **Internet Protocol (TCP/IP) Properties (Свойства интернет-протокола (TCP/IP)**.

9. Щелкните по **OK**, чтобы закрыть окно **Local Area Connection Properties (Свойства соединения ЛВС)**.

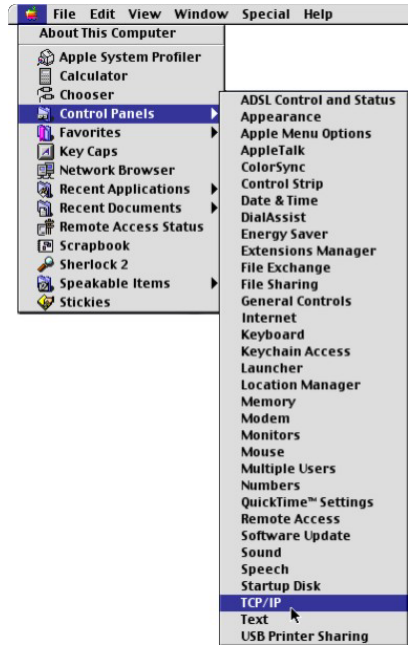
10. Включите OMNI ADSL и перезапустите компьютер (при появлении соответствующей подсказки).

Проверка правильности настроек

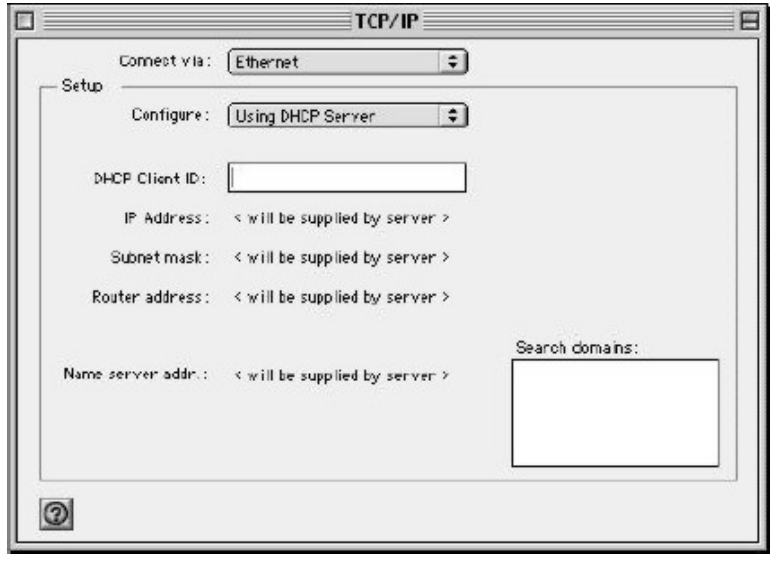
1. Щелкните по **Start**, **All Programs**, **Accessories** и **Command Prompt**.
2. В окне **Command Prompt** наберите "ipconfig", а затем нажмите [ENTER]. Можно также открыть окно **Network Connections**, щелкнуть правой кнопкой мыши по сетевому соединению, щелкнуть по **Status,** а затем щелкнуть по закладке **Support.**

Macintosh OS 8/9

1. Щелкните по меню **Apple**, **Control Panel (Панель управления)**, а затем дважды щелкните по **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.



2. Выберите **Ethernet built-in** из списка **Connect via (Соединение через)**.



3. При динамически назначаемых параметрах выберите **Using DHCP Server** из списка

Configure.

4. При статически назначаемых параметрах выполните следующее:

   В окне **Configure** выберите **Manually**.

   Введите Ваш IP-адрес в окне **IP Address**.

   Введите маску подсети в окне **Subnet mask**.

   Введите IP-адрес OMNI ADSL в окне **Router address (Адрес маршрутизатора)**.

5. Закройте **TCP/IP Control Panel**.

6. При появлении соответствующей подсказки щелкните по **Save** для сохранения изменений в конфигурации.

