P-660H/HW

Модем ADSL2+ с 4-портовым коммутатором

802.11g+ беспроводной модем ADSL2+ с 4-портовым коммутатором

Техническое руководство

Версия 3.40

Август 2004

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. Она также не передает никаких лицензий на свои патентные права, а также на патентные права третьих сторон. Кроме того, корпорация ZyXEL сохраняет право вносить изменения в любые описанные здесь изделия без дополнительного уведомления. Данное издание также может быть изменено без уведомления.

Товарные знаки

ZyNOS (ZyXEL Network Operating System - сетевая операционная система корпорации ZyXEL) является зарегистрированной торговой маркой корпорации ZyXEL Communications, Inc. Другие товарные знаки, упомянутые в данном издании, используются только в целях идентификации и могут являться собственностью соответствующих владельцев.

Предисловие

Поздравляем с приобретением 802.11g+ беспроводного модема ADSL 2+ P-660W или 802.11g+ беспроводного модема ADSL 2+ P-660HW с 4-портовым коммутатором

Зарегистрируйте Ваш продукт Онлайн для получения электронных писем о бесплатных обновлениях микропрограмм и посетите сайт www.zyxel.com для получения информации о линейке продукции.

Модели P-660W и P-660HW имеют встроенный mini-PCI модуль и обеспечивают подключение беспроводной сети 802.11g без затрат на дополнительную кабельную инфраструктуру.

Ваше устройство легко устанавливается и конфигурируется.

О данном Руководстве пользователя

В данном руководстве последовательно рассматриваются все аспекты правильного конфигурирования Prestige для различных задач. Разделы данного руководства, посвященные Web-конфигуратору, содержат основную информацию о характеристиках, конфигурируемых при помощи Web-конфигуратора. Разделы данного руководства, посвященные SMT, содержат основную информацию только о характеристиках, не настраиваемых при помощи Web-конфигуратора.

Для конфигурирования Prestige следует использовать Web-конфигуратор, системный терминал управления (интерфейс SMT) или интерфейс интерпретатора команд. Не все характеристики можно сконфигурировать при помощи любого интерфейса.

Сопроводительная документация

- Справочный компакт-диск

  На входящем в комплект компакт-диске расположена справочная документация.

- Краткое руководство

  Краткое руководство должно помочь Вам начать работу немедленно. В них содержится информация о подключении и указания по началу работы.

- Онлайн - справка по Web-конфигуратору
  Встроенная сетевая справка с описанием отдельных экранов и дополнительной информацией.

- корпорации ZyXEL Глоссарий и web-сайт
  См. онлайн - глоссарий программных терминов и дополнительную справочную документацию на сайте www.zyxel.com.

Обратная связь с пользователем

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

Условные обозначения

- “Введите” означает, что Вам следует напечатать один или несколько символов. "Выберите" означает, что Вам следует использовать одну из предложенных опций.
- Заголовки и надписи меню SMT выполнены полужирным шрифтом **Bold 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.
- Действия курсором мыши описаны через запятую. Например, “щелкнуть на значке Apple, **Control Panels** и **Modem**” означает, что сначала следует щелкнуть на значке Apple, затем перевести курсор мыши на пункт **Control Panels,** а затем щелкнуть на пункте **Modem**.
- Для краткости в данном руководстве будет использоваться "напр." вместо "например" и "т.е." вместо "то есть" и "другими словами".
- Далее в данном Руководстве серия Prestige 660H/HW может обозначаться как Prestige. Это относится ко всем моделям (ADSL по обычной телефонной сети и ADSL по сети ISDN), если иное не оговорено особо.

Введение в DSL

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, телефонные коммутационные устройства предназначены для блокировки сигналов частотой выше 4,000 Гц с целью отфильтровывания помех на линии голосовой связи. Однако в настоящий момент идет активный поиск способов увеличения пропускной способности для облегчения доступа в сеть - а значит, технологий DSL.

Существует семь типов услуги DSL в зависимости от скорости (от 16 Кбит/с до 52 Мбит/с). Услуга может быть либо симметричной (одинаковая скорость в обоих направлениях), либо асимметричной (объем принимаемых данных превышает объем передаваемых данных). Ассиметричные услуги (ADSL) подходят, прежде всего, для пользователей Интернета, так как обычно ими больше информации принимается, чем передается. Например, простым нажатием на кнопку в web-браузере можно запустить расширенную загрузку, включающую графику и текст.

При возрастании скорости передачи данных уменьшается расстояние, 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 установлена всегда и вызов не требуется.

Введение в ADSL

ASDL представляет собой асимметричную технологию. Это означает, что скорость исходящего потока данных намного больше, чем скорость входящего. Как уже было сказано, такая система хорошо подходит для обычного Интернет - сеанса связи, в течение которого большее количество информации загружается, например, с web-серверов, чем выгружается. ADSL работает в более высоком диапазоне частот, чем диапазон частот голосовых услуг, поэтому обе системы могут использовать один кабель.

Глава I:

НАЧАЛО РАБОТЫ

Эта часть содержит пошаговые инструкции обеспечивающие доступ к Prestige. Рассматриваются основные функции и варианты использования, доступ к Web-конфигуратору и конфигурирование экранов Мастера Установки первоначальной настройки.

Раздел 1
Знакомство с Prestige

В этой главе описываются основные функции и варианты использования Prestige.

1.1 Ознакомление с Prestige

Prestige конструктивно объединяет в себе высокоскоростной (10/100 Мбит/с) интерфейс(ы) LAN с автоматическим выбором скорости и высокоскоростной порт ADSL. Prestige отлично подходит для высокоскоростного поиска в сети Интернет и соединения локальных сетей (LAN-to-LAN) с удаленными сетями. Prestige содержит маршрутизатор, совместимый со стандартом ADSL. При дальнейшем обновлении микропрограммного обеспечения будут поддерживаться стандарты ADSL2/ADSL2+. Максимальные скорости передачи данных, достигаемые Prestige для каждого стандарта, представлены в следующей таблице.

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

Стандарт, поддерживаемый Вашим Интернет-провайдером, устанавливает достижение максимальных скоростей приема и передачи данных. Достижение фактической скорости зависит также от расстояния до Вашего Интернет-провайдера, шума, качества линии и т.д.

Объединяя DSL и NAT, Prestige обеспечивает простоту установки и доступа в Интернет. Prestige является также универсальным безопасным решением с надежным межсетевым экраном, контент-фильтрованием и защищенным Wi-Fi доступом (WPA).

Модели, включенные в эту серию на момент написания, следующие:

- Prestige серии 660W
- Prestige серии 660HW

“H” обозначает встроенный 4-портовый коммутатор (концентратор), а “W” обозначает входящую в комплект беспроводную карту расширения. Prestige 660W и Prestige 660HW обеспечивают возможность подключения к беспроводной 802.11g LAN, позволяющей пользователям наслаждаться удобством и мобильностью работы в пределах зоны охвата.

Модели, заканчивающиеся на “1”, напр. P660HW-61, обозначают устройство, которое работает через аналоговую телефонную систему POTS (Plain Old Telephone Service/Услуга традиционной телефонной сети общего пользования). Модели, заканчивающиеся на “3”, обозначают устройство, которое работает через ISDN (Integrated Synchronous Digital System/Цифровая сеть связи с комплексными услугами). Модели, заканчивающиеся на “7”, обозначают устройство, которое работает через T-ISDN (UR-2).

Используйте только то микропрограммное обеспечение, которое установлено для конкретной модели Prestige. См. маркировочный знак на основании Prestige.

Web-браузер на базе Графического Интерфейса Пользователя обеспечивает простоту управления.

1.2 Характеристики Prestige

В следующих разделах представлено описание характеристик устройств серии Prestige. Характеристики варьируются в зависимости от модели Prestige. В данной таблице перечислены только основные характеристики изделий Prestige. Для получения более подробной информации см. описание характеристик, представленное ниже.

Некоторые характеристики имеются не в каждой модели. См. таблицу *Характеристики модели*, чтобы увидеть какие характеристики определены для Вашей модели Prestige.

Табл. 1-1 Характеристики модели

МОДЕЛЬ PRESTIGE / ХАРАКТЕРИСТИКИ	P660W	P660HW
Четырехпортовый коммутатор		O
Интерфейс LAN Ethernet с автоопределением скорости 10/100 Мбит/с	O	O
Кнопка перезапуска	O	O
Выключатель питания	O	O

Табл. 1-1 Характеристики модели

МОДЕЛЬ PRESTIGE / ХАРАКТЕРИСТИКИ	P660W	P660HW
Система сетевой безопасности IEEE 802.1x	O	O
Переадресация трафика	O	O
Межсетевой экран	O	O
Контент-фильтр	O	O
Маршрутизация на базе стратегии IP	O	O
Унифицированная функция Plug and Play (UPnP)	O	O
Дистанционное управление	O	O
Централизованные регистрационные журналы	O	O
Защищенный доступ Wi-Fi (WPA)	O	O
Параметры таблицы: “O” в столбце модели указывает на то, что модель имеет данную характеристику. Конкретный номер в определенной модели может отображаться поочередно. Информация, представленная в этой таблице верна на момент написания, но она может изменяться.		

- **Высокоскоростной доступ в Интернет**

Маршрутизатор ADSL Prestige может поддерживать скорости приема и передачи данных, представленные в *Разделе 1.1*. Величина фактической достижимой скорости зависит от DSLAM оборудования Интернет-провайдера.

- **Начальная конфигурация доступа в Интернет**

При включении и подключении Prestige к телефонной розетке, он автоматически обнаруживает настройки подключения к Интернету (такие как номера VCI/VPI и метод инкапсуляции), полученные от Интернет-провайдера и производит необходимые изменения конфигурации. В случаях, когда требуется дополнительная учетная информация (такая как имя и пароль учетной записи пользователя Интернет) или Prestige не может подключиться к Интернет-провайдеру, происходит переадресация к web-экрану(-ам) по вводной информации или устранению неисправностей.

- **Любой IP**

Функция Любой IP позволяет компьютеру получить доступ в Интернет и Prestige без изменения настроек сети (таких как IP-адрес и маска подсети) компьютера, даже если IP-адреса компьютера и Prestige находятся в разных подсетях.

- **Межсетевой экран**

В Prestige реализован полнофункциональный межсетевой экран с защитой от DoS (Denial of Service/ Отказ от обслуживания). По умолчанию, при активированном межсетевом экране весь входящий трафик из WAN в LAN блокируется, если только он не инициирован из LAN. Межсетевой экран Prestige поддерживает контроль TCP/UDP, распознавание и предотвращение DoS, извещения в реальном времени, отчеты и журнальные регистрации.

Большинство характеристик Prestige можно сконфигурировать посредством SMT, однако межсетевой экран и контент-фильтрование рекомендуется конфигурировать при помощи Web-конфигуратора.

- **Контент-фильтрование**

Контент-фильтрование позволяет блокировать доступ на запрещенные web-сайты Интернета, планировать фильтрование Prestige и предоставлять правомочный IP-адрес LAN нефильтруемого доступа в Интернет.

- **Беспроводная 11 Мбит/с LAN IEEE 802.11g**

IEEE 802.11g полностью совместим со стандартом IEEE 802.11b. Это означает, что радио карта IEEE 802.11b может непосредственно связываться с точкой доступа IEEE 802.11g (и наоборот) на скорости 11 Мбит/с или ниже, в зависимости от режима. IEEE 802.11g имеет несколько промежуточных вариантов скорости передачи между максимальной и минимальной скоростью передачи данных. Скорость передачи данных IEEE 802.11g и режим модуляции выглядят следующим образом:

IEEE 802.11g	
СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ (МБИТ/С)	**МОДУЛЯЦИЯ**
1	DBPSK (Differential Binary Phase Shift Keyed/Кодирование дифференциальным двоичным сдвигом фазы)
2	DQPSK (Differential Quadrature Phase Shift Keying/Кодирование дифференциальным квадратурным сдвигом фазы)
5.5/ 11	CCK (Complementary Code Keying/Дополнительная кодовая манипуляция)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing/Ортогональное мультиплексирование с разделением частот)

Prestige может воспринимать радиочастотные помехи от других устройств в диапазоне 2.4 ГГц, таких как микроволновые печи, радиотелефоны, устройства технологии Bluetooth и других беспроводных LAN.

- **Фильтрация MAC-адреса беспроводной LAN**

Prestige может проверять MAC-адреса базы данных настроек пользователя согласно списку допущенных или отвергнутых MAC-адресов.

- **Кодирование WEP**

WEP (Конфиденциальность, равная конфиденциальности в проводных сетях) кодирует пакеты данные до их передачи через беспроводную сеть для обеспечения соблюдения конфиденциальности связи в сети.

- **Защищенный доступ Wi-Fi**

Защищенный доступ Wi-Fi (WPA) является разновидностью спецификации безопасности IEEE 802.11i. Основные различия между WPA и WEP заключаются в применении аутентификации пользователя и усовершенствованном шифровании данных.

- **Переадресация трафика**

Переадресация трафика пересылает трафик WAN на резервный шлюз, если Prestige не может установить соединение с Интернетом, таким образом выступая в качестве вспомогательного соединения, если не устанавливается обычное соединение WAN.

- **Унифицированный Plug and Play (UPnP)**

Используя стандартный протокол TCP/IP, Prestige и другие устройства с функцией UPnP могут динамически подсоединяться к сети, получать IP-адрес и передавать свои возможности другим устройствам в сети.

- **Поддержка PPPoE (RFC2516)**

PPPoE (Протокол “точка-точка“ через Ethernet) эмулирует коммутируемое соединение. Это позволяет Интернет-провайдеру использовать новые широкополосные технологии, такие как ADSL, в существующей конфигурации сети. Драйвер PPPoE, установленный на Prestige, прозрачен для компьютеров в LAN, которые видят только Ethernet и не распознают PPPoE, таким образом избавляя Вас от необходимости управления клиентами PPPoE на отдельных компьютерах.

- **Трансляция сетевых адресов (NAT)**

Трансляция сетевых адресов (NAT) допускает трансляцию адреса межсетевого протокола (IP), используемого в одной сети (напр., частный IP-адрес, используемый в местной сети) в другие IP-адреса, известные в другой сети (напр., общедоступный IP-адрес, используемый в Интернете).

- **Интерфейс(ы) 10/100M Ethernet/Fast Ethernet с автоматическим выбором скорости**

Функция автоматического выбора скорости позволяет Prestige определять скорость входящего потока данных и соответствующим образом настраиваться без ручного вмешательства. Она позволяет быстро передавать данные (со скоростью 10 Мбит/с или 100 Мбит/с) в полудуплексном или дуплексном режиме в зависимости от возможностей сети Интернет.

- **Интерфейс(ы) 10/100 Мбит/с Ethernet с автоматическим распознаванием кабеля (MDI/MDI-X)**

Эти интерфейсы автоматически настраиваются на использование 'прямого' или 'перекрестного' кабеля Ethernet.

- **Поддержка динамического DNS**

С поддержкой динамического DNS можно получить псевдоним статического имени хоста для динамического IP-адреса, обеспечивающего хосту возможность быть более доступным из различных частей Интернета. Для использования этой услуги необходимо зарегистрироваться у провайдера услуг динамического DNS.

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

Prestige поддерживает до 8 PVC.

- **Стандарты скорости передачи данных ADSL**

  - Режим полной скорости (ANSI T1.413, выпуск 2; G.dmt (G.992.1), поддерживающий скорость линии до 8 Мбит/с для приема данных и 832 кбит/с для передачи данных.
  - G.lite (G.992.2), поддерживающий скорость линии до 1.5 Мбит/с для приема данных и 512 кбит/с для передачи данных.
  - Поддерживает многорежимный стандарт (ANSI T1.413, выпуск 2; G.dmt (G.992.1); G.lite (G992.2)).
  - TCP/IP (Протокол управления передачей/Межсетевой протокол) - протокол сетевого уровня.
  - ATM (Асинхронный режим передачи) Forum UNI 3.1/4.0 PVC.
  - Поддерживает до 8 PVC (UBR, CBR, VBR).
  - Многопротокольный через AAL5 (Уровень 5 адаптации ATM) (RFC 1483).
  - PPP (Протокол “точка-точка“) через AAL5 (RFC 2364).
  - PPP через Ethernet через AAL5 (RFC 2516).

- RFC 1661.
- PPP через PAP (Протокол аутентификации по паролю) (RFC 1334).
- PPP через CHAP (Протокол аутентификации по методу “вызов-рукопожатие“) (RFC 1994).

➢ **Поддержка протоколов**

- Поддержка DHCP

  DHCP (Dynamic Host Configuration Protocol/Протокол динамического конфигурирования хост-машины) позволяет отдельным клиентским компьютерам при включении получать доступ к конфигурации TCP/IP с центрального сервера DHCP. У Prestige возможности сервера DHCP реализованы аппаратно и включены по умолчанию. Он может назначать IP-адреса, шлюз IP по умолчанию и серверы DNS для клиентов DHCP. Кроме того, Prestige 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 несколько логических сетей с помощью одного интерфейса Ethernet. Prestige поддерживает три логических интерфейса LAN через один физический интерфейс Ethernet, при этом сам Prestige выступает в качестве шлюза для каждой сети LAN.

- Маршрутизация на базе стратегии IP (IPPR)

  Обычно маршрутизация основывается только на адресе назначения, а маршрутизатор выбирает кратчайший 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.

- Протокол канального уровня PPP (Point-to-Point Protocol/Протокол “точка-точка“).
- Прозрачная передача протоколов для неподдерживаемых протоколов сетевого уровня.
- RIP I/RIP II
- Proxy-сервер IGMP
- Поддержка ICMP
- Поддержка ATM QoS
- Поддержка MIB II (RFC 1213)

➢ **Сетевая совместимость**

Prestige совместим с ADSL DSLAM (Мультиплексор цифровых абонентских линий) большинства ведущих производителей, что максимально упрощает его конфигурирование

- **Мультиплексирование**

Prestige поддерживает мультиплексирование на базе VC и LLC.

- **Инкапсуляция**

Prestige поддерживает PPPoA (RFC 2364 - PPP через уровень 5 адаптации ATM), инкапсуляцию (RFC 1483) через ATM, маршрутизацию с инкапсуляцией MAC (ENET), а также PPP через Ethernet (RFC 2516).

- **Сетевое управление**

  - Меню управляется SMT (System Management Terminal/Системная консоль)
  - Встроенный Web-конфигуратор
  - CLI (Интерпретатор командной строки)
  - Дистанционное управление посредством Telnet или Web.
  - Возможность управления по протоколу SNMP
  - Сервер DHCP/Клиент/Ретранслятор
  - Встроенные средства диагностики
  - Системный журнал
  - Поддержка Telnet (Защищенный паролем сетевой теледоступ к внутреннему диспетчеру конфигурации)
  - Сервер TFTP/FTP, обновление микропрограммного обеспечения и резервное сохранение конфигурации/поддержки
  - Поддержка OAM F4/F5 методом обратной передачи, AIS и ячейки OAM RDI

- **Другие характеристики PPPoE**

  - Время простоя PPPoE
  - Предоставление канала по требованию PPPoE

- **Возможности диагностики**

Prestige может выполнять различные самодиагностические тесты. Эти тесты проверяют целостность следующих цепей:

  - Флэш-память
  - Цепь ADSL

- ОЗУ
- Порт LAN

➢ **Фильтры пакетов**

Функции фильтрации пакетов Prestige позволяют повысить уровень защиты и управления сетью.

➢ **Простота установки**

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

➢ **Корпус**

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

1.3 Применение Prestige

Вот несколько примеров использования Prestige, где он незаменимым.

1.3.1 Доступ в Интернет

Prestige является отличным решением для высокоскоростного доступа в Интернет. Prestige поддерживает протокол TCP/IP, который использует Интернет. Prestige совместим с ADSL DSLAM (Концентратор цифровых абонентских линий) всех ведущих производителей. DSLAM представляет собой стойку с линейными картами ADSL, данные с которых мультиплексируются в магистральный сетевой интерфейс/соединение (напр., T1, OC3, DS3, ATM или Frame Relay). Он может также использоваться в качестве эквивалента модемной стойки для ADSL. Кроме того, Prestige 660H/HW позволяет беспроводным клиентам получать доступ к сетевым ресурсам. Типичный пример организации доступа в Интернет приведен ниже.

Рис. 1-1 Организация доступа в Интернет Prestige

Учетная запись одиночного пользователя для доступа в Интернет

Для среды SOHO (Small Office/Home Office - Малый офис/Домашний офис) Prestige предлагает функцию учетной записи одиночного пользователя (SUA), которая позволяет множеству пользователей LAN (Локальная вычислительная сеть) одновременно получать доступ в Интернет по цене одного IP-адреса.

1.3.2 Межсетевой экран для надежного широкополосного доступа в Интернет

Prestige обеспечивает защиту от атаки Интернет-хакеров. По умолчанию, межсетевой экран блокирует весь входящий трафик из WAN. Межсетевой экран поддерживает контроль TCP/UDP, распознавание и предотвращение DoS (Отказ от обслуживания), а также извещения в реальном времени и журнальные регистрации.

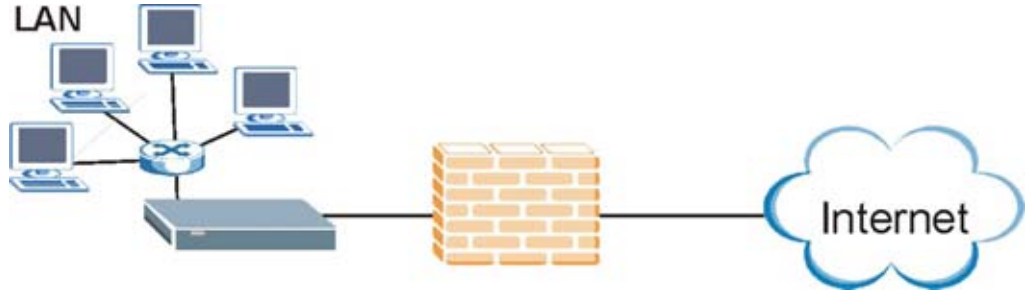


Рис. 1-2 Применение межсетевого экрана

1.3.3 Организация соединения локальных сетей

Prestige можно также использовать для соединения двух географически разделенных сетей с помощью линии ADSL. Типичный пример организации соединения локальных сетей приведен ниже.

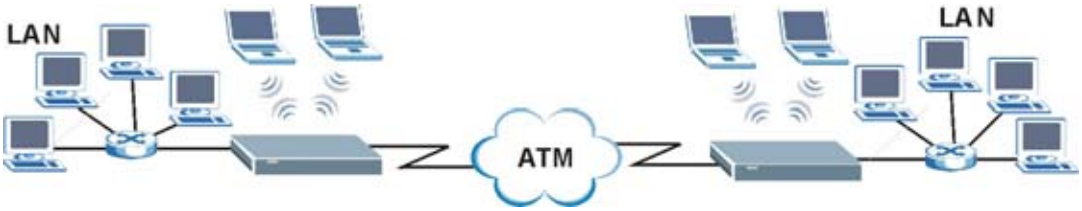


Рис. 1-3 Организация соединения локальных сетей Prestige

Раздел 2
Знакомство с Web-конфигуратором

В этой главе содержится информация о том, как получить доступ к Web-конфигуратору и как управлять им.

2.1 Знакомство с Web-конфигуратором

Встроенный Web-конфигуратор обеспечивает возможность дистанционного управления Prestige при помощи браузера Microsoft Internet Explorer или Netscape Navigator. Используйте Internet Explorer 6.0 (и выше) или Netscape Navigator 7.0 (и выше) с включенной поддержкой JavaScript. Рекомендуется установить разрешение экрана 1024 на 768 точек

2.2 Доступ к Web-конфигуратору системы Prestige

Step 1. Убедитесь, что аппаратное обеспечение Prestige подключено надлежащим образом (см. *Краткое руководство*).

Step 2. Подготовьте компьютер/компьютерную сеть для подключения к Prestige (см. *Краткое руководство*).

Step 3. Запустите Web-браузер.

Step 4. Наберите "192.168.1.1" как URL.

Step 5. Отобразится окно **Enter Network Password (Введите Сетевой Пароль)**. Введите имя пользователя (по умолчанию “admin”), пароль (по умолчанию “1234”) и щелкните **OK**.

Рис. 2-1 Окно ввода пароля

Step 6. Вы увидите меню **SITE MAP (Карта сайта)**.

Prestige автоматически отменит регистрацию и очистит экран после 5 минут неактивности. Если это произойдет, просто зарегистрируйтесь снова.

2.3 Перезапуск Prestige

Если Вы забыли пароль или не можете получить доступ к Web-конфигуратору, необходимо использовать кнопку **RESET (Перезапуск)** на задней панели Prestige для перезагрузки установленного по умолчанию файла конфигурации. Это означает, что все конфигурации, настроенные прежде, будут утрачены, а пароль будет установлен “1234”.

Comment [CTY1]: P334: т
обратной связи BETA

2.3.1 Использование кнопки перезапуска

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

Step 1. Удерживайте кнопку **RESET (ПЕРЕЗАПУСК)** в течении десяти секунд до тех пор, пока светодиод **SYS** или светодиод **PWR/SYS** не начнет мигать, а затем отпустите ее. Когда светодиод **SYS** или светодиод **PWR/SYS** начинает мигать, это означает, что настройки по умолчанию восстановлены и Prestige перезапускается.

2.4 Управление Web-конфигуратором системы Prestige

Следующие шаги описывают как управлять Web-конфигуратором из меню **SITE MAP (Карта сайта)**. В качестве примера в этом руководстве используются окна web Prestige 660HW-61. В разных моделях Prestige окна немного различаются.

- Щелкните **Wizard Setup (Мастер Установки),** чтобы начать конфигурирование Prestige в первый раз.
- Щелкните по ссылке под **Advanced Setup (Дополнительная настройка)** для конфигурирования дополнительных характеристик Prestige.
- Щелкните по ссылке под **Maintenance (Сопровождение)** для просмотра статистики производительности Prestige, загрузки встроенного программного обеспечения и резервного сохранения восстановления или загрузки файла конфигурации.
- Щелкните **Site Map (Карта сайта),** чтобы открыть окно **Site Map**.
- Щелкните **Logout (Конец сеанса)** на Панели навигации, при завершении сеанса управления Prestige.

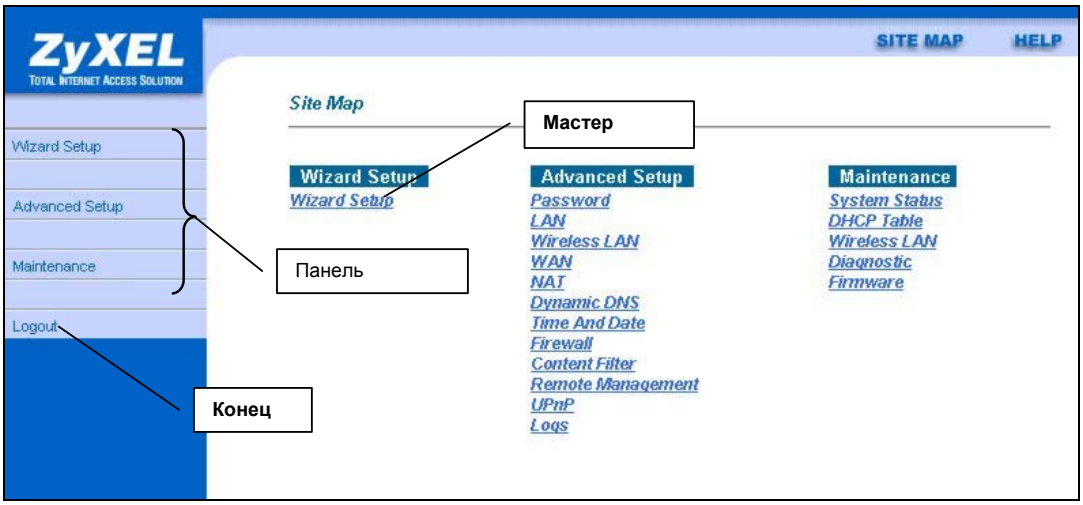


Рис. 2-2 Экран SITE MAP Web-конфигуратора

Щелкните по иконке HELP (размещенной в верхнем правом углу большинства экранов) для вызова встроенной справки.

Табл. 2-1 Сводка экранов Web-конфигуратора

LINK (ССЫЛКА)	SUB-LINK (ПОДМЕНЮ)	FUNCTION (ФУНКЦИЯ)
Wizard Setup (Мастер установки)		Используйте эти экраны для первоначального конфигурирования, настройки параметров Интернет-провайдера для доступа в Интернет и назначения IP-адресов WAN, сервера DNS и MAC.
Advanced Setup (Дополнительная настройка)		
Password (Пароль)		Используйте этот экран для смены пароля.
LAN (ЛВС)		Используйте этот экран для конфигурирования параметров DHCP LAN и TCP/IP.
WIRELESS LAN (Беспроводная ЛВС)	Wireless (Беспроводная)	Используйте этот экран для конфигурирования настроек беспроводной ЛВС.
	MAC Filter (MAC-фильтр)	Используйте этот экран для изменения в Prestige настроек MAC-фильтра .
	802.1X	Используйте этот экран для конфигурирования настроек аутентификации WLAN.
	Local User Database (Локальная база данных пользователя)	Используйте этот экран для конфигурирования локальной учетной записи(ей) пользователя в Prestige.
	RADIUS	Сконфигурируйте этот экран для использования внешнего сервера для беспроводной аутентификации.
WAN (ГВС)	WAN Setup (Настройка ГВС)	Используйте этот экран для изменения настроек удаленного узла ГВС.
	WAN Backup (Резервный доступ в ГВС)	Используйте этот экран для конфигурирования свойств переадресации трафика и настроек резервного доступа к ГВС.
NAT (Трансляция сетевых адресов)	SUA Only (Единственная учетная запись одиночного пользователя)	Используйте этот экран для конфигурирования серверов в Prestige.

Табл. 2-1 Сводка экранов Web-конфигуратора

LINK (ССЫЛКА)	SUB-LINK (ПОДМЕНЮ)	FUNCTION (ФУНКЦИЯ)
	Full Feature (Все функции)	Используйте этот экран для конфигурирования правил трансляции сетевых адресов.
Dynamic DNS (Динамический DNS)		Используйте этот экран для создания динамического DNS.
Time and Date (Время и дата)		Используйте этот экран для изменения в Prestige времени и даты.
Firewall (Межсетевой экран)	Default Policy (Стратегия по умолчанию)	Используйте этот экран для активации/деактивации межсетевого экрана и направления сетевого трафика для которого применяется правила.
	Rule Summary (Сводка правил)	Этот экран демонстрирует сводку правил межсетевого экрана и позволяет редактировать/добавлять правило.
	Anti Probing (Противозондирование)	Используйте этот экран для изменения настроек противозондирования.
	Threshold (Пороговое значение)	Используйте этот экран для конфигурирования допустимого предела для атаки типа DoS.
Content Filter (Контент-фильтр)	Keyword (Ключевое слово)	Используйте этот экран для блокирования сайтов, содержащих определенные ключевые слова в URL.
	Schedule (Планирование)	Используйте этот экран для установки дней и времени, когда Prestige будет производить контент-фильтрование.
	Trusted (Правомочный)	Используйте этот экран для исключения диапазона пользователей в ЛВС из контент-фильтрования Prestige.
Remote Management (Дистанционное управление)		Используйте этот экран для конфигурирования и установления с помощью какого интерфейса(ов) и с какого IP-адреса(ов) пользователи могут использовать Telnet/FTP/Web для управления Prestige.
UPnP		Используйте этот экран для включения в Prestige функции UPnP.
Logs (Журналы регистрации)	Log Settings (Настройки журнала регистрации)	Используйте этот экран для изменения настроек журнала регистрации Prestige.

Табл. 2-1 Сводка экранов Web-конфигуратора

LINK (ССЫЛКА)	SUB-LINK (ПОДМЕНЮ)	FUNCTION (ФУНКЦИЯ)
	View Log (Просмотр журнальной регистрации)	Используйте этот экран для просмотра журнальных регистраций для категорий, которые Вы выбрали .
Maintenance (Сопровождение)		
System Status (Статус системы)		Этот экран содержит административную и общесистемную информацию.
DHCP Table (Таблица DHCP)		Этот экран отображает информацию относительно DHCP (Dynamic Host Configuration Protocol/Протокол динамического конфигурирования хост-машины) и используется только для чтения.
WIRELESS LAN (Беспроводная LAN)	Association List (Список соединений)	Этот экран отображает MAC-адрес(а) базы данных настроек пользователей, которые в данный момент зарегистрированы в сети.
Diagnostic (Диагностика)	General (Основная)	Эти экраны отображают информацию, позволяющую идентифицировать проблемы, связанные основным подключением Prestige.
	DSL Line (Линия DSL)	Эти экраны отображают информацию, позволяющую идентифицировать проблемы, связанные с линией DSL.
Firmware (Встроенное программное обеспечение)		Используйте этот экран для загрузки встроенного программного обеспечения в Prestige
LOGOUT (Конец сеанса)		Щелкните по этому полю для выхода из Web-конфигуратора.

Раздел 3
Мастер Установки

В этой главе представлена информация об экранах Мастера Установки Web-конфигуратора.

3.1 Введение в Мастер Установки

Используйте экраны Мастера Установки для конфигурирования настроек системы для доступа в Интернет и заполните поля в таблице *Учетная Информация Для Сети Интернет Краткого Руководства*. Возможно Ваш Интернет-провайдер автоматически сконфигурирует некоторые поля в экранах Мастера Установки.

3.2 Инкапсуляция

Убедитесь, что используется метод инкапсуляции, предписанный Вашим Интернет-провайдером. Prestige поддерживает следующие методы.

3.2.1 ENET ENCAP

Протокол маршрутизации канального уровня с инкапсуляцией MAC (ENET ENCAP) реализуется только в сетевом протоколе IP. IP-пакеты маршрутизируются между интерфейсом Ethernet и интерфейсом WAN, а затем форматируются таким образом, что могут быть поняты в среде передачи. Напр., маршрутизированные кадры Ethernet инкапсулируются в передаваемые ячейки ATM. Для реализации ENET ENCAP необходимо задать IP-адрес шлюза в поле **ENET ENCAP Gateway** в экране Мастера Установки. Эту информацию можно получить у Интернет-провайдера.

3.2.2 PPP через Ethernet

PPPoE обеспечивает управление доступом и возможность составления счетов аналогично услугам по коммутируемой линии, использующим PPP. Prestige передает сеанс связи PPP через Ethernet (PPP over Ethernet, RFC 2516) с Вашего компьютера на постоянный виртуальный канал ATM (Permanent Virtual Circuit - PVC), соединенный с концентратором доступа ADSL , в котором сеанс связи PPP завершается. Один PVC может поддерживать любое количество сеансов связи PPP из LAN. Более подробно о PPPoE, см. *Приложения*.

3.2.3 PPPoA

PPPoA означает Протокол “точка-точка“ через уровень 5 адаптации ATM (AAL5). Функции подключения PPPoA аналогичны коммутируемому подключению к Интернету. Prestige инкапсулирует сеанс связи PPP на базе RFC1483 и передает его через постоянный виртуальный канал ATM (Permanent Virtual Circuit - PVC) Интернет-провайдеру на концентратор DSLAM. Более подробно о PPPoA см. в RFC 2364. Более подробно о PPP см. в RFC 1661.

3.2.4 RFC 1483

RFC 1483 описывает два метода многопротокольной инкапсуляции через уровень адаптации 5 ATM (AAL5). Первый метод позволяет мультиплексировать несколько протоколов через один виртуальный канал ATM (мультиплексирование на базе LLC), а второй метод 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 используется метод мультиплексирования, предписанный Вашим 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 множество протоколов, снабженных идентифицирующей информацией, которая содержится в заголовке каждого пакета. Несмотря на использование дополнительной пропускной способности 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

Убедитесь в правильности используемых номеров идентификатора виртуального пути (Virtual Path Identifier - VPI) и идентификатора виртуального канала (Virtual Channel Identifier - VCI), назначенных

Вам. Действительный диапазон для VPI - от 0 до 255, а для VCI - от 32 до 65535 (0 - 31 зарезервированы для локального управления трафиком ATM). Более подробно см. в Приложениях.

3.5 Конфигурирование Мастера Установки: Первый экран

В меню **SITE MAP** щелкните **Wizard Setup** для отображения первого экрана Мастера Установки.