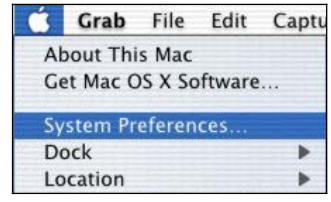
7. Включите OMNI ADSL и перезапустите компьютер (при появлении соответствующей подсказки).

Проверка правильности настроек

Проверьте свойства TCP/IP в окне**TCP/IP Control Panel.**

Macintosh OS X

1. Щелкните по меню **Apple** и по **System Preferences (Системные предпочтения)** для вызова окна **System Preferences (Системные предпочтения)**.

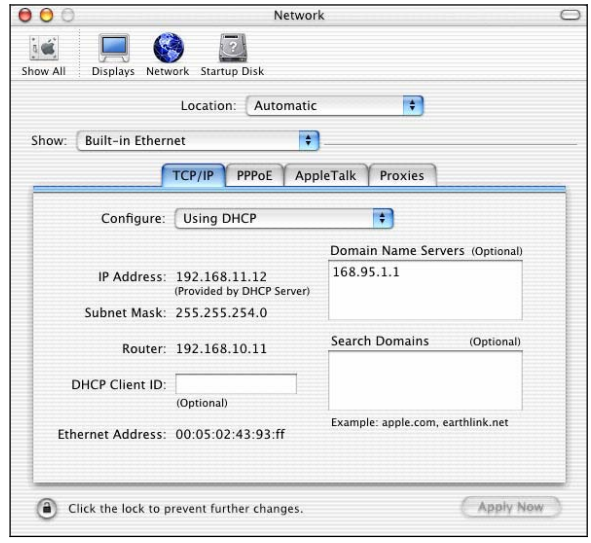


2. Щелкните по иконке в виде клавиши **Network (Сеть)**.

   - Выберите **Automatic (Автоматически)** в списке **Location (Местонахождение)**.

   - Выберите **Built-in Ethernet (Встроенный Ethernet)** в списке **Show (Показать)**.

   - Щелкните по клавише **TCP/IP**.



3. При динамически назначаемых параметрах выберите **Using DHCP Server** из списка **Configure**

4. При статически назначаемых параметрах выполните следующее:

   В окне **Configure (Сконфигурировать)** выберите **Manually (Вручную)**.

   Введите Ваш IP-адрес в окне **IP Address**.

   Введите маску подсети в окне **Subnet mask**.

   Введите IP-адрес OMNI ADSL в окне **Router address (Адрес маршрутизатора)**.

5. Щелкните по **Apply Now** и закройте окно.

6. Включите OMNI ADSL и перезапустите компьютер (при появлении соответствующей подсказки).

Проверка правильности настроек

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

Appendix G
Сплиттеры и микрофильтры

В этом приложении рассказывается о том как выполнить инсталляцию сплиттера POTS (частотного разделителя для подключения телефонного аппарата) или телефонного микрофильтра.

Подключение сплиттера POTS

При использовании стандарта Full Rate (G.dmt) ADSL, можно пользоваться сплиттером POTS (Plain Old Telephone Service/Обычная телефонная сеть) для разделения телефонных сигналов и сигналов ADSL. Это позволяет использовать одну и ту же линию при одновременной работе в сети Интернет и пользовании телефоном. Применение сплиттера помогает также избавиться от отрицательного воздействия помех, вызванных работой телефонных аппаратов.

Установите сплиттер POTS в точке входа телефонных проводов в помещение, как показано на следующем рисунке.

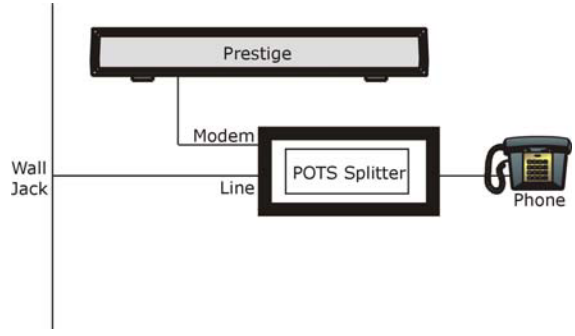


Схема G-1 Подключение сплиттера POTS

Step 1. Подключите сторону с обозначением "Phone" к телефону.