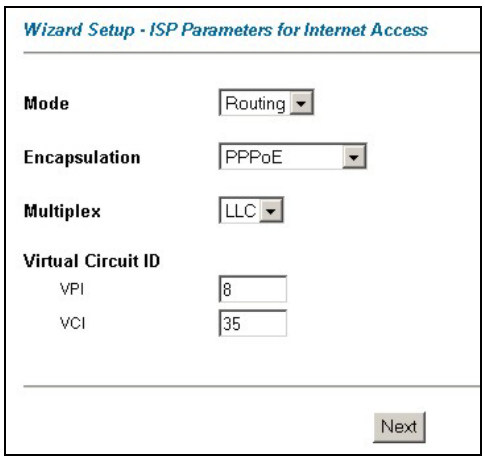


Рис. 3-1 Экран 1 Мастера Установки

В следующей таблице представлено описание полей данного экрана.

Табл. 3-1 Экран 1 Мастера Установки

ПОЛЕ	ОПИСАНИЕ
Mode (Режим)	Из выпадающего списка **Mode** выберите **Routing** (установлен по умолчанию), если Интернет-провайдер допускает использование нескольким компьютерам одинаковых учетных записей Интернет. В противном случае выберите **Bridge**.

Табл. 3-1 Экран 1 Мастера Установки

ПОЛЕ	ОПИСАНИЕ
Encapsulation (Инкапсуляция)	Из выпадающего списка **Encapsulation** выберите тип инкапсуляции, используемый Интернет-провайдером. Опции различаются в зависимости от того, что Вы выбираете в поле **Mode**. Если Вы выбираете **Bridge** в поле **Mode**, выберите **PPPoA** или **RFC 1483**. Если Вы выбираете **Routing** в поле **Mode**, выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
Multiplex (Мультиплексирование)	Из выпадающего списка **Multiplex** выберите метод мультиплексирования, используемый Интернет-провайдером на базе VC или на LLC.
Virtual Circuit ID (Идентификатор виртуального канала)	VPI (Идентификатор виртуального пути) и VCI (Идентификатор виртуального канала) определяют виртуальный канал. Более подробно см. в Приложении.
VPI (Идентификатор виртуального пути)	Введите назначенный идентификатор виртуального пути. Это поле может быть уже заполнено.
VCI (Идентификатор виртуального канала)	Введите назначенный идентификатор виртуального канала. Это поле может быть уже заполнено.
Next (Следующий)	Щелкните по этой кнопке для вызова следующего экрана Мастера Установки. Следующий экран Мастера Установки зависит от того, какой протокол Вы выбрали до этого. Щелкните по ссылке протокола для отображения следующего экрана Мастера Установки для этого протокола.

3.6 IP-адрес и маска подсети

Точно так же, как все дома, находящиеся на одной улице, имеют общее название улицы, все компьютеры в локальной сети имеют общий сетевой адрес.

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

Если Интернет-провайдер не предоставляет явным образом сетевой IP-адрес, то вероятнее всего Вы имеете учетную запись одиночного пользователя, и Интернет-провайдер назначает при установлении соединения динамический IP-адрес. Если это именно такой случай, рекомендуется выбирать сетевой номер от 192.168.0.0 до 192.168.255.0 и придется включить в Prestige функцию Трансляции Сетевых Адресов (NAT) . Агентство по назначению имен и уникальных параметров протоколов Интернет

(IANA) специально зарезервировало блок адресов для частного использования. Если не предписано иное, не следует использовать адреса за пределами этого диапазона. Если,'напр., выбрать в качестве сетевого адреса 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.

Однажды выбрав сетевой номер, выберите для Prestige и IP-адрес, который легко запоминается, напр., 192.168.1.1, но убедитесь, что никакое другое устройство в сети не использует тот же IP-адрес.

Маска подсети определяет сетевую часть IP-адреса. Prestige вычисляет маску подсети автоматически на основании введенного IP-адреса. Если не указано иное,'не следует изменять маску подсети, вычисленную Prestige.

3.7 Назначение IP-адреса

Статический IP-адрес - это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не фиксирован, Интернет-провайдер каждый раз назначает новый адрес. Функция "Учетная запись одиночного пользователя"может быть включена или отключена в зависимости от характера имеющегося IP-адреса (статический или динамический). Тем не менее, на выбор IP-адреса и шлюза ENET ENCAP влияет предписанный метод инкапсуляции.

3.7.1 Назначение IP-адреса с помощью инкапсуляции PPPoA или PPPoE

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

3.7.2 Назначение IP-адреса с помощью инкапсуляции RFC 1483

В этом случае *следует* 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 помощью инкапсуляции ENET ENCAP

В этом случае может назначаться как статический, так и динамический IP-адрес. Для статического IP-адреса необходимо заполнить все поля IP Address и ENET ENCAP Gateway в соответствии с указаниями Интернет-провайдера. Однако для динамического IP-адреса Prestige выступает в качестве клиента DHCP на порте WAN, поэтому поля IP Address и ENET ENCAP Gateway будут недоступны (N/A), так как они предписываются Prestige сервером DHCP.

3.7.4 IP-адреса для частных сетей

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

```
10.0.0.0      –  10.255.255.255

172.16.0.0    –  172.31.255.255

192.168.0.0   –  192.168.255.255
```

IP-адрес может быть получен от IANA, от Интернет-провайдера или может быть назначен частной сетью. Если Ваша организация относительно небольшая, и доступ в Интернет осуществляется через Интернет-провайдера, Интернет-провайдер может предоставить адреса 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; всегда следуйте приведенным выше указаниям. За дополнительной информацией по назначению адресов следует обращаться к RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

3.8 Полупостоянное соединение (PPP)

Полупостоянное соединение представляет собой коммутируемую линию, где соединение всегда поддерживается в активном состоянии независимо от требований трафика. Если Вы устанавливаете полупостоянное соединение, Prestige выполняет два действия. Первое заключается в том, что он отключает функцию времени простоя. Второе заключается в том, что Prestige пытается включить соединение при включении и каждый раз, когда соединение отключается. Полупостоянное соединение может быть очень дорогостоящим по очевидным причинам.

Не устанавливайте полупостоянное соединение, если телефонная компания не предлагает услугу единого тарифа (без повременного учета) или если Вам необходима постоянная связь, а стоимость не очень велика

3.9 Трансляция сетевых адресов

NAT (Network Address Translation/Трансляция сетевых адресов - NAT, RFC 1631) это преобразование IP-адреса хоста в пакете, напр., адрес источника исходящего пакета, используемого в одной сети, в другой IP-адрес, известный в другой сети.

3.10 Конфигурирование Мастера Установки: Второй экран

Второй экран Мастера Установки различается в зависимости от того, какой используется тип инкапсуляции. Все экраны представлены в режиме маршрутизации. Для продолжения заполните поля и щелкните **Next**.

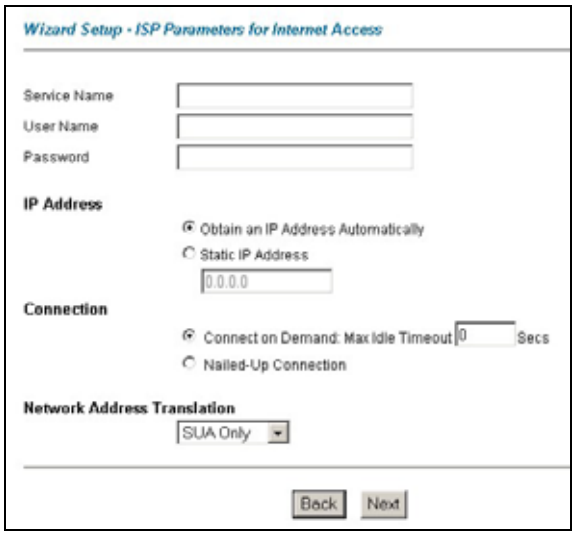


Рис. 3-2 Подключение к Интернету при помощи PPPoE

В следующей таблице представлено описание полей данного экрана.

Табл. 3-2 Подключение к Интернету при помощи PPPoE

ПОЛЕ	ОПИСАНИЕ

Табл. 3-2 Подключение к Интернету при помощи PPPoE

ПОЛЕ	ОПИСАНИЕ
Service Name (Сервисное имя)	Введите имя сервиса PPPoE.
User Name (Имя пользователя)	Введите имя пользователя в точности так как назначено Интернет-провайдером. Если имя назначено в виде user@domain, где домен идентифицирует сервисное имя, тогда введите оба компонента точно как представлено.
Password (Пароль)	Введите пароль соответствующий имени пользователя, представленному выше.
IP Address (IP-адрес)	Статический IP-адрес - это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не фиксирован; Интернет-провайдер каждый раз назначает новый адрес при подключении к Интернету. Учетная запись одиночного пользователя может быть включена или отключена в зависимости от типа имеющегося IP-адреса (статический или динамический). Выберите **Obtain an IP Address Automatically**, если имеется динамический IP-адрес, или выберите **Static IP Address** и введите назначенный Интернет-провайдером IP-адрес в текстовое поле **IP Address**.
Connection (Подключение)	Выберите **Connect on Demand**, если Вы не хотите подключаться все время и установите время простоя (в секундах) в поле **Max. Idle Timeout**. Установка по умолчанию выбирает **Connection on Demand** с 0 в качестве времени простоя, что означает, что сеанс связи с Интернетом не будет ограничиваться по времени. Выберите **Nailed-Up Connection**, если Вы хотите иметь подключение все время. Если соединение разъединится, Prestige автоматически попытается подключиться снова. Правило(а) планирования в меню 26 SMT имеет приоритет над настройками **Connection**.
Network Address Translation (Трансляция сетевых адресов)	Выберите **None**, **SUA Only** или **Full Feature** из выпадающего списка. Для дополнительной информации см. главу NAT.
Back (Назад)	Щелкните **Back** для возвращения к первому экрану Мастера Установки.

Табл. 3-2 Подключение к Интернету при помощи PPPoE

ПОЛЕ	ОПИСАНИЕ
Next (Следующий)	Щелкните **Next** для перехода к следующему экрану Мастера Установки.

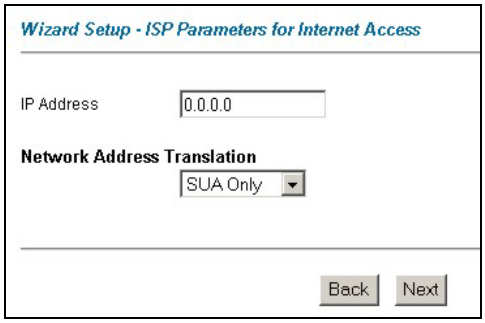


Рис. 3-3 Подключение к Интернету при помощи RFC 1483

В следующей таблице представлено описание полей данного экрана.

Табл. 3-3 Подключение к Интернету при помощи RFC 1483

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Это поле доступно, если Вы выберете **Routing** в поле **Mode**. Введите в это поле назначенный Интернет-провайдером IP-адрес.
Network Address Translation (Трансляция сетевых адресов)	Выберите **None**, **SUA Only** или **Full Feature** из выпадающего списка. Для дополнительной информации см. главу NAT.
Back (Назад)	Щелкните **Back** для возвращения к первому экрану Мастера Установки.
Next (Следующий)	Щелкните **Next** для перехода к следующему экрану Мастера Установки.

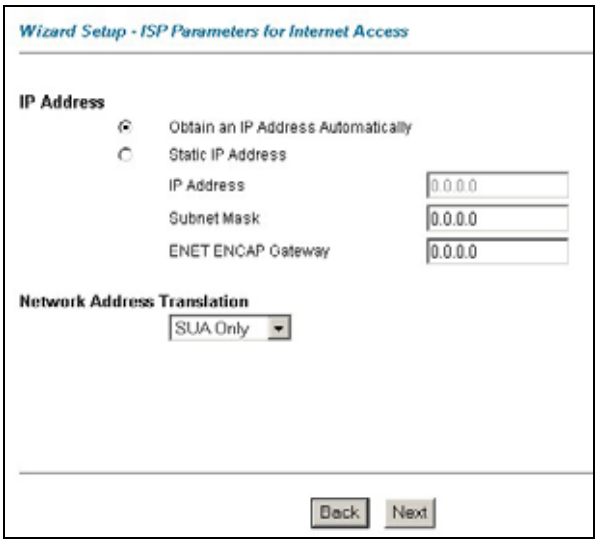


Рис. 3-4 Подключение к Интернету при помощи ENET ENCAP

В следующей таблице представлено описание полей данного экрана.

Табл. 3-4 Подключение к Интернету при помощи ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Статический IP-адрес - это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не фиксирован; Интернет-провайдер каждый раз назначает новый адрес при подключении к Интернету. Учетная запись одиночного пользователя может быть включена или отключена в зависимости от типа имеющегося IP-адреса (статический или динамический). Выберите **Obtain an IP Address Automatically**, если имеется динамический IP-адрес; или выберите **Static IP Address** и введите, назначенный Интернет-провайдером IP-адрес в текстовое поле **IP Address**.
Subnet Mask (Маска подсети)	Введите маску подсети в десятичном виде с разделительными точками. Для вычисления маски подсети см. Приложение *Организация подсетей* (если Вы их используете).

Табл. 3-4 Подключение к Интернету при помощи ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
ENET ENCAP Gateway (Шлюз ENET ENCAP)	Необходимо определить IP-адрес шлюза (предоставляется Интернет-провайдером), если используется **ENET ENCAP** в поле **Encapsulation** предыдущего экрана.
Network Address Translation (Трансляция сетевых адресов)	Выберите **None**, **SUA Only** или **Full Feature** из выпадающего списка. Для дополнительной информации см. главу NAT.
Back (Назад)	Щелкните **Back** для возвращения к первому экрану Мастера Установки.
Next (Следующий)	Щелкните **Next** для перехода к следующему экрану Мастера Установки.

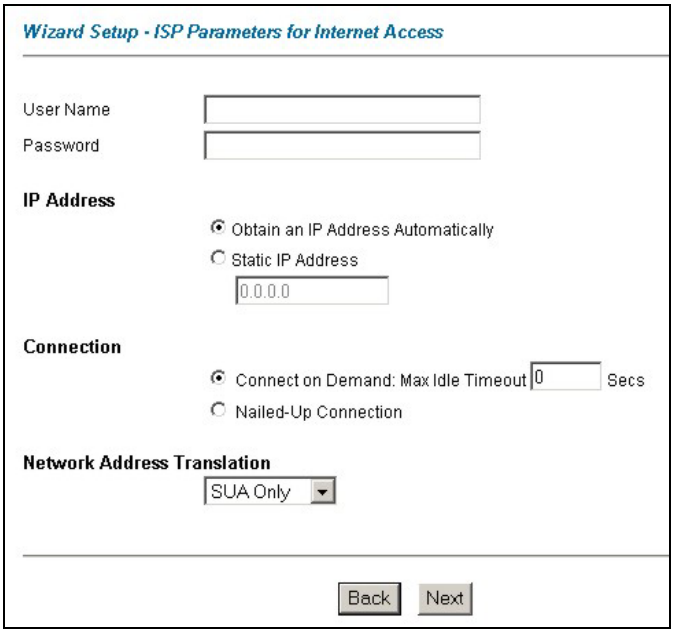


Рис. 3-5 Подключение к Интернету при помощи PPPoA

В следующей таблице представлено описание полей данного экрана.

Табл. 3-5 Подключение к Интернету при помощи PPPoA

ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите регистрационное имя, которое назначает Интернет-провайдер.
Password (Пароль)	Введите пароль соответствующий имени пользователя, представленному выше.
IP Address (IP-адрес)	Эта опция доступна, если Вы выбираете **Routing** в поле **Mode**. Статический IP-адрес - это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не фиксирован; Интернет-провайдер каждый раз назначает новый адрес при подключении к Интернету. Учетная запись одиночного пользователя может быть включена или отключена в зависимости от типа имеющегося IP-адреса (статический или динамический). Щелкните **Obtain an IP Address Automatically**, если имеется динамический IP-адрес, или щелкните **Static IP Address и** введите IP-адрес, назначенный Интернет-провайдером, в текстовое поле **IP Address**.
Connection (Подключение)	Выберите **Connect on Demand**, если Вы не хотите подключаться все время и установите время простоя (в секундах) в поле **Max. Idle Timeout**. Установка по умолчанию выбирает **Connection on Demand** с 0 в качестве времени простоя, что означает, что сеанс связи с Интернетом не будет ограничиваться по времени. Выберите **Nailed-Up Connection**, если Вы хотите иметь подключение все время. Если соединение разъединится Prestige автоматически попытается подключиться снова. Правило(а) планирования в меню 26 SMT имеет приоритет над настройками **Connection**.

Табл. 3-5 Подключение к Интернету при помощи PPPoA

ПОЛЕ	ОПИСАНИЕ
Network Address Translation (Трансляция сетевых адресов)	Эта опция доступна, если Вы выбираете **Routing** в поле **Mode**. Выберите **None**, **SUA Only** или **Full Feature** из выпадающего списка. Для дополнительной информации см. главу NAT.
Back (Назад)	Щелкните **Back** для возвращения к первому экрану Мастера Установки.
Next (Следующий)	Щелкните **Next** для перехода к следующему экрану Мастера Установки.

3.11 Настройка DHCP

DHCP (Протокол динамического конфигурирования хост-машины, RFC 2131 и RFC 2132) позволяет отдельным клиентам получать доступ к конфигурации TCP/IP при загрузки с сервера. Можно сконфигурировать Prestige в качестве сервера DHCP или отключить его. При конфигурировании в качестве сервера, Prestige обеспечивает установление конфигураций TCP/IP у своих клиентов. Если Вы отключаете сервер DHCP, то необходимо иметь в LAN другой сервер DHCP, в противном случае придется конфигурировать компьютеры вручную.

3.11.1 Настройка IP-пула

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

3.12 Конфигурирование Мастера Установки: Третий экран

Проверьте настройки экрана, как показано ниже. Для изменения параметров LAN в Prestige, щелкните **Change LAN Configurations**. Или щелкните **Save Settings** для сохранения конфигурации и перейдите к разделу 3.13.

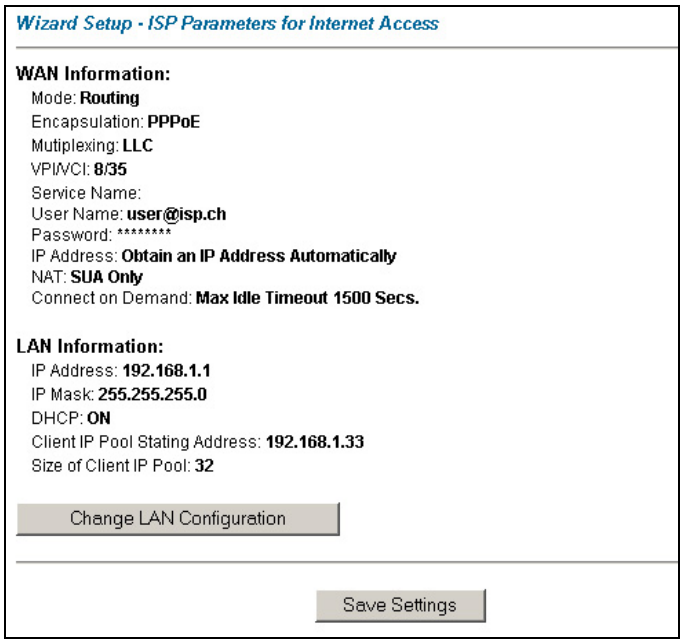


Рис. 3-6 Экран 3 Мастера Установки

Step 2. Если Вы хотите изменить настройки LAN в Prestige, щелкните **Change LAN Configuration** для отображения экрана показанного ниже.

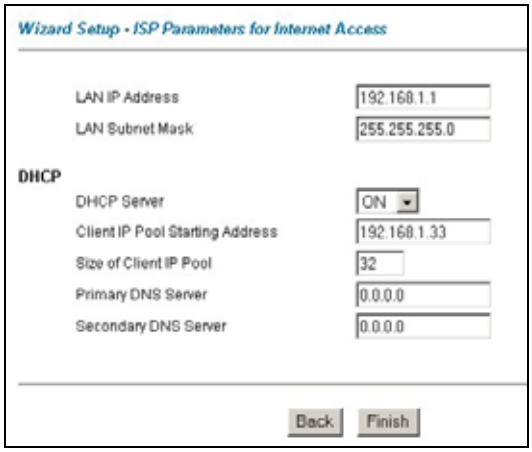


Рис. 3-7 Мастер Установки : Конфигурирование LAN

В следующей таблице представлено описание полей данного экрана.

Табл. 3-6 Мастер Установки : Конфигурирование LAN

ПОЛЕ	ОПИСАНИЕ
LAN IP Address (IP-адрес LAN)	Введите IP-адрес Prestige в десятичном виде с разделительными точками, напр., 192.168.1.1 (установленный изготовителем по умолчанию). **Если Вы изменили IP-адрес Prestige в LAN , дальше необходимо использовать новый IP-адрес, если Вы снова хотите получить доступ к Web-конфигуратору.**
LAN Subnet Mask (Маска подсети LAN)	Введите маску подсети в десятичном виде с разделительными точками.
DHCP (Dynamic Host Configuration Protocol/Протокол динамического выбора конфигурации хост-машины)	

Табл. 3-6 Мастер Установки : Конфигурирование LAN

ПОЛЕ	ОПИСАНИЕ
DHCP Server (Сервер DHCP)	Из выпадающего списка **DHCP Server** выберите **On** для назначения Prestige IP-адреса, шлюза IP по умолчанию и серверов DNS для системных компьютеров, поддерживающих клиента DHCP. Выберите **Off** для отключения сервера DHCP. Если сервер DHCP используется, сконфигурируйте следующие параметры:
Client IP Pool Starting Address (Начальный адрес клиентского IP-пула)	Это поле определяет первый из непрерывных адресов в пуле непрерывных IP-адресов.
Size of Client IP Pool (Размер клиентского IP-пула)	Это поле определяет размер пула или количество непрерывных IP-адресов в пуле.
Primary DNS Server (Основной сервер DNS)	Введите IP-адреса серверов DNS. Адреса серверов DNS пересылаются клиентам DHCP вместе с IP-адресом и маской подсети.
Secondary DNS Server (Дополнительный сервер DNS)	Как показано выше.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему экрану Мастера Установки.
Finish (Конец)	Щелкните **Finish** для сохранения настроек и перехода к следующему экрану Мастера Установки.

3.13 Конфигурирование Мастера Установки: Проверка соединения

Prestige автоматически проверяет подключение компьютера(ов) к портам LAN. Для проверки соединения Prestige с Интернет-провайдером щелкните **Start Diagnose**. Или щелкните **Return to Main Menu** для возвращения к экрану **Site Map**.

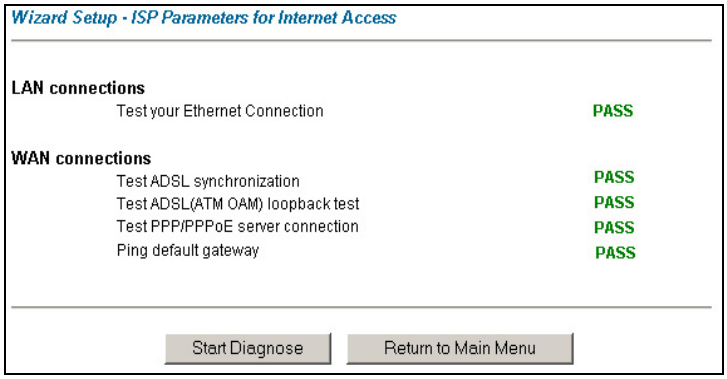


Рис. 3-8 Экран 4 Мастер Установки

3.14 Проверьте подключение к Интернету

Запустите web-браузер и наберите www.zyxel.com. Сразу начинается доступ в Интернет. Для более подробной информации о полном диапазоне характеристик Prestige см. оставшуюся часть *Руководства пользователя*. Если Вы не можете подключиться к Интернету откройте еще раз Web-конфигуратор, для проверки правильности настроек Интернета, сконфигурированных с помощью Мастера Установки.

Глава II:

Пароль, LAN, Беспроводная LAN и WAN

В этой части дается обзор настроек пароля, LAN (Локальная вычислительная сеть), беспроводной LAN и WAN.

Раздел 4
Настройка пароля

В этой части содержится обзор экрана Пароль.

4.1 Описание экрана Пароль

Настоятельно рекомендуется изменить пароль для доступа к Prestige.

4.2 Изменение Пароля

Для изменения пароля Prestige (рекомендуется) щелкните **Password (Пароль)**. Отобразится окно, указанное ниже.

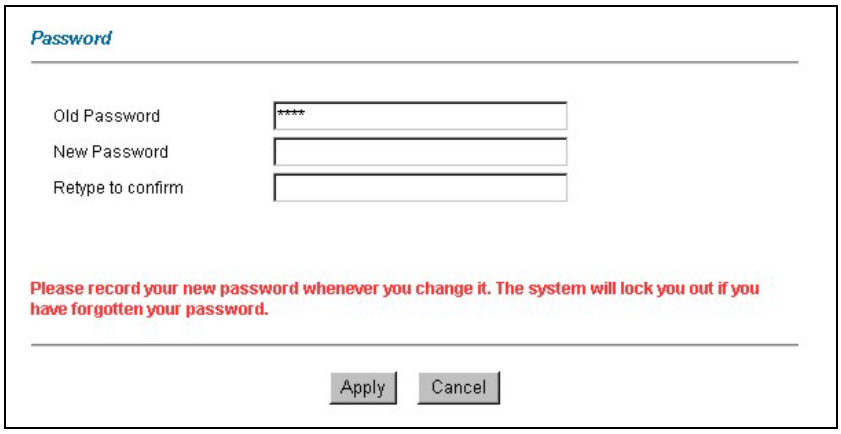


Рис. 4-1 Пароль

В следующей таблице представлено описание полей данного экрана.

Табл. 4-1 Пароль

ПОЛЕ	ОПИСАНИЕ

Табл. 4-1 Пароль

ПОЛЕ	ОПИСАНИЕ
Old Password (Старый пароль)	Введите в это поле пароль по умолчанию или существующий пароль, используемый для доступа в систему.
New Password (Новый пароль)	Введите в это поле новый пароль.
Retype to confirm (Подтверждение пароля)	Снова введите в это поле новый пароль для подтверждения.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

Раздел 5
Настройка LAN

В этой главе описывается конфигурирование настроек LAN.

5.1 Обзор LAN

Локальная вычислительная сеть (LAN) это общая система связи, к которой подключается много компьютеров. LAN представляет собой компьютерную сеть, ограниченную по площади и размещаемую обычно на территории одного здания или одного этажа. При помощи экранов LAN можно сконфигурировать сервер DHCP LAN и управлять IP-адресами.

5.1.1 LAN, WAN и Prestige

Фактическое физическое соединение определяет, являются ли порты Prestige портами LAN или WAN. Ниже приведен пример с двумя раздельными IP-сетями, - одной внутренней сетью LAN, а другой внешней сетью WAN:

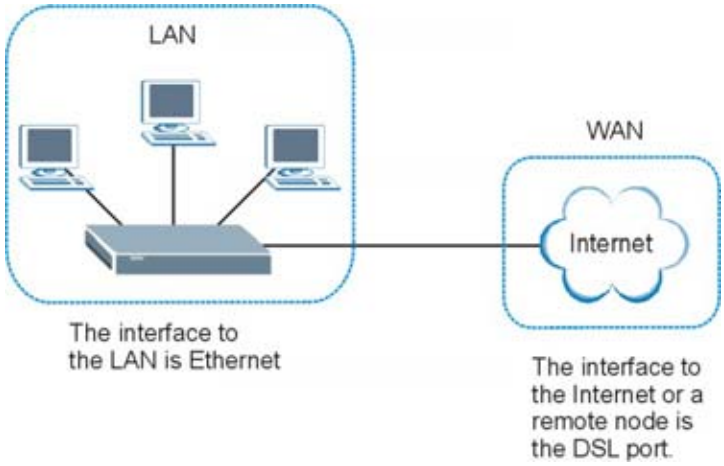


Рис. 5-1 IP-адреса LAN и WAN

5.2 Адрес сервера DNS

Сервер DNS (Domain Name System/Служба имен доменов) предназначен для отображения имени домена на соответствующий IP-адрес и наоборот. Сервер DNS играет крайне важную роль, так как без него нужно было бы точно знать IP-адрес каждой машины, к которой нужно получить доступ. Адреса сервера 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 серверов DNS, обычно в виде информационного листка при оформлении подписки. В этом случае следует ввести эти адреса в поля **DNS Server** в меню **LAN Setup**, в противном случае, оставить их незаполненными.

Некоторые Интернет-провайдеры предпочитают передавать адреса серверов DNS после подключения с помощью DNS-расширения протокола PPP IPCP (Протокол управления IP). Если Интернет-провайдер не предоставляет адрес серверов DNS в явной форме, значит, они передаются в процессе согласования IPCP. Prestige поддерживает DNS-расширение протокола IPCP через функцию прокси-сервера DNS.

Если поля **Primary** и **Secondary DNS Server** в меню **LAN Setup** не определены, напр., оставлено 0.0.0.0, Prestige сообщает клиентам DHCP, что он сам является сервером DNS. Когда компьютер посылает запрос DNS на Prestige, Prestige пересылает запрос на истинный сервер DNS, определенный с помощью IPCP и ретранслирует ответ назад компьютеру.

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

5.3 Назначение адреса сервера DNS

Используйте сервер DNS (Domain Name System/Служба имен доменов) для отображения имени домена на соответствующий IP-адрес и наоборот. Сервер DNS играет крайне важную роль, так как без него нужно было бы точно знать IP-адрес каждого компьютера, к которому нужно получить доступ.

Существует два способа распространения адресов серверов DNS Интернет-провайдером.

1. Интернет-провайдер сообщает адреса серверов DNS, обычно в виде информационного листка при оформлении подписки. Если Интернет-провайдер назначает адреса серверов DNS, введите их в поля DNS Server в меню DHCP Setup.

2. Prestige выступает в качестве прокси-сервера DNS, если поля **Primary** и **Secondary DNS Server** оставлены незаполненными в меню **LAN Setup**.

5.4 TCP/IP LAN

Prestige имеет функцию встроенного сервера DHCP, который может назначать IP-адреса и серверы DNS системе компьютеров поддерживающих клиента DHCP.

5.4.1 Заводские настройки LAN по умолчанию

В Prestige предварительно установлены следующие значения параметров LAN:

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

Данные параметры работоспособны в большинстве случаев. Если Интернет-провайдер предоставляет адрес(а) серверов DNS в явной форме, см. справку о встроенном Web-конфигураторе, где представлена информация о том какие поля необходимо заполнять.

5.4.2 IP-адрес и маска подсети

Для дополнительной информации см. раздел *IP-адрес и маска подсети* в главе **Мастер Установки**.

5.4.3 Настройка RIP

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

1. **Both -** Prestige осуществляет периодическую широковещательную рассылку своей маршрутной таблицы и полученных данных RIP.
2. **In Only -** Prestige не посылает пакеты RIP, но принимает все входящие пакеты RIP.
3. **Out Only -** Prestige посылает пакеты RIP, но не принимает входящие пакеты RIP.
4. **None -** Prestige не посылает пакеты RIP и игнорирует входящие пакеты RIP.

Поле **Version (Версия)** управляет форматом и методом широковещательной рассылки пакетов RIP, которые посылает Prestige (оба формата распознаются при получении). Формат **RIP-1** является общепринятым; но формат RIP-2 содержит больше информации. Для большинства сетей подходит RIP-1, если только сеть не имеет какой-либо специфической топологии.

Оба формата **RIP-2B** и **RIP-2M** осуществляют передачу данных маршрутизации в формате RIP-2; отличие заключается в том, что **RIP-2B** использует циркулярную рассылку для подсети, а **RIP-2M**-многоадресную рассылку.

5.4.4 Многоадресная рассылка

Как правило, пакеты IP передаются одним из двух способов - путем одноадресной (1 отправитель - 1 получатель) или циркуляционной рассылки (1 отправитель - все абоненты сети). Многоадресная рассылка представляет собой третий способ передачи пакетов IP группе хост-машин, подключенных к сети - но не всем и не только одной.

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 все еще широко используется. Для получения более подробной информации о возможности взаимодействия между версиями 2 и 1 IGMP, см. разделы 4 и 5 RFC 2236. IP-адрес класса D используется для идентификации групп хост-машин и может находиться в диапазоне 224.0.0.0 - 239.255.255.255. Адрес 224.0.0.0 не назначен 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 IP хост-машины (включая шлюзы). Для участия в IGMP все хост-машины должны принадлежать к группе 224.0.0.1. Адрес 224.0.0.2 назначается группе маршрутизаторов, участвующих в многоадресной рассылке.

Prestige поддерживает как версию 1 IGMP (**IGMP-v1**), так и версию 2 IGMP (**IGMP-v2**). При запуске Prestige запрашивает все сети, к которым он непосредственно подключен, с целью определения принадлежности к группе. В дальнейшем Prestige будет периодически обновлять эту информацию. В Prestige многоадресную рассылку IP можно включить/отключить на интерфейсах LAN и/или WAN с помощью Web-конфигуратора (**LAN**; **WAN**). Для отключения многоадресной рассылки IP на этих интерфейсах выберите **None**.

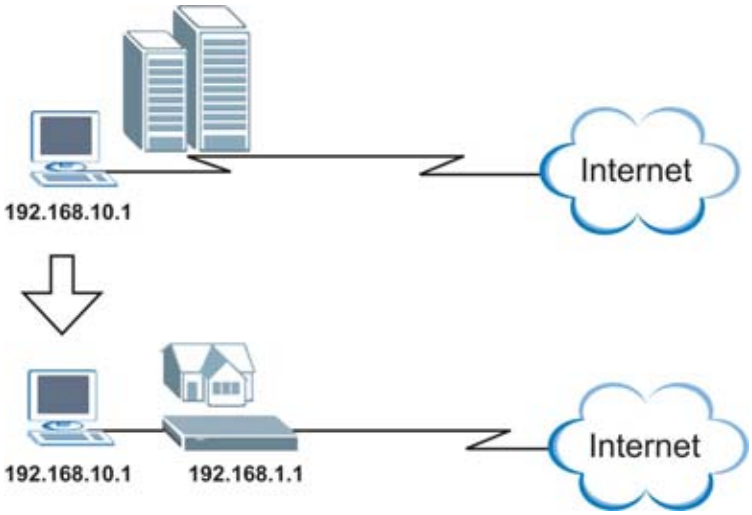
5.5 Any IP

Чтобы посредством Prestige обеспечить доступ компьютера к Интернету как правило, необходимо, чтобы IP-адреса и маски подсети компьютера и Prestige находились в одной и той же подсети. В случаях, когда компьютеру необходимо использовать статический IP-адрес в другой сети, может потребоваться конфигурировать сетевые настройки компьютера вручную, всякий раз, когда Вы хотите получить доступ в Интернет при помощи Prestige.

С функцией Any IP и включенным NAT, Prestige позволяет компьютеру получить доступ в Интернет без изменения настроек сети (таких как IP-адрес и маска подсети) компьютера, даже если IP-адреса компьютера и Prestige находятся в разных подсетях. Неважно, установлен ли компьютер для

использования динамического или статического (фиксированного) IP-адреса, можно просто подключить компьютер к Prestige и получить доступ в Интернет.

На следующем рисунке изображен сценарий, где компьютер установлен для использования статического частного IP-адреса в корпоративной среде. Если Prestige установлен для бытового использования, Вы можете продолжать использовать компьютер для доступа в Интернет без изменения настроек сети, даже если IP-адреса компьютера и Prestige находятся в разных подсетях.



Функция Any IP не применяется к компьютерам, использующим динамический или статический IP-адрес, находящийся в одной и той же подсети, что и IP-адрес Prestige.

Для использования в Prestige функции Any IP *необходимо* включить NAT/SUA .

5.5.1 Управление функцией Any IP

Протокол разрешения адресов (ARP) - это протокол, предназначенный для сопоставления адреса межсетевого протокола (IP-адрес) физическому адресу машины, также известному как MAC-адрес в локальной вычислительной сети. Таблица маршрутизации IP определяет для IP устройств Ethernet (Prestige) какой использовать транзитный пункт для пересылки данных вместе с их конкретным назначением.

Если компьютер при помощи Prestige подключается к Интернету в первый раз, предпринимаются следующие действия.

1. Если компьютер (находящийся в другой подсети) в первый раз пытается получить доступ к Интернету, он отправляет пакеты на свой шлюз по умолчанию (не являющийся шлюзом Prestige), получая MAC-адрес в своей таблице ARP.
2. Если компьютер не может определить шлюз по умолчанию, запрос ARP передается в LAN.
3. Prestige получает запрос ARP и отвечает компьютеру со своим собственным MAC-адресом.
4. Компьютер обновляет MAC-адрес для шлюза по умолчанию в таблице ARP. Обновив таблицу ARP, компьютер может подключаться к Интернету с помощью Prestige.
5. При получении Prestige пакетов от компьютера, он создает запись в таблице маршрутизации IP, поэтому он может правильно пересылать пакеты, предназначенные для компьютера.