Step 2. Подключите сторону с обозначением "Modem" к OMNI ADSL.

Step 3. Подключите сторону с обозначением "Line" к стенной розетке телефона.

Телефонные микрофильтры

Передача голосовых сигналов телефона происходит в диапазоне низких частот (0 - 4 кГц), в то время как передача сигналов ADSL осуществляется в более высоком диапазоне частот (более 4 кГц). Микрофильтр выступает в качестве фильтра низких частот для Вашего телефона, обеспечивая защиту

передачи данных ADSL от помех, вызванных передачей голосовых сигналов по телефону. Использование телефонного микрофильтра не является обязательным.

Step 1. Подключите телефонный провод, идущий от стенной розетки, к концу Y-образного разъема с одним выводом.

Step 2. Подключите провод, идущий от конца Y-образного разъема с двумя выводами, к "стенной" стороне микрофильтра.

Step 3. Подключите другой провод, идущий от конца Y-образного разъема с двумя выводами, к OMNI ADSL.

Step 4. Подключите "телефонную" сторону микрофильтра к телефону, как показано на следующем рисунке.

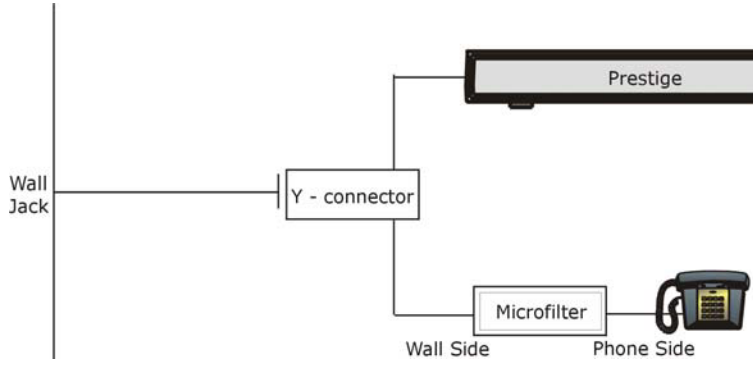


Схема G-2 Подключение микрофильтра

OMNI ADSL с ISDN

Эта часть адресована только тем, кто пользуется маршрутизатором OMNI ADSL с ADSL через ISDN (цифровую сеть с предоставлением комплексных услуг). Ниже приведен пример установки OMNI ADSL с ISDN.

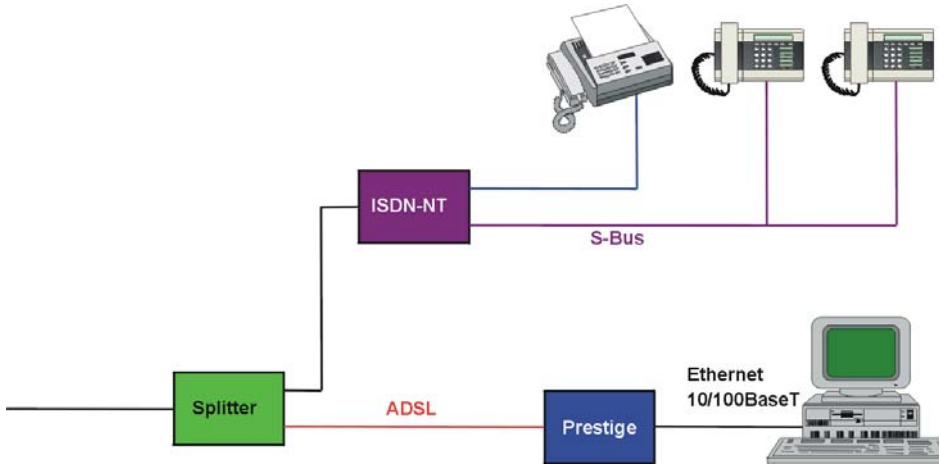


Схема G-3 OMNI ADSL с ISDN

Appendix H
Описание журнала

В данном приложении приводятся описания примеров сообщений журнала маршрутизатора OMNI ADSL[1].

Схема H-1 Журналы сопровождения системы

СООБЩЕНИЕ	ОПИСАНИЕ
`Time calibration is successful`	Маршрутизатор успешно выполнил согласование времени, на основании информации, полученной от сервера времени.
`Time calibration failed`	Маршрутизатор не смог получить информацию от сервера времени.
`DHCP client gets %s`	Клиент DHCP получил новый IP-адрес от сервера DHCP.
`DHCP client IP expired`	Истекло время пользования клиентским IP-адресом DHCP.
`DHCP server assigns %s`	Сервер DHCP назначил клиенту IP-адрес.
`SMT Login Successfully`	Кто-то подключился к интерфейсу SMT маршрутизатора.
`SMT Login Fail`	Кто-то неудачно пытался подключиться к интерфейсу SMT маршрутизатора.
`WEB Login Successfully`	Кто-то подключился к интерфейсу Web-конфигуратора маршрутизатора.
`WEB Login Fail`	Кто-то неудачно пытался подключиться к интерфейсу Web-конфигуратора маршрутизатора.
`TELNET Login Successfully`	Кто-то подключился к маршрутизатору через telnet.
`TELNET Login Fail`	Кто-то неудачно пытался подключиться к маршрутизатору через

[1] На момент написания руководства OMNI ADSL поддерживал генерацию не всех показанных здесь журналов.

Схема H-1 Журналы сопровождения системы

	telnet.
`FTP Login Successfully`	Кто-то подключился к маршрутизатору через ftp.
`FTP Login Fail`	Кто-то неудачно пытался подключиться к маршрутизатору через ftp.

Схема H-2 Журналы UPnP

СООБЩЕНИЕ	ОПИСАНИЕ
`UPnP pass through Firewall`	Пакеты UPnP могут проходить через межсетевой экран.

Журналы регистрации атак могут включать протокол пакета (например, TCP или UDP), инициирующих запись в журнале.

Схема H-3 Журналы регистрации атак

СООБЩЕНИЕ	ОПИСАНИЕ
`attack (Protocol)`	Межсетевым экраном обнаружена атака. Журнал также может отображать протокол (например, TCP или UDP).
`land Protocol)`	Межсетевой экран обнаружил атаку типа land. Журнал также может отображать протокол (например, TCP или UDP).
`icmp echo ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку типа ICMP echo. См. раздел о сообщениях ICMP для получения дополнительной информации о типах и кодах.
`syn flood TCP`	Межсетевой экран обнаружил атаку типа "TCP syn flood".
`ports scan TCP`	Межсетевой экран обнаружил атаку типа "сканирование порта TCP".
`teardrop (Protocol)`	Межсетевой экран обнаружил атаку типа "teardrop".
`illegal command TCP`	Межсетевой экран обнаружил атаку типа "запрещенная команда TCP SMTP".
`NetBIOS TCP`	Межсетевой экран обнаружил атаку типа "TCP NetBIOS".

Схема H-3 Журналы регистрации атак

СООБЩЕНИЕ	ОПИСАНИЕ
`ip spoofing - no routing entry (Protocol)`	Межсетевой экран обнаружил атаку типа "IP spoofing", при отсутствии у OMNI ADSL маршрута, заданного по умолчанию. Журнал также может отображать протокол (например, TCP или UDP).
`vulnerability ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку типа "ICMP vulnerability"; См. раздел о сообщениях ICMP для получения дополнительной информации о типах и кодах.
`traceroute ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку типа "ICMP traceroute"; См. раздел о сообщениях ICMP для получения дополнительной информации о типах и кодах.