После того, как вся информация о маршрутизации обновлена, компьютер может получить доступ к Prestige и к Интернету, так как будто он находится в той же подсети, что и Prestige.

5.6 Конфигурирование LAN

Щелкните **LAN** для отображения следующего экрана.

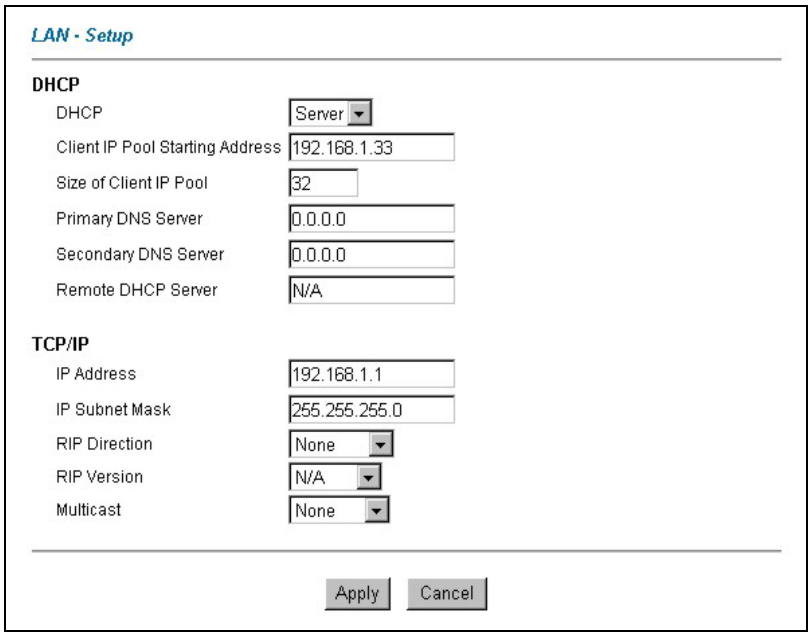


Рис. 5-2 LAN

В следующей таблице представлено описание полей данного экрана.

Табл. 5-1 LAN

ПОЛЕ	ОПИСАНИЕ
DHCP (Dynamic Host Configuration Protocol/Протокол динамического выбора конфигурации хост-машины)	
DHCP (Dynamic Host Configuration Protocol/Протокол динамического выбора конфигурации хост-машины)	Если в данном поле установлено **Server**, то Prestige 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**, то Prestige выступает в качестве фиктивного сервера DHCP и передает запросы и ответы DHCP между удаленным сервером и клиентами. В этом случае, в поле **Remote DHCP Server** следует ввести IP-адрес фактического удаленного сервера DHCP. Если используется DHCP, необходимо задать следующие параметры:
Client IP Pool Starting Address (Начальный адрес клиентского IP-пула)	В этом поле задается первый адрес из пула непрерывных IP-адресов.
Size of Client IP Pool (Размер клиентского IP-пула)	В этом поле задается размер или счетчик пула непрерывных IP-адресов.
Primary DNS Server (Основной сервер DNS)	Введите IP-адреса серверов DNS. Серверы DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Secondary DNS Server (Дополнительный сервер DNS)	Как показано выше.
Remote DHCP Server (Удаленный сервер DHCP)	Если в поле **DHCP** выбрано **Relay**, здесь следует ввести IP-адрес фактического удаленного сервера DHCP.

Табл. 5-1 LAN

ПОЛЕ	ОПИСАНИЕ
TCP/IP (Протокол управления передачей/Протокол Интернет)	
IP Address (IP-адрес)	Введите IP-адрес Prestige в десятичном виде с разделительными точками, напр., 192.168.1.1 (установленный изготовителем по умолчанию).
IP Subnet Mask (Маска подсети IP)	Введите назначенную Интернет-провайдером маску подсети (если предоставлена).
RIP Direction (Направление RIP)	Выберите направление RIP из **None**, **Both**, **In Only** и **Out Only**.
RIP Version (Версия RIP)	Выберите версию RIP из **RIP-1**, **RIP-2B** и **RIP-2M**.
Multicast (Многоадресная рассылка)	IGMP (Internet Group Multicast Protocol/Протокол многоадресной рассылки) - это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Prestige поддерживает как версию 1 IGMP (**IGMP-v1**), так и версию 2 **IGMP-v2**. Выберите **None** для ее отключения.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

Раздел 6
Настройка беспроводной LAN

В этой главе описывается конфигурирование в Prestige беспроводной LAN.

6.1 Описание беспроводной LAN

В данном разделе дается описание беспроводной LAN и некоторых основных конфигураций. Беспроводная LAN может быть настолько проста, как два компьютера с сетевой радиокартой, сообщающихся в одноранговой сети или так сложна, как множество компьютеров с сетевой радиокартой, сообщающихся через точки доступа, которые передают сетевой трафик в проводную LAN.

Экранные меню беспроводной LAN становятся доступны только при установленной сетевой радиокарте WLAN.

6.1.1 Дополнительные требования по установке для использования 802.1x

- Компьютер с сетевой радиокартой IEEE 802.11b/g и Web-браузером (с поддержкой JavaScript) и/или Telnet.
- Компьютер беспроводной станции должен управляться IEEE 802.1x-совместимым программным обеспечением. В настоящее время, это реализовано в Windows XP.
- Дополнительный сетевой сервер RADIUS для аутентификации и учета удаленного пользователя.

6.1.2 Канал

Канал представляет собой радиочастоту(ты), используемую беспроводными устройствами IEEE 802.11b/g. Доступность каналов зависит от географического положения. У Вас может быть набор каналов (для Вашего региона), поэтому для уменьшения помех следует использовать другие каналы, нежели в смежной точке доступа (AP). Помехи имеют место, если радио сигналы от различных точек доступа перекрывают друг друга, вызывая интерференцию и снижение пропускной способности канала.

Однако, смежные каналы частично перекрываются. Во избежании помех из-за перекрывания, канал точки доступа (AP) должен отстоять по крайней мере на пять каналов от частот, которые используют

смежные точки доступа. Напр., если Ваш регион имеет 11 каналов и смежная точка доступа использует канал 1, то Вам необходимо выбрать канал 6 или 11.

6.1.3 Идентификатор ESS

Расширенный набор служб (ESS) - это группа точек доступа или беспроводных шлюзов, подключенных к проводной LAN в одной и той же подсети. Идентификатор ESS однозначно идентифицирует каждый набор. Все точки доступа или беспроводные шлюзы и связанные с ними беспроводные станции в одной сети должны иметь одинаковый идентификатор ESS.

6.1.4 RTS/CTS

Случай “невидимого“ узла имеет место, когда две станции находятся в рабочей зоне одной точки доступа, но вне рабочих зон друг друга. Следующий рисунок иллюстрирует ситуацию “невидимого“ узла. Обе станции (STA) находятся в рабочей зоне точки доступа (AP) или беспроводного шлюза, но вне рабочих зон друг друга, поэтому они не могут “слышать” друг друга, т.е. они не знают используется ли в данный момент канал. Поэтому, они считаются невидимыми друг для друга.

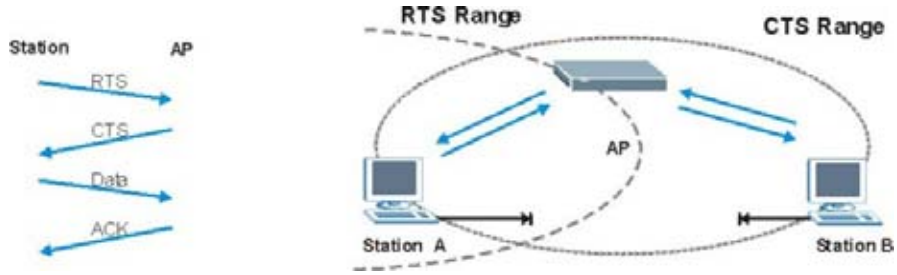


Рис. 6-1 RTS/CTS

Если станция A посылает данные в Prestige, она может не знать, что станция B уже использует канал. Если эти две станции послали данные одновременно, может произойти конфликт, когда обе партии данных достигают AP одновременно, результатом чего является потеря сообщений от обеих станций.

RTS/CTS предназначен для предотвращения конфликтов из-за невидимых узлов. **RTS/CTS** определяет самый большой размер кадра данных, который можно послать активировав разрешение на сеанс связи RTS (Request To Send/Запрос на передачу)/CTS (Clear to Send/Готовность к приему).

Если кадр данных превышает значение **RTS/CTS,** установленное в диапазоне от 0 до 2432 байт, станция, которая хочет передать этот кадр, должна вначале послать сообщение RTS (Request To Send/Запрос на передачу) на AP для получения разрешения на пересылку. Затем AP отвечает

сообщением CTS (Clear to Send/Готовность к приему) всем другим станциям в этой рабочей зоне диапазоне, чтобы известить их о необходимости задержки передачи данных. Это сообщение одновременно подтверждает запросившей станции время на передачу кадра данных.

Кадры, меньше указанных в **RTS/CTS**, станции могут посылать в AP непосредственно, без запроса разрешения на сеанс связи.

Если существует возможность “невидимых“ узлов в сети, необходимо сконфигурировать только **RTS/CTS** и “стоимость” повторной отправки больших фрагментов большей, чем дополнительные сетевые издержки, вызванные запросом разрешения на сеанс связи RTS/CTS.

Если значение **RTS/CTS** больше, чем значение **Порога фрагментации** (см. далее), тогда запрос разрешения на сеанс связи RTS/CTS не будет происходить, так как кадры данных будут отфрагментированы до того как они достигнут размера **RTS/CTS**.

Включение порога RTS устраняет сбои, но вызывает дополнительные сетевые издержки, которые могут негативно сказаться на пропускной способности сети.

6.1.5 Порог фрагментации

Порог фрагментации - это максимальный размер фрагмента данных (в диапазоне от 256 до 2432 байт), который может быть послан в беспроводную сеть и при превышении которого Prestige разделит пакет на меньшие кадры данных.

Большой **Порог фрагментации** рекомендуется для сетей, не склонных к помехам, тогда как для загруженных сетей или сетей склонных к помехам, необходимо установить меньший порог.

Если значение **Порога фрагментации** меньше, чем значение **RTS/CTS** (см. ранее), которое Вы установили, тогда запрос разрешения на сеанс связи RTS (Request To Send)/CTS (Clear to Send) никогда не будет происходить, так как кадры данных будут отфрагментированы до того как они достигнут размера **RTS/CTS**.

6.2 Уровни защиты

Безопасность беспроводной связи является существенной для сети, так как обеспечивает защиту связи между беспроводными станциями, точками доступа и проводной сетью.

Рисунок, представленный ниже, демонстрирует возможности уровней защиты беспроводной связи в Prestige. EAP (Extensible Authentication Protocol/Расширенный протокол аутентификации) используется для аутентификации и осуществления обмена динамическими ключами WEP. Он требует взаимодействия с сервером RADIUS (Remote Authentication Dial-In User Service/Услуга Удаленной аутентификации коммутируемого пользователя) в WAN или в LAN для обеспечения услуги аутентификации беспроводных станций.

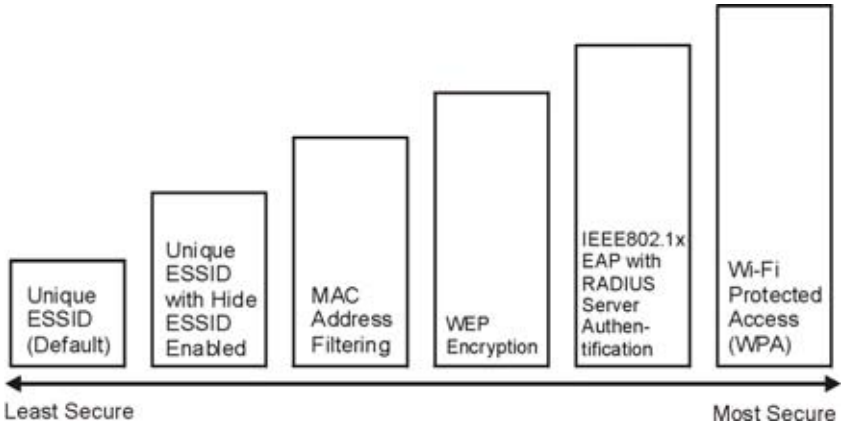


Рис. 6-2 Уровни беспроводной защиты Prestige

Если Вы не включаете никакую беспроводную защиту в Prestige, то сеть доступна для любых беспроводных сетевых устройств, находящихся в этой рабочей зоне.

Чтобы сконфигурировать и создать настройки безопасности беспроводной LAN, используйте Web-конфигуратор системы Prestige. Для подробной информации о доступе к Web-конфигуратору см. главу об использовании Web-конфигуратора системы.

6.3 Кодирование данных с использованием WEP

WEP-кодирование шифрует передачу данных между беспроводными станциями и точками доступа для предотвращения несанкционированного доступа. Оно кодирует передачи одноадресной и многоадресной рассылки в сети. Беспроводные станции и точки доступа должны использовать одинаковые ключи WEP для шифрования и дешифрования данных.

Prestige позволяет сконфигурировать до четырех 64-битных, 128-битных или 256-битных ключей WEP, но одновременно может быть включен только один ключ.

Чтобы сконфигурировать и включить WEP-кодирование; щелкните **Wireless LAN** и **Wireless** для отображения экрана **Wireless**.

6.4 Конфигурирование беспроводной LAN

Если Вы конфигурируете Prestige с компьютера, подключенного к беспроводной LAN и измените настройки ESSID или WEP Prestige, Вы потеряете Ваше беспроводное соединение, если нажмете клавишу Apply для

подтверждения. В этом случае необходимо изменить беспроводные настройки компьютера для соответствия новым настройкам Prestige.

Щелкните **Wireless LAN**, **Wireless** для отображения экрана **Wireless**.

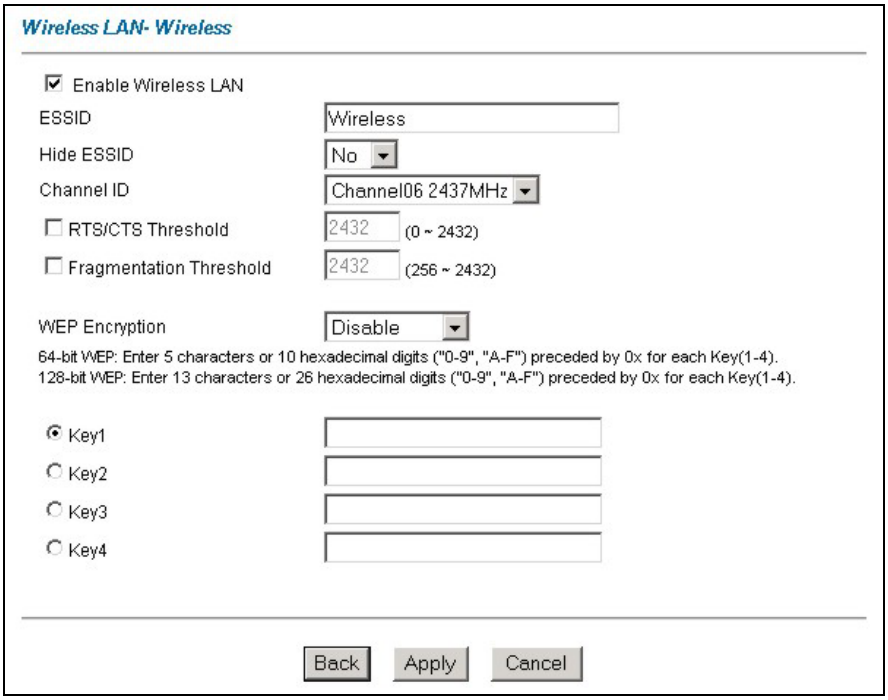


Рис. 6-3 Беспроводная LAN

В следующей таблице представлено описание полей данного экрана.

Табл. 6-1 Беспроводная LAN

ПОЛЕ	ОПИСАНИЕ

Табл. 6-1 Беспроводная LAN

ПОЛЕ	ОПИСАНИЕ
Enable Wireless LAN (Включение беспроводной LAN)	Беспроводная LAN по умолчанию выключена, поэтому перед включением беспроводной LAN необходимо сконфигурировать защиту настройкой MAC-фильтров и/или безопасность 802.1x; в противном случае беспроводная LAN будет уязвима при ее включении. Для включения беспроводной LAN поставьте галочку в этом поле.
ESSID	ESSID (Extended Service Set Identification/Расширенный набор служб идентификации) - это уникальное имя для идентификации Prestige в беспроводной LAN. Беспроводная станция, связанная с Prestige должна иметь тот же ESSID. Введите идентифицирующее имя (до 32 символов).
Hide ESSID (Скрытый ESSID)	Выберите **Yes** для скрытия ESSID, чтобы какая-либо станция не могла получить ESSID при помощи пассивного сканирования. Выберите **No**, чтобы сделать ESSID видимой для того, чтобы станция могла получить ESSID при помощи пассивного сканирования.
Channel ID (Идентификатор канала)	Радиочастота, используемая беспроводными устройствами IEEE 802.11b, называется каналом. Выберите канал из выпадающего списка.
RTS/CTS Threshold (Порог RTS/CTS)	Порог RTS (Request To Send/Запрос на передачу) (количество байт) предназначен для включения квитирования RTS/CTS. Данные с размером кадра больше, чем данное значение обеспечат квитирование RTS/CTS. Настройка этой характеристики больше, чем максимальный размер MSDU (MAC service data unit), приведет к отключению квитирования RTS/CTS. Настройка этой характеристики близкой к нулю приведет к включению квитирования RTS/CTS. Введите значение от 0 до 2432.
Fragmentation Threshold (Порог фрагментации)	Порог (количество байт) фрагментации предназначен для прямых сообщений. Это максимальный размер фрагмента данных, который можно послать. Введите значение от 256 до 2432.

Табл. 6-1 Беспроводная LAN

ПОЛЕ	ОПИСАНИЕ
WEP Encryption (WEP-кодирование)	WEP-кодирование (Wired Equivalent Privacy/Конфиденциальность, равная Конфиденциальности в проводных сетях) кадров данных перед передачей через беспроводную сеть. Выберите **Disable** для того, чтобы все беспроводные компьютеры поддерживали связь с точками доступа без шифрования данных. Выберите **64-bit WEP**, **128-bit WEP** или **256-bit WEP** для использования шифрования данных.
Key 1 to Key 4 (Ключи)	Ключи WEP используются для кодирования данных. Как Prestige, так и беспроводные станции должны использовать одинаковые ключи WEP для передачи данных. Если Вы выбираете **64-bit WEP**, тогда следует ввести любые 5 символов ASCII или 10 шестнадцатеричных символов ("0-9", "A-F"). Если Вы выбираете **128-bit WEP**, тогда следует ввести 13 символов ASCII или 26 шестнадцатеричных символов ("0-9", "A-F"). Если Вы выбираете **256-bit WEP**, тогда следует ввести 29 символов ASCII или 58 шестнадцатеричных символов ("0-9", "A-F"). Необходимо сконфигурировать все четыре ключа, но одновременно может быть активирован только один ключ. Ключом по умолчанию является ключ 1.
Back (Назад)	Щелкните **Back** для возвращения к экрану основного Меню настройки беспроводной LAN.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

6.5 Конфигурирование MAC-фильтра

Экран MAC-фильтра позволяет сконфигурировать Prestige для получения монопольного доступа вплоть до 32 устройств (Ассоциация доступа) или оградить до 32 устройств от доступа к Prestige (Ассоциация отказа). Каждое устройство Ethernet имеет уникальный MAC (Media Access Control/Управление доступом к среде) адрес. MAC-адрес назначается на заводе и состоит из шести пар шестнадцатеричных символов, напр., 00:A0:C5:00:00:02. Для конфигурирования этого экрана необходимо знать MAC-адрес устройства.

Для изменения настроек MAC-фильтра Prestige щелкните **Wireless LAN**, **MAC Filter** для отображения экрана **MAC Filter**. Отобразится окно, указанное ниже.

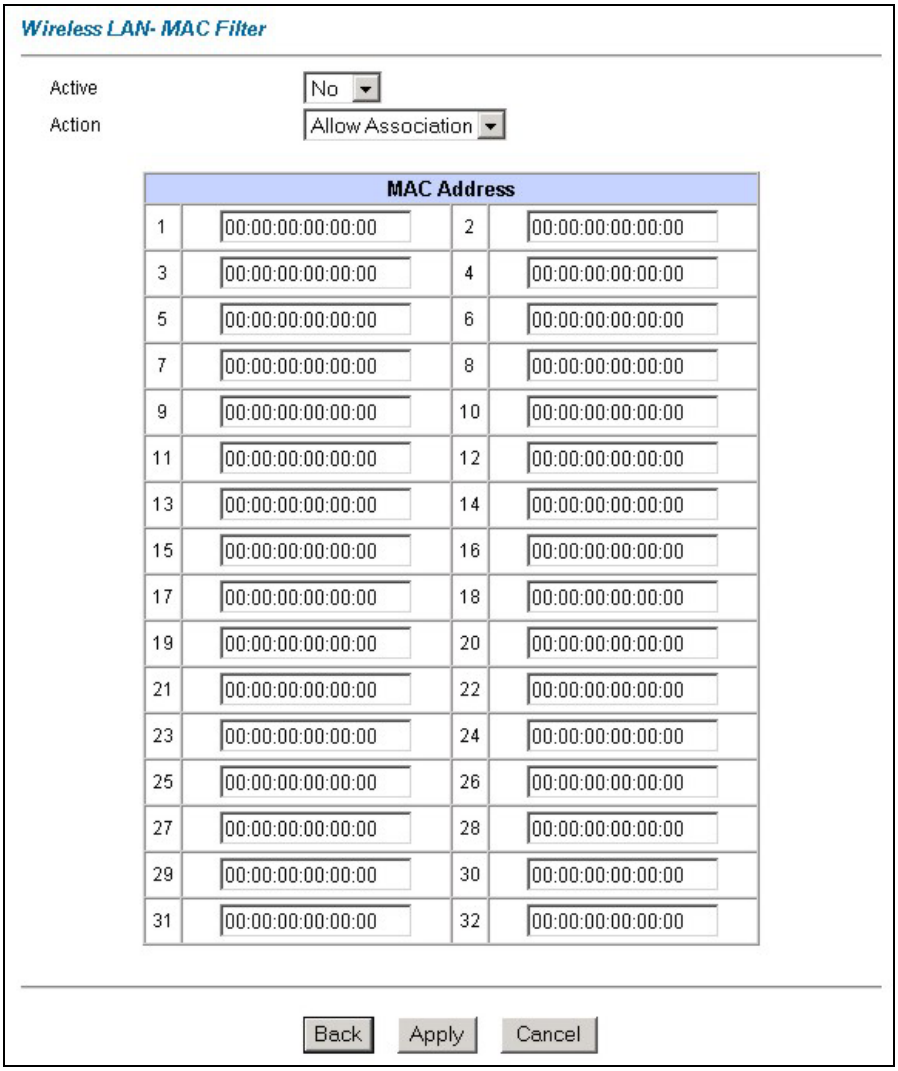


Рис. 6-4 MAC-адрес фильтра

В следующей таблице представлено описание полей данного меню.

Табл. 6-2 MAC-адрес фильтра

ПОЛЕ	ОПИСАНИЕ
Active (Активно)	Выберите **Yes** из выпадающего списка для включения фильтрации MAC-адреса
Action (Действие)	Определите действие фильтра из списка MAC-адресов в таблице **MAC Address**. Выберите **Deny Association**, чтобы блокировать доступ к маршрутизатору. MAC-адресам, не указанным в списке, будет разрешен доступ к маршрутизатору. Выберите **Allow Association**, чтобы разрешить доступ к маршрутизатору. MAC-адресам, не указанным в списке, будет отказано в доступе к маршрутизатору.
MAC Address (MAC-адрес)	Введите в эти поля MAC-адреса (в формате XX:XX:XX:XX:XX:XX) беспроводных станций, которым разрешается или отказывается в доступе к Prestige.
Back (Назад)	Щелкните **Back** для возвращения к экрану основного Меню настройки беспроводной LAN.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

6.6 Сетевая аутентификация

Вы можете активировать Prestige и сеть на выполнение аутентификации беспроводной станции, до того как станция подключится к Prestige и к проводной сети, к которой подключен Prestige.

6.6.1 EAP

EAP - это протокол аутентификации, первоначально разработанный для передачи кадров PPP (Point-to-Point Protocol/Протокол “точка-точка“), поддерживающий многочисленные типы аутентификации пользователей. Используя EAP для взаимодействия с EAP-совместимым сервером RADIUS,точка доступа помогает беспроводной станции и серверу RADIUS произвести аутентификацию.

6.6.2 RADIUS

RADIUS (Служба аутентификации удаленных пользователей по коммутируемым каналам связи) - это модель на базе клиент-сервер, которая поддерживает аутентификацию, авторизацию и учет. Точка доступа - это клиент и сервер в сервере RADIUS. Сервер RADIUS выполняет следующие задачи:

- **Аутентификация**

  Устанавливает подлинность пользователей.

- **Авторизация**

  Определяет сетевые службы, доступные для аутентифицированных пользователей, после того как они подключились к сети.

- **Учет**

  Отслеживает активность сетевых клиентов.

RADIUS использует простой обмен пакетами, в котором Prestige выступает в качестве передатчика сообщений между беспроводной станцией и сетевым сервером RADIUS.

Типы сообщений RADIUS

Следующие типы сообщений RADIUS пересылаются между точкой доступа и сервером RADIUS в целях аутентификации пользователей:

- **Access-Request (Доступ-Запрос)**

  Посылается точкой доступа при запросе аутентификации.

- **Access-Reject (Доступ-Отказ)**

  Посылается сервером RADIUS при отказе в доступе.

- **Access-Accept (Доступ-Прием)**

  Посылается сервером RADIUS при разрешении доступа.

- **Access-Challenge (Доступ-Вызов)**

  Посылается сервером RADIUS при запросе дополнительной информации для получения доступа. Точка доступа посылает надлежащий ответ от пользователя, а затем посылает еще одно сообщение Access-Request.

Следующие типы сообщений RADIUS пересылаются между точкой доступа и сервером RADIUS в целях учета пользователей:

- **Accounting-Request (Учет-Запрос)**

  Посылается точкой доступа при запросе учета.

- **Accounting-Response (Учет-Ответ)**

  Посылается сервером RADIUS и указывает, что учет начался или закончился.

Для обеспечения сетевой безопасности, точка доступа и сервер RADIUS используют коллективный секретный ключ, который является паролем, известным им обоим. Ключ не пересылается через сеть. Помимо секретного ключа, обмен информацией о пароле также кодируется для защиты сети от неправомочного доступа.

6.6.3 Обзор аутентификации EAP

EAP (Extensible Authentication Protocol/Расширенный протокол аутентификации) - это протокол аутентификации, представляющий собой верхний уровень транспортного механизма IEEE802.1x для поддержки многочисленных типов аутентификации пользователей. Используя EAP для взаимодействия с EAP-совместимым сервером RADIUS, точка доступа помогает беспроводной станции и серверу RADIUS произвести аутентификацию.

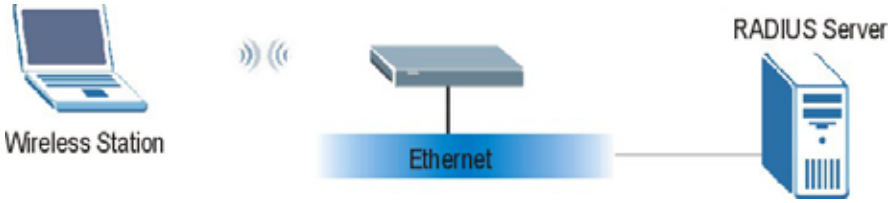


Рис. 6-5 Аутентификация EAP

Ниже представлено общее описание функционирования аутентификации EAP IEEE 802.1x. Примерный список этапов аутентификации EAP-MD5, см. в приложении о IEEE 802.1x.

Беспроводная станция посылает “начальное” сообщение в Prestige.

Step 3. Prestige посылает сообщение “запрос на подлинность” беспроводной станции для идентификации информации.

Step 4. Беспроводная станция посылает ответ о подлинности информации, включая имя пользователя и пароль.

Step 5. Сервер RADIUS проверяет данные пользователя в своей базе данных настроек пользователей и определяет, прошла или нет аутентификация беспроводной станции.

6.7 Введение в WPA

Защищенный доступ Wi-Fi (WPA) является разновидностью проекта спецификации безопасности IEEE 802.11i. Основные различия между WPA и WEP заключаются в аутентификации пользователя и усовершенствовании шифрования данных.

6.7.1 Аутентификация пользователя

WPA применяет IEEE 802.1x и Расширенный протокол аутентификации (EAP) для аутентификации беспроводных клиентов, использующих базу данных внешнего сервера RADIUS. Вы не можете использовать Локальную Базу Данных Пользователей Prestige в целях аутентификации WPA, так как Локальная База Данных Пользователей применяет EAP-MD5, которая не может использоваться для создания ключей. Для дополнительной информации относительно IEEE 802.1x, RADIUS и EAP см. далее в этой главе и приложениях.

Поэтому, если нет внешнего сервера RADIUS, следует использовать WPA-PSK (WPA -Pre-Shared Key/Предварительно согласованный ключ), для которого требуется ввести только единичный (идентичный) пароль для каждой точки доступа, беспроводного шлюза и беспроводного клиента. Если пароль совпадает, клиенту будет предоставлен доступ во WLAN.

6.7.2 Шифрование

WPA улучшает шифрование данных при использовании Протокола Целостности Временного Ключа (Temporal Key Integrity Protocol) (TKIP), Проверки Целостности Сообщений (Message Integrity Check) (MIC) и IEEE 802.1x.

Протокол Целостности Временного Ключа (TKIP) использует 128-битные ключи, которые динамически создаются и распределяются сервером аутентификации. Он включает функцию попакетного смешивания ключей, Проверку Целостности Сообщения (MIC), именуемую Michael, вектор расширенной инициализации (IV) с правилами упорядочивания, механизм повторного кодирования.

TKIP регулярно изменяет и чередует ключи шифрования для того, чтобы одни и те же ключи шифрования никогда не использовались дважды. Сервер RADIUS распределяет ключ Pairwise Master Key (Парный старший ключ) (PMK) на AP, которая затем устанавливает ключевую иерархию и систему управления с использованием парного ключа для динамического образования уникальных ключей шифрования данных, чтобы зашифровать все пакеты данных, беспроводно передаваемые между AP и беспроводными клиентами. Все это происходит автоматически в фоновом режиме.

Проверка Целостности Сообщений (MIC) предназначена для предотвращения перехвата пакетов данных злоумышленниками, их изменения и повторной отправки. MIC задает строгую

математическую функцию, по которой получатель и передатчик вычисляют, а затем сравнивают MIC. Если они не соответствуют, считается, что данные испорчены умышленно и пакет сбрасывается .

Создавая уникальные ключи шифрования данных для пакетов данных и механизм проверки целостности (MIC), TKIP создает намного больше сложностей для дешифровки данных в сети Wi-Fi, чем WEP, затрудняя для злоумышленника взлом сети.

Механизм шифрования, используемый для WPA и WPA-PSK тот же самый. Единственное отличие между ними состоит в том, что WPA-PSK использует простой общий пароль, вместо особых мандатов пользователей. Метод общего пароля делает WPA-PSK восприимчивым к грубым попыткам угадать пароль, но он все еще имеет больше преимуществ по сравнению с WEP, поскольку использует удобный в применении, совместимый, единичный, буквенно-цифровой пароль.

6.8 Пример использования WPA-PSK

Применение WPA-PSK выглядит следующим образом.

Step 6. Вначале введите идентичные пароли для AP и всех беспроводных клиентов. Предварительно согласованный ключ (PSK) должен состоять из 8- 63 символов ASCII (включая пробелы и знаки).

Step 7. AP проверяет пароль каждого клиента и только после проверки соответствия паролей подключает к сети.

Step 8. AP устанавливает и распределяет ключи для беспроводных клиентов.

Step 9. AP и беспроводные клиенты используют процесс кодирования TKIP для кодирования данных, передаваемых между ними.

Рис. 6-6 Аутентификация WPA - PSK

6.9 Пример использования WPA с RADIUS

Требуется IP-адрес сервера RADIUS, номер его порта (по умолчанию - 1812) и согласованный секретный ключ RADIUS. Пример использования WPA с внешним сервером RADIUS выглядит следующим образом. “A” - это сервер RADIUS. “DS” - это система распределения.

AP пересылает запрос на аутентификацию беспроводного клиента на сервер RADIUS.

Сервер RADIUS проводит идентификацию пользователя по своей базе данных и соответственно предоставляет или запрещает доступ в сеть.

Сервер RADIUS распределяет ключ Pairwise Master Key (Парный старший ключ) (PMK) на AP, затем устанавливает ключевую иерархию и систему управления с использованием парного ключа для динамического образования уникальных ключей шифрования данных, чтобы зашифровать все пакеты данных, которые беспроводно передаются между AP и беспроводными клиентами.

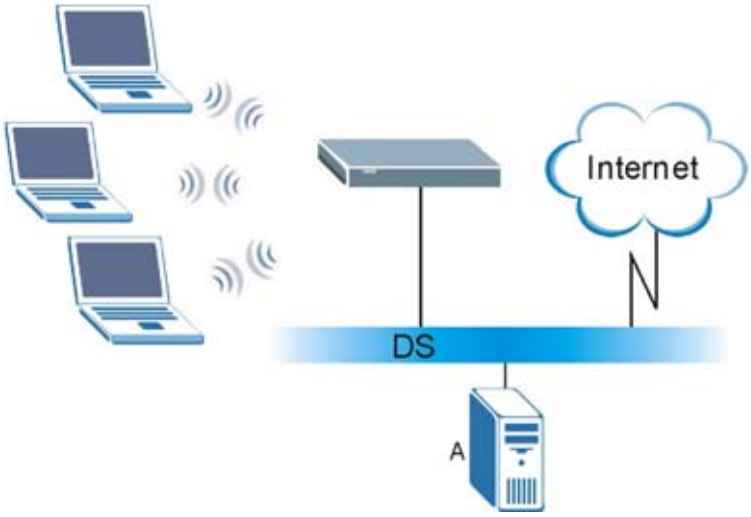


Рис. 6-7 Пример использования WPA с RADIUS

6.10 Сводка параметров безопасности

Обратитесь к таблице, чтобы увидеть какие еще параметры безопасности необходимо сконфигурировать для каждого типа протокола в части Метода аутентификации и управления ключами. Вручную введите ключи, вначале выбрав **64-bit WEP** или **128-bit WEP** в поле **WEP**

Encryption, а затем введя ключи (в ASCII или шестнадцатеричном формате) в текстовое окно. MAC-адрес фильтров не зависит от того как Вы конфигурируете эти характеристики безопасности.

Табл. 6-3 Матрица взаимосвязей беспроводной безопасности

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL (МЕТОД АУТЕНТИФИКАЦИИ/ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧОМ)	ENCRYPTION METHOD (МЕТОД КОДИРОВАНИЯ)	ENTER MANUAL KEY (РУЧНОЙ ВВОД КЛЮЧА)	ENABLE IEEE 802.1X (ВКЛЮЧЕНИЕ IEEE 802.1X)
Открытый	НЕТ	НЕТ	НЕТ
Открытый	WEP	НЕТ	Включен с динамическим ключом WEP
		ДА	Включен с динамическим ключом WEP
		ДА	Отключен
Коллективный	WEP	НЕТ	Включен с динамическим ключом WEP
		ДА	Включен с динамическим ключом WEP
		ДА	Отключен
WPA	WEP	НЕТ	ДА

Табл. 6-3 Матрица взаимосвязей беспроводной безопасности

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL (МЕТОД АУТЕНТИФИКАЦИИ/ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧОМ)	ENCRYPTION METHOD (МЕТОД КОДИРОВАНИЯ)	ENTER MANUAL KEY (РУЧНОЙ ВВОД КЛЮЧА)	ENABLE IEEE 802.1X (ВКЛЮЧЕНИЕ IEEE 802.1X)
WPA	TKIP	НЕТ	ДА
WPA-PSK	WEP	ДА	ДА
WPA-PSK	TKIP	ДА	ДА

6.11 Драйверы WPA беспроводных клиентов

Драйвер беспроводного клиента - это программное обеспечение, управляемое операционной системой, предоставляя беспроводному клиенту информацию об использовании WPA. На момент написания, наиболее широко распространенными драйверами являются: WPA -вставка для Windows XP, Funk Software's Odyssey client, и Meetinghouse Data Communications' AEGIS client.

Вставка в Windows XP представляет собой бесплатную подпрограмму, которая добавляет функцию WPA встроенной в Windows XP начальной конфигурации беспроводного клиента. Однако, для ее использования необходимо запустить Windows XP.