Журналы регистрации доступа могут включать следующую информацию:

- (Protocol) - является протоколом, использующимся пакетом (например, TCP или UDP), инициирующим запись в журнале.
- (Direction) - является направлением, по которому передавался пакет (например, LAN - WAN или WAN - LAN)
- (Rule) - является номером правила межсетевого журнала, инициирующим запись в журнале.

Схема H-4 Журналы регистрации доступа

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy (Protocol, Direction)`	Доступ соответствует стратегии, заданной по умолчанию, и OMNI ADSL блокирует или пересылает его трафик согласно конфигурации стратегии межсетевого экрана, заданной по умолчанию.
`Firewall rule match (Protocol, Direction, Rule)`	Доступ соответствует правилу межсетевого экрана, и OMNI ADSL блокирует или пересылает его трафик согласно конфигурации правила.
`Firewall rule NOT match: (Protocol, Direction, Rule)`	Доступ не соответствует правилу межсетевого экрана, и OMNI ADSL регистрирует его.
`dest port (Protocol, Direction)`	Доступ не соответствует правилу межсетевого экрана о порте назначения, и OMNI ADSL регистрирует его.

Схема H-4 Журналы регистрации доступа

СООБЩЕНИЕ	ОПИСАНИЕ
src port (Protocol, Direction)	Доступ не соответствует правилу межсетевого экрана о порте источника, и OMNI ADSL регистрирует его.
dest IP (Protocol, Direction)	Доступ не соответствует правилу межсетевого экрана об IP-адресе назначения, и OMNI ADSL регистрирует его.
src IP (Protocol, Direction)	Доступ не соответствует правилу межсетевого экрана об IP-адресе источника, и OMNI ADSL регистрирует его.
protocol (Protocol, Direction)	Доступ не соответствует правилу межсетевого экрана о протоколе, и OMNI ADSL регистрирует его.
Triangle route packet forwarded (Protocol)	Межсетевой экран разрешает проведение через него сеанса связи с маршрутом типа "треугольник".
ICMP Source Quench	OMNI ADSL отправил или получил ICMP пакет для передачи хосту указания уменьшить скорость передачи данных.
ICMP Time Exceed	OMNI ADSL отправил или получил ICMP пакет о превышении времени, поскольку пакет с нулевой установкой "времени жизни" - Time To Live (TTL) был сброшен.
ICMP Destination Unreachable	При сбросе пакета данных OMNI ADSL отправил или получил ICMP пакет "недостижимый адресат назначения", из-за того что порт назначения не был открыт.
Packet without a NAT table entry blocked (Protocol)	Маршрутизатор заблокировал пакет, не имеющий записи, отвечающей таблице NAT.
Out of order TCP handshake packet blocked (Protocol)	Маршрутизатор заблокировал пакет квитирования TCP, вышедший с нарушением очередности
Unsupported/out-of-order ICMP (Protocol)	OMNI ADSL генерирует этот журнал после сброса пакета ICMP по одной из следующих причин: 1. OMNI ADSL не поддерживает протокол обработки пакетов ICMP. 2. Пакет ICMP является ответом типа "эхо", для которого не было соответствующего ему запроса этого типа.
Router reply ICMP packet	Маршрутизатор отправил ответный пакет ICMP. Этот пакет автоматически обошел межсетевой экран.

Схема H-4 Журналы регистрации доступа

СООБЩЕНИЕ	ОПИСАНИЕ
Remote access denied	Маршрутизатор блокировал попытку удаленного доступа.

Схема H-5 Журналы сброса TCP

СООБЩЕНИЕ	ОПИСАНИЕ
Межсетевой экран отправил пакеты сброса TCP	Межсетевой экран отправил пакеты сброса TCP.