6.12 Конфигурирование 802.1x и WPA

Для изменения настроек аутентификации Prestige щелкните ссылку **Wireless LAN** под **Advanced Setup**, а затем закладку **802.1x/WPA**. Вид экрана будет различным, в зависимости от того какой протокол управления ключами Вы выбираете.

Если Вы выберете **No Access Allowed** или **No Authentication Required** отобразится следующий экран в поле **Wireless Port Control**.

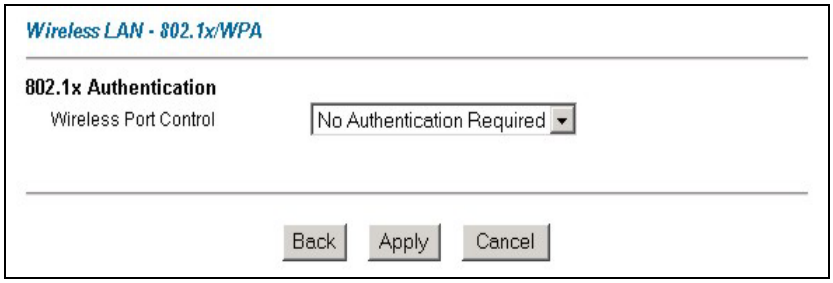


Рис. 6-8 Беспроводная LAN: 802.1x/WPA

В следующей таблице представлено описание полей данного экрана.

Табл. 6-4 Беспроводная LAN: 802.1x/WPA

ПОЛЕ	ОПИСАНИЕ
Wireless Port Control (Управление беспроводным портом)	Для управления доступом беспроводной станции к проводной сети выберите метод управления из выпадающего списка. Выберите из **No Access Allowed**, **No Authentication Required** и **Authentication Required**. **No Access Allowed** блокирует доступ всех беспроводных станций к проводной сети. **No Authentication Required** разрешает доступ всех беспроводных станций к проводной сети без введения имен пользователей и паролей. Это является установкой по умолчанию. **Authentication Required** означает, что все беспроводные станции должны ввести имена пользователей и пароли для подключения к проводной сети.. Для конфигурирования **Key Management Protocol** и других, относящихся к нему полей выберите **Authentication Required**.
Back (Назад)	Щелкните **Back** для возвращения к экрану основного Меню настройки беспроводной LAN.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

Необходима аутентификация: 802.1x

Выберите **Authentication Required** в поле **Wireless Port Control** и **802.1x** в поле **Key Management Protocol** для отображения следующего окна.

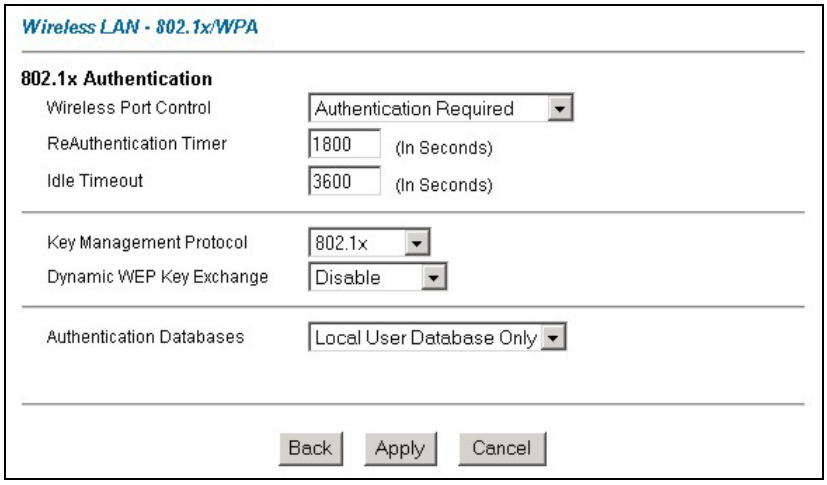


Рис. 6-9 Беспроводная LAN: Протокол 802.1x/WPA для 802.1x

В приводимой ниже таблице представлены описания надписей данного окна.

Табл. 6-5 Беспроводная LAN: Протокол 802.1x/WPA для 802.1x

ПОЛЕ	ОПИСАНИЕ
Wireless Port Control (Управление беспроводным портом)	Для управления доступом беспроводной станции к проводной сети выберите метод управления из выпадающего списка. Выберите из **No Authentication Required**, **Authentication Required** и **No Access Allowed**. Следующие поля доступны только, если Вы выберете **Authentication Required**.
ReAuthentication Timer (in Seconds) (Таймер повторной аутентификации) (в секундах)	Определите как часто беспроводная станция должна заново вводить имена пользователей и пароли для того, чтобы оставаться в сети. Данное поле доступно только, если Вы выберете **Authentication Required** в поле **Wireless Port Control**. Введите период времени в диапазоне от 10 до 9999 секунд. Временной интервал по умолчанию - **1800** секунд (30 минут). **Если аутентификация беспроводной станции производится с помощью сервера RADIUS, таймер повторной аутентификации на сервере RADIUS имеет приоритет.**

Табл. 6-5 Беспроводная LAN: Протокол 802.1x/WPA для 802.1x

ПОЛЕ	ОПИСАНИЕ
Idle Timeout (in Seconds) (Время простоя) (в секундах)	Prestige автоматически отключает беспроводную станцию от проводной сети после периода простоя. Для подключения к проводной сети станции может потребоваться снова ввести имя пользователя и пароль. Данное поле доступно только, если Вы выберете **Authentication Required** в поле **Wireless Port Control**. Временной интервал по умолчанию - **3600** секунд (или 1 час).
Key Management Protocol (Протокол управления ключами)	Выберите **802.1x** из выпадающего списка.
Dynamic WEP Key Exchange (Обмен динамическими ключами WEP)	Данное поле доступно только, если Вы выберете **Authentication Required** в поле **Wireless Port Control**. Установите также поле **Authentication Databases** в **RADIUS Only**. Локальная база данных пользователей может не использоваться. Выберите **Disable** для подключения беспроводных станций к точкам доступа без использования обмена динамическими ключами WEP. Выберите **64-bit WEP** или **128-bit WEP** для включения шифрования данных. Доступ к Prestige могут получить до 32 станций, если Вы конфигурируете обмен динамическими ключами WEP. Данное поле не доступно, если в поле **Key Management Protocol** Вы установили **WPA** или **WPA-PSK**.

Табл. 6-5 Беспроводная LAN: Протокол 802.1x/WPA для 802.1x

ПОЛЕ	ОПИСАНИЕ
Authentication Databases (База данных аутентификации)	База данных аутентификации содержит регистрационные сведения базы данных настроек пользователя. Локальная база данных пользователя представляет собой встроенную в Prestige базу данных. RADIUS является внешним сервером. Используйте этот выпадающий список для выбора какой (вначале) базой данных следует воспользоваться Prestige для аутентификации беспроводной станции. Перед определением приоритета, убедитесь, что Вы правильно создали соответствующую первую базу данных. Выберите **Local User Database Only** для того, чтобы Prestige проверил по встроенной базе данных имя пользователя и пароля беспроводной станции. Выберите **RADIUS Only** для того, чтобы Prestige проверил имя пользователя и пароль радиостанции по базе данных пользователей на конкретном сервере RADIUS. Выберите **Local first, then RADIUS** для того, чтобы Prestige вначале проверил имя пользователя и пароля беспроводной станции по базе данных пользователей в Prestige. Если имя пользователя не найдено, тогда Prestige проверяет по базе данных пользователей на конкретном сервере RADIUS. Выберите **RADIUS first, then Local** для того, чтобы Prestige вначале проверил имя пользователя и пароль беспроводной станции по базе данных пользователей на конкретном сервере RADIUS. Если Prestige не может обнаружить сервер RADIUS, тогда Prestige проверяет по локальной базе данных пользователей в Prestige. Если на сервере RADIUS имя пользователя не найдено или не соответствует пароль, Prestige не будет проверять по локальной базе данных и откажет в аутентификации.
Back (Назад)	Щелкните **Back** для возвращения к экрану основного Меню настройки беспроводной LAN.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

После включения аутентификации пользователя необходимо определить внешний сервер RADIUS или создать локальные учетные записи пользователя в Prestige для аутентификации.

Необходима аутентификация: WPA

Выберите **Authentication Required** в поле **Wireless Port Control** и **WPA** в поле **Key Management Protocol** для отображения следующего экрана.

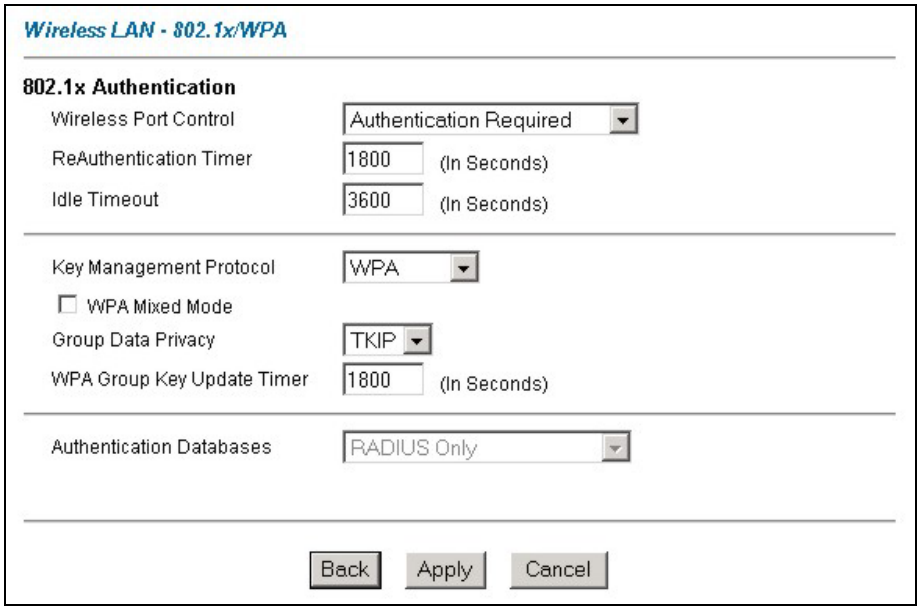


Рис. 6-10 Беспроводная LAN: Протокол 802.1x/WPA для WPA

В приводимой ниже таблице, даны описания полей, не рассматривавшихся ранее

Табл. 6-6 Беспроводная LAN: Протокол 802.1x/WPA для WPA

ПОЛЕ	ОПИСАНИЕ

Табл. 6-6 Беспроводная LAN: Протокол 802.1x/WPA для WPA

ПОЛЕ	ОПИСАНИЕ
Key Management Protocol (Протокол управления ключами)	В данном поле выберите **WPA** .
WPA Mixed Mode (Режим WPA Mixed)	Prestige может функционировать в режиме **WPA Mixed Mode**, который обеспечивает работу в одной сети Wi-Fi как клиентов, управляющих WPA так и клиентов, управляющих обменом динамическими ключами WEP при помощи 802.1x. Поставьте галочку в этом поле для активирования режима WPA mixed, или не ставьте галочку и заполните поле **Group Data Privacy**.
Group Data Privacy (Конфиденциальность группы данных)	**Group Data Privacy** позволяет выбрать **TKIP** (рекомендуется) или **WEP** для трафика широковещательной и многоадресной рассылки (“группы”), если в **Key Management Protocol** выбран **WPA,** а **WPA Mixed Mode -** отключен. **WEP** используется автоматически, если включен **WPA Mixed Mode**. Весь трафик одноадресной рассылки автоматически кодируется **TKIP**, если в **Key Management Protocol** выбирается **WPA** или **WPA-PSK**.
WPA Group Key Update Timer (Таймер обновлений ключей группы WPA)	**WPA Group Key Update Timer** - это частота, с которой AP (если используется управление ключами **WPA-PSK**) или сервер RADIUS (если используется управление ключами **WPA**) отправляет новую группу ключей всем клиентам. Процесс повторного кодирования представляет собой эквивалент WPA автоматически с заданным периодом изменяющий ключ WEP для AP и всех станций в WLAN. Настройка **WPA Group Key Update Timer** поддерживается и в режиме WPA-PSK. По умолчанию в Prestige это 1800 секунд (30 минут).
Authentication Databases (База данных аутентификации)	Если Вы конфигурируете **Key Management Protocol** в **WPA**, то **Authentication Databases** должно быть в положении **RADIUS Only**. **Local User Database Only** можно использовать только с **802.1x Key Management Protocol**.

Необходима аутентификация: WPA-PSK

Выберите **Authentication Required** в поле **Wireless Port Control** и **WPA-PSK** в поле **Key Management Protocol** для отображения следующего экрана.

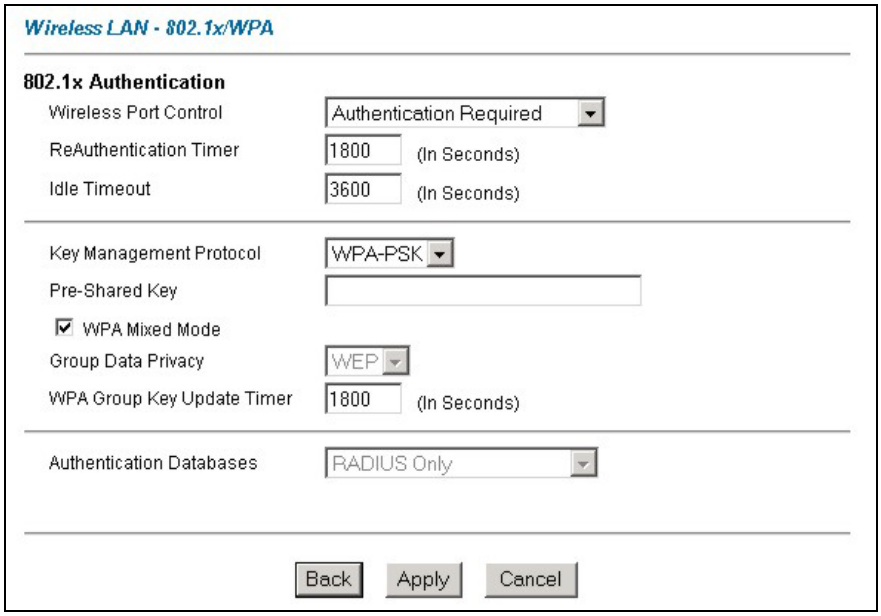


Рис. 6-11 Беспроводная LAN: Протокол 802.1x/WPA для WPA-PSK

В приводимой ниже таблице дается описания полей, не рассматривавшихся ранее

Табл. 6-7 Беспроводная LAN: Протокол 802.1x/WPA для WPA-PSK

ПОЛЕ	ОПИСАНИЕ
Key Management Protocol (Протокол управления ключами)	В данном поле выберите **WPA-PSK** .
Pre-Shared Key (Предварительно согласованный ключ)	Механизмы шифрования, используемые для **WPA** и **WPA-PSK,** одинаковы. Единственная разница между ними состоит в том, что **WPA-PSK** использует общий пароль, вместо мандатов индивидуальных пользователей. Введите предварительно согласованный ключ от 8 до 63 символов ASCII с учетом регистра (включая пробелы и знаки).

Табл. 6-7 Беспроводная LAN: Протокол 802.1x/WPA для WPA-PSK

ПОЛЕ	ОПИСАНИЕ
WPA Mixed Mode (Режим WPA Mixed)	Prestige может функционировать в режиме **WPA Mixed Mode**, который обеспечивает работу в одной сети Wi-Fi как клиентов, управляющих WPA так и клиентов, управляющих обменом динамическими ключами WEP при помощи 802.1x. Поставьте галочку в этом поле для активирования режима WPA mixed, или не ставьте галочку и заполните поле **Group Data Privacy**.
Group Data Privacy (Конфиденциальность группы данных)	**Group Data Privacy** позволяет выбрать **TKIP** (рекомендуется) или **WEP** для трафика широковещательной и многоадресной рассылки (“группы”), если в **Key Management Protocol** выбран **WPA,** а **WPA Mixed Mode -** отключен. **WEP** используется автоматически, если включен **WPA Mixed Mode**. Весь трафик одноадресной рассылки автоматически кодируется **TKIP**, если в **Key Management Protocol** выбирается **WPA** или **WPA-PSK**.
Authentication Databases (База данных аутентификации)	Данное поле видимо только при включенном режиме **WPA Mixed Mode**.

6.13 Конфигурирование локальной аутентификации пользователей

Сохраняя настройки пользователя локально, Prestige предоставляет обслуживание по аутентификации беспроводных пользователей без взаимодействия с сетевым сервером RADIUS. Однако, существует ограничение на число пользователей, которых можно аутентифицировать таким образом.

Для изменения локальной базы данных пользователей Prestige щелкните **Wireless LAN**, **Local User Database**. Отобразится окно, указанное ниже.

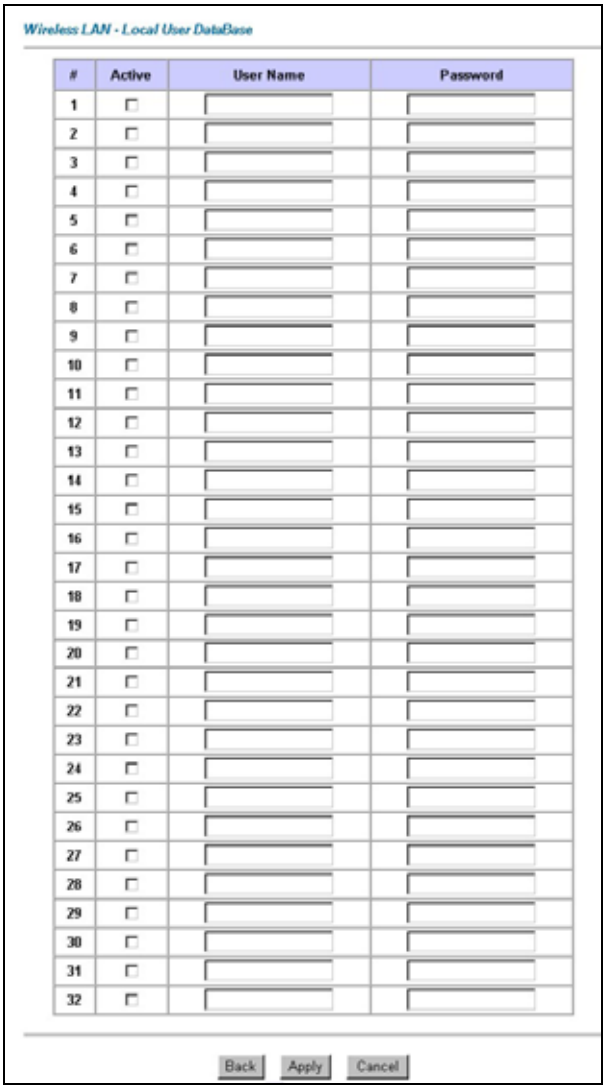


Рис. 6-12 Локальная база данных пользователей

В следующей таблице представлено описание полей данного экрана.