Схема H-6 Узлы ICMP

ТИП	КОД	ОПИСАНИЕ
0		Ответ типа "эхо"
	0	Ответное сообщение типа "эхо"
3		Адресат недоступен
	0	Сеть недоступна
	1	Хост недоступен
	2	Протокол недоступен
	3	Порт недоступен
	4	Пакет, требующий фрагментации, был сброшен, поскольку он был отправлен с признаком Don't Fragment (Не фрагментировать - DF)
	5	Проблема маршрута источника
4		Срыв источника
	0	Шлюз может сбросить датаграмму Интернета, если у него не хватает объема буферной памяти для постановки датаграммы в очередь на передачу в следующую сеть по маршруту к сети назначения.
5		ПЕРЕНАПРАВЛЕНИЕ
	0	Перенаправление датаграмм для сети

Схема H-6 Узлы ICMP

ТИП	КОД	ОПИСАНИЕ
	1	Перенаправление датаграмм для хоста
	2	Перенаправление датаграмм для типов сервиса и сети
	3	Перенаправление датаграмм для типов сервиса и хоста
8		ЭХО
	0	Сообщение типа "эхо"
11		Превышение лимита времени
	0	"Время жизни" истекло в пути
	1	Превышен лимит времени восстановления фрагмента
12		Проблема параметра
	0	Указатель показывает ошибку
13		Временной ярлык
	0	Сообщение с запросом и временным ярлыком
14		Ответ на временной ярлык
	0	Ответное сообщение с временным ярлыком
15		Запрос информации
	0	Сообщение с запросом информации
16		Информационный ответ
	0	Ответное информационное сообщение

Appendix I
Характеристики адаптера питания

I.1 Маршрутизатор ADSL OMNI ADSL LAN R-E1/-E3/-E7

СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACS
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/23 Вт (макс)
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	AA-121A
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/18 Вт (макс)
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
ЮЖНО-АЗИАТСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACCP-5720
Входное напряжение	Напряжение переменного тока 220 В/50 Гц/18 Вт
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	CCEE (GB8898)
ЮЖНО-АЗИАТСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	BH-48 (AA-121AP)
Входное напряжение	Напряжение переменного тока 220 В/50 Гц

Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	CCEE (GB8898)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	DV-121AACCP-5716
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/100 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	TUV-GS, CE (EN 60950)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	AA-121ABN
Входное напряжение	Переменный ток 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)
СТАНДАРТ ВЕЛИКОБРИТАНИИ	
Модель адаптера питания переменного тока	AA-121AD
Входное напряжение	Переменный ток 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950, BS 7002)

I.2 Маршрутизатор ADSL OMNI ADSL LAN R-11

СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACS
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/23 Вт
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт

Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
ЮЖНО-АЗИАТСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACCP-5720
Входное напряжение	Напряжение переменного тока 220 В/50 Гц/18 Вт
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	CCEE (GB8898)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	DV-121AACUP-5716
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/19 Вт
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	TUV, CE (EN 61558)

I.3 Маршрутизатор ADSL Ethernet OMNI ADSL LAN R-13/-17

СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACS
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/23 Вт (макс).
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	12 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	AA-121A
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/18 Вт (макс)
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	12 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)

ЮЖНО-АЗИАТСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACCP-5720
Входное напряжение	Напряжение переменного тока 220 В/50 Гц/18 Вт
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	12 Вт
Нормы техники безопасности	CCEE (GB8898)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	AA-121ABN
Входное напряжение	Переменный ток 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	12 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)

I.4 Маршрутизатор ADSL через ISDN OMNI ADSL LAN R-31/-33

СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACS
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/23 Вт (макс).
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	AA-121A
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/18 Вт (макс)
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)

ЮЖНО-АЗИАТСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACCP-5720
Входное напряжение	Напряжение переменного тока 220 В/50 Гц/18 Вт
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	CCEE (GB8898)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	AA-121ABN
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	DV-121AACCP-5716
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/100 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	TUV-GS, CE (EN 60950)
СТАНДАРТ ВЕЛИКОБРИТАНИИ	
Модель адаптера питания переменного тока	AA-121AD
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	8 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)

I.5 Маршрутизатор ADSL с 4-портовым коммутатором Ethernet OMNI ADSL LAN H-11/-13

СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ

Модель адаптера питания переменного тока	DV-1215A
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/30 Вт
Выходное напряжение	Напряжение переменного тока 12 В/ 1,25 А
Выходная мощность	12 Вт
Нормы техники безопасности	UL, CUL, CSA (UL 1310, CSA C22.2 No.223)
СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	AA-121A25
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/19 Вт
Выходное напряжение	Напряжение переменного тока 12 В/ 1,25 А
Выходная мощность	12 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	**AA-121A3BN**
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В /1,3 А
Выходная мощность	12 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)

I.6 Маршрутизатор ADSL с 4-портовым коммутатором Ethernet/Беспроводная LAN OMNI ADSL LAN HW-11/-13/

СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-1215A
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/30 Вт
Выходное напряжение	Напряжение переменного тока 12 В/ 1,25 А
Выходная мощность	13 Вт
Нормы техники безопасности	UL, CUL, CSA (UL 1310, CSA C22.2 No.223)
СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	AA-121A25

Входное напряжение	Напряжение переменного тока 120 В/60 Гц/19 Вт
Выходное напряжение	Напряжение переменного тока 12 В/ 1,25 А
Выходная мощность	13 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	AA-121A3BN
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1,3 А
Выходная мощность	13 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)

I.7 Модели маршрутизатора OMNI ADSL LAN H-31/-33/-37 и OMNI ADSL LAN HW-31/-33/-37 и маршрутизатор ADSL с 4-портовым коммутатором для беспроводной LAN

СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-1215A
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/30 Вт
Выходное напряжение	Напряжение переменного тока 12 В/ 1,25 А
Выходная мощность	15 Вт
Нормы техники безопасности	UL, CUL, CSA (UL 1310, CSA C22.2 No.223)
СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	AA-121A25
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/19 Вт
Выходное напряжение	Напряжение переменного тока 12 В/ 1,25 А
Выходная мощность	15 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	AA-121A3BN

Входное напряжение	Напряжение переменного тока 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1,3 А
Выходная мощность	15 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)
СТАНДАРТ ВЕЛИКОБРИТАНИИ	
Модель адаптера питания переменного тока	AA-121A3D
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1,3 А
Выходная мощность	15 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)

I.8 Маршрутизатор ADSL с 4-портовым коммутатором OMNI ADSL LAN H-E1/3/7

СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACS
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/23 Вт (макс).
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
СЕВЕРОАМЕРИКАНСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	AA-121A
Входное напряжение	Напряжение переменного тока 120 В/60 Гц/18 Вт (макс)
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	UL, CUL (UL 1310, CSA C22.2 № 223)
ЮЖНО-АЗИАТСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	DV-121AACCP-5720

Входное напряжение	Напряжение переменного тока 220 В/50 Гц/18 Вт
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	CCEE (GB8898)
ЮЖНО-АЗИАТСКИЙ СТАНДАРТ	
Модель адаптера питания переменного тока	BH-48 (AA-121AP)
Входное напряжение	Напряжение переменного тока 220 В/50 Гц
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	CCEE (GB8898)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	DV-121AACUP-5716
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/100 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	TUV-GS, CE (EN 60950)
СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	AA-121ABN
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950)
СТАНДАРТ ВЕЛИКОБРИТАНИИ	
Модель адаптера питания переменного тока	AA-121AD
Входное напряжение	Напряжение переменного тока 230 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	ITS-GS, CE (EN 60950, BS 7002)

АВСТРАЛИЙСКИЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ	
Модель адаптера питания переменного тока	AA-121AE
Входное напряжение	Напряжение переменного тока 240 В/50 Гц/140 мА
Выходное напряжение	Напряжение переменного тока 12 В/1 А
Выходная мощность	10 Вт
Нормы техники безопасности	(AS/NZS 60950: 2000)