Табл. 6-8 Локальная база данных пользователей

ПОЛЕ	ОПИСАНИЕ
#	Это индекс локальной учетной записи пользователя.
Active (Активно)	Поставьте галочку в этом поле для включения настройки пользователя
User Name (Имя пользователя)	Введите имя настройки пользователя.
Password (Пароль)	Введите пароль (до 31 символа) для данной настройки пользователя.
Back (Назад)	Щелкните **Back** для возвращения к экрану основного Меню настройки беспроводной LAN.
Apply (Применить)	Щелкните **Apply** для сохранения этих настроек в Prestige.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

6.14 Конфигурирование RADIUS

После включения аутентификации EAP, необходимо установить сервер для внешней аутентификации и учета удаленных пользователей.

Для создания в Prestige настроек сервера RADIUS щелкните **WIRELESS LAN**, **RADIUS**. Отобразится окно, указанное ниже.

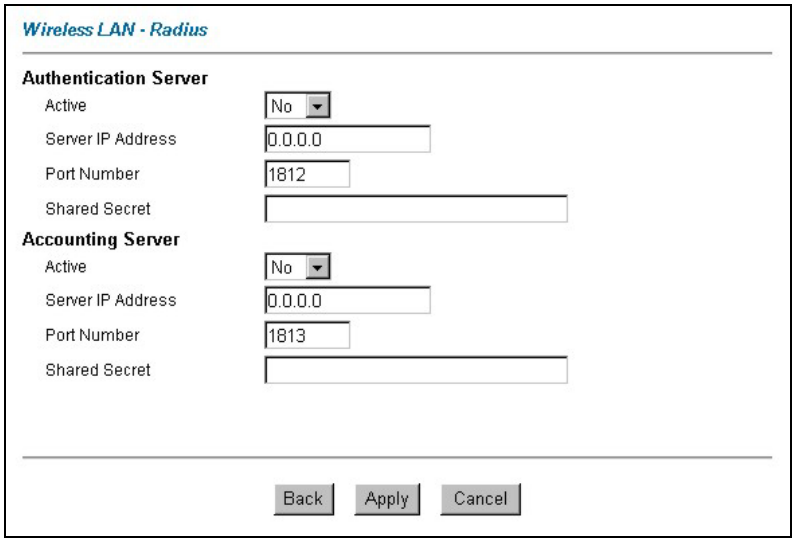


Рис. 6-13 RADIUS

В следующей таблице представлено описание полей данного экрана.

Табл. 6-9 RADIUS

ПОЛЕ	ОПИСАНИЕ
Authentication Server (Сервер аутентификации)	
Active (Активно)	Выберите **Yes** из выпадающего списка для включения аутентификации пользователей с помощью сервера внешней аутентификации.
Server IP Address (IP-адрес сервера)	Введите IP-адрес сервера внешней аутентификации в десятичном виде с разделительными точками.
Port Number (Номер порта)	Порт аутентификации сервера RADIUS по умолчанию - **1812**. Не следует изменять это значение, если сетевой администратор не предоставит дополнительной информации.

Табл. 6-9 RADIUS

ПОЛЕ	ОПИСАНИЕ
Shared Secret (Коллективный ключ)	Введите пароль (до 31 буквенно-цифрового символа) в качестве ключа согласованного с сервером внешней аутентификации и точками доступа. Ключ не пересылается через сеть. Данный ключ должен быть одним и тем же для сервера внешней аутентификации и для Prestige.
Accounting Server (Сервер учета)	
Active (Активно)	Выберите **Yes** из выпадающего списка для включения аутентификации пользователей с помощью сервера учета.
Server IP Address (IP-адрес сервера)	Введите IP-адрес сервера внешнего учета в десятичном виде с разделительными точками.
Port Number (Номер порта)	Порт учета сервера RADIUS по умолчанию - **1813**. Не следует изменять это значение, если сетевой администратор не предоставит дополнительной информации.
Shared Secret (Коллективный ключ)	Введите пароль (до 31 буквенно-цифровых символов) в качестве ключа, согласованного с сервером внешнего учета и точками доступа. Ключ не пересылается через сеть. Данный ключ должен быть одним и тем же для сервера внешнего учета и для Prestige.
Back (Назад)	Щелкните **Back** для возвращения к экрану основного Меню настройки беспроводной LAN.
Apply (Применить)	Щелкните **Apply** для сохранения этих настроек в Prestige.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

Раздел 7
Настройка WAN

В этой главе описывается конфигурирование настроек WAN.

7.1 Описание WAN

WAN (Wide Area Network/Глобальная вычислительная сеть) - это внешнее соединение с другой сетью или Интернетом.

Для более подробной информации о полях экранов WAN см. главу *Мастер Установки*.

7.2 Метрика

Метрика определяет "стоимость передачи". Маршрутизатор определяет лучший маршрут для передачи, выбирая траекторию с наименьшей "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве своего рода единицы стоимости, с минимальным значением, равным "1" стоимости прямого соединения. Число должно находиться в диапазоне от "1" до "15"; число больше, чем "15" означает, что связь отсутствует. Чем меньше число, тем меньше "стоимость".

Метрика устанавливает приоритет для маршрутов Prestige в Интернете. Если любые два маршрута по умолчанию имеют одинаковую метрику, Prestige использует следующие предопределенные приоритеты:

1. Стандартный маршрут: выделенный Интернет-провайдером (см. *раздел 7.5*)
2. Маршрут переадресации трафика (см. *раздел 7.7*)
3. Резервный маршрут WAN, также называемый резервным соединением (см. *раздел 7.7*)

Напр., если стандартный маршрут имеет метрику "1" , а маршрут переадресации трафика имеет метрику "2" и резервный маршрут имеет метрику "3", тогда стандартный маршрут выступает в качестве основного маршрута по умолчанию. Если по стандартному маршруту не удается подключиться к Интернету, Prestige пробует следующий маршрут переадресации трафика. Таким же образом, Prestige использует резервный маршрут, если маршрут переадресации трафика также терпит неудачу.

Если Вы хотите, чтобы резервный маршрут имел более высокий приоритет над маршрутом переадресации трафика или даже стандартным маршрутом, все, что необходимо сделать, это установить метрику "1" для резервного маршрута, а для остальных "2" (или больше).

Маршрутизация на базе стратегии IP игнорирует схему маршрутизации по умолчанию и имеет приоритет над всеми маршрутами, упомянутыми выше (см. главу *Маршрутизация на базе стратегии IP*).

7.3 Инкапсуляция PPPoE

Prestige поддерживает PPPoE (Point-to-Point Protocol over Ethernet/Протокол “точка-точка“ через Ethernet). PPPoE это стандарт IETF (RFC 2516), определяющий как персональный компьютер (PC) взаимодействует с широкополосным модемным соединением (DSL, кабель, беспроводной канал и т. д.). Функция **PPPoE** применяется для коммутируемого соединения, использующего PPPoE.

Для провайдера услуг, PPPoE предлагает доступ и метод аутентификации, взаимодействующий с существующими системами управления доступом (напр. Radius). PPPoE предоставляет регистрацию и метод аутентификации, которые может активировать существующее микропрограммное обеспечение удаленного доступа к сети Microsoft, и поэтому не требующее предварительного изучения или специальных методик для пользователей Windows.

Одно из преимуществ PPPoE заключается в возможности получения доступа к одной из многочисленных сетевых услуг, функции известной как динамической выбор услуги. Это позволяет провайдеру услуг без труда создать и предложить новые услуги IP для отдельных клиентов.

Функционально, PPPoE сохраняет затраты, сделанные Вами Интернет-провайдером или владельцем сети, так как он не требует особой конфигурации широкополосного модема у клиента.

PPPoE непосредственно внедрен в Prestige (а не в отдельные компьютеры), поэтому нет необходимости установки микропрограммного обеспечения PPPoE на компьютерах LAN, так как Prestige выполняет эту часть задачи. Кроме того, с NAT, все компьютеры LAN будут иметь доступ.

7.4 Формирование трафика

Функция формирования трафика представляет собой соглашение между владельцем сети и абонентом, предназначенное для регулировки средней скорости и колебаний скорости передачи данных через сеть ATM. 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 данных в 832 кбит/с дает максимальную скорость PCR 1962 ячеек/с. Однако эта скорость не гарантирована, потому что она зависит от скорости линии.

Sustained Cell Rate (SCR) (Поддерживаемая скорость ячеек) представляет собой значение средней скорости ячеек каждого пульсирующего источника данных (отправителя). Она указывает максимальную
среднюю скорость, на которой можно осуществлять передачу ячеек через виртуальное соединение. Поддерживаемая скорость ячеек не может быть больше, чем скорость PCR.

Максимальный размер пакета (MBS) это максимальное количество ячеек, которое может быть передано со скоростью PCR. После достижения MBS,
скорость ячеек опускается ниже SCR, до тех пор пока скорость ячеек снова не выравняется до SCR. К этому времени, большинство ячеек (вплоть до
MBS) могут снова передаваться со скоростью PCR.

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

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

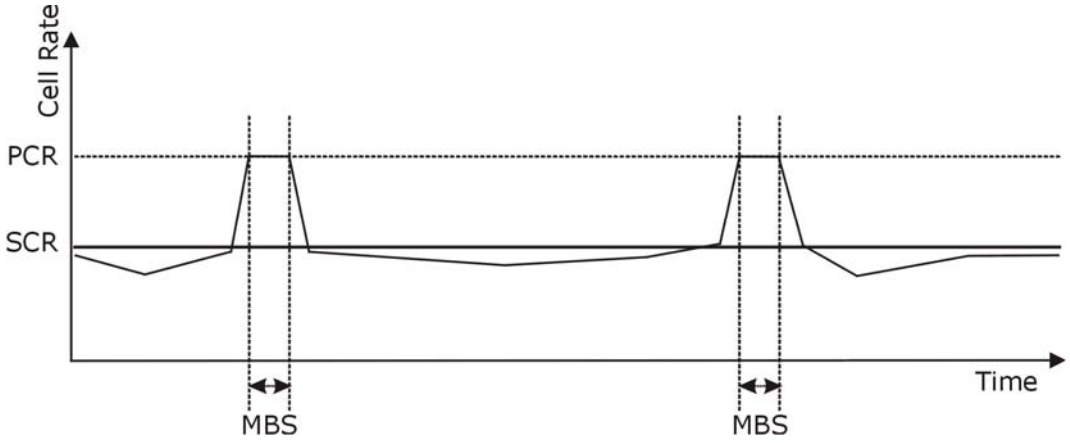


Рис. 7-1 Пример формирования трафика

7.5 Начальная конфигурация доступа в Интернет

При включении и подключении Prestige к телефонной розетке, он автоматически обнаруживает настройки подключения к Интернету (такие как номера VCI/VPI и метод инкапсуляции), полученные от Интернет-провайдера и производит необходимые изменения конфигурации. В случаях, когда

требуется дополнительная учетная информация (такая как имя и пароль учетной записи пользователя Интернет) или Prestige не может подключиться к Интернет-провайдеру, происходит переадресация к web-экрану(-ам) по вводу информации или устранению неисправностей.

Начальная конфигурация доступа в Интернет отключена, если

- Prestige находится в режиме межсетевого моста
- Prestige установлен в режим использования статического (фиксированного) IP-адреса WAN.

7.6 Конфигурирование настройки WAN

Щелкните **WAN**, **WAN Setup** для изменения в Prestige настроек удаленного узла WAN. Вид экрана различается в зависимости от типа используемой инкапсуляции.

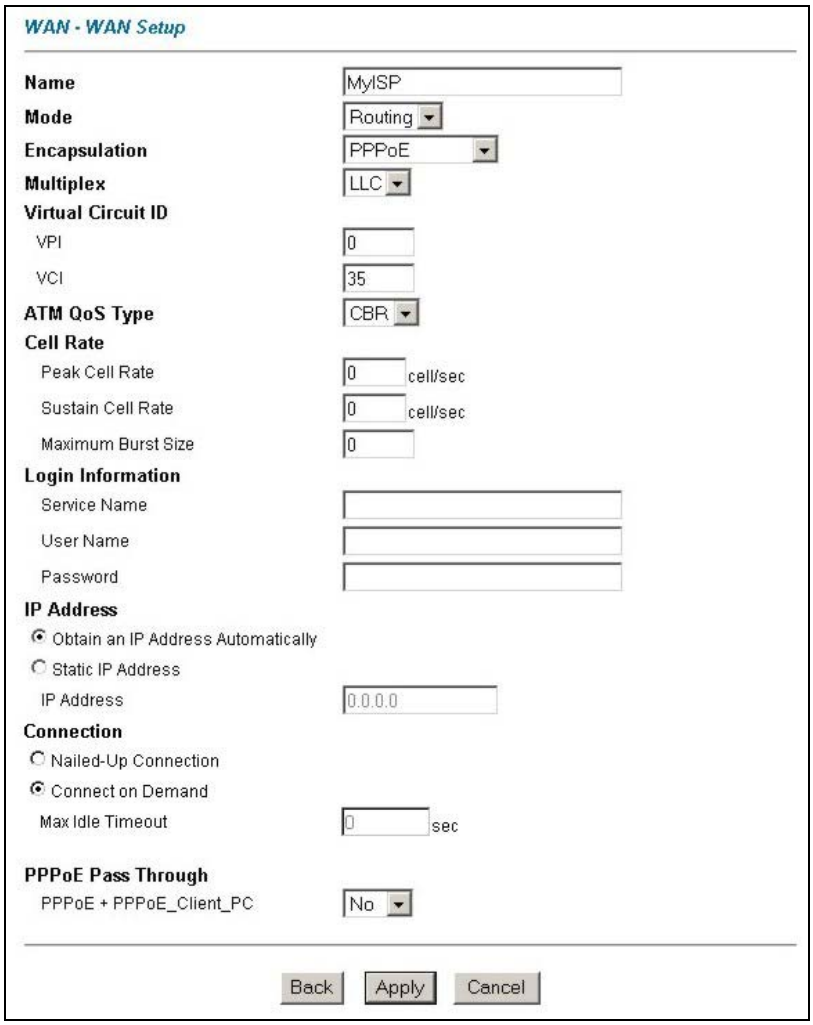


Рис. 7-2 Настойка WAN

В следующей таблице представлено описание полей данного экрана.

Табл. 7-1 Настройка WAN

ПОЛЕ	ОПИСАНИЕ
Name (Имя)	Введите имя Интернет-провайдера, напр., MyISP. Эта информация нужна только для идентификации.
Mode (Режим)	Из выпадающего списка выберите **Routing** (по умолчанию), если Интернет-провайдер допускает использование нескольким компьютерам одинаковых учетных записей. В противном случае выберите **Bridge**.
Encapsulation (Инкапсуляция)	Из выпадающего списка выберите метод инкапсуляции, используемый Интернет-провайдером. Возможности различаются в зависимости от того, что Вы выбрали в поле **Mode**. Если в поле **Mode** Вы выбираете **Bridge**, выберите **PPPoA** или **RFC 1483**. Если в поле **Mode** Вы выбираете **Routing**, выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
Multiplex (Мультиплексный)	Из выпадающего списка выберите метод мультиплексирования, используемый Интернет-провайдером. Вариантами являются: **VC** или **LLC**.
Virtual Circuit ID (Идентификатор виртуального канала)	VPI (Идентификатор виртуального пути) и VCI (Идентификатор виртуального канала) определяют виртуальный канал. Более подробно см. в приложении.
VPI (Идентификатор виртуального пути)	Допустимый диапазон для VPI - от 0 до 255. Введите назначенный VPI.
VCI (Идентификатор виртуального канала)	Допустимый диапазон для VCI - от 32 до 65535 (0 - 31 зарезервировано для локального управления трафиком ATM). Введите назначенный идентификатор виртуального канала.
ATM QoS Type (Тип QoS ATM)	Выберите **CBR** (Continuous Bit Rate/Постоянная скорость передачи в битах), чтобы определить фиксированную (всегда включена) пропускную способность для голосовой связи или передачи данных. Выберите **UBR** (Unspecified Bit Rate - Не определена скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите **VBR** (Variable Bit Rate/Регулируемая скорость передачи в битах) для пульсирующего трафика и пропускной способности, совместимой с другими вариантами использования.
Cell Rate (Скорость ячеек)	Конфигурирование скорости ячеек часто помогает устранить перегрузку трафика, замедляющего передачу данных в реальном времени, напр., аудио- и видеоданных.

Табл. 7-1 Настройка WAN

ПОЛЕ	ОПИСАНИЕ
Peak Cell Rate (Пиковая скорость ячеек)	Разделите скорость линии DSL (в битах в секунду) на 424 (размер ячейки ATM), чтобы получить значение скорости PCR (Peak Cell Rate/Максимальной скорости ячеек). Это — максимальная скорость, с которой отправитель может передавать ячейки. Введите в этом поле значение PCR.
Sustain Cell Rate (Поддерживаемая скорость ячеек)	Поддерживаемая скорость ячеек (SCR) устанавливает значение средней скорости (на длительный период) передачи ячеек. Введите SCR, которая должна быть меньше PCR. Следует отметить, что по умолчанию - 0 ячеек/с.
Maximum Burst Size (Максимальный размер пакета)	Максимальный размер пакета (MBS) обозначает максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите MBS, который должен быть меньше 65535.
Login Information (Регистрационные сведения)	(PPPoA и только инкапсуляция PPPoE)
Service Name (Сервисное имя)	(только PPPoE) Введите имя сервиса PPPoE.
User Name (Имя пользователя)	Введите имя пользователя в точности так как назначено Интернет-провайдером. Если имя назначено в виде user@domain, где домен идентифицирует сервисное имя, тогда введите оба компонента точно как представлено.
Password (Пароль)	Введите пароль, соответствующий имени пользователя, указанному выше.
IP Address (IP-адрес)	Эта опция доступна, если Вы выбираете **Routing** в поле **Mode**. Статический IP-адрес - это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не фиксирован; Интернет-провайдер каждый раз назначает новый адрес при подключении к Интернету. Учетная запись одиночного пользователя может быть включена или отключена в зависимости от характера имеющегося IP-адреса (статический или динамический). Выберите **Obtain an IP Address Automatically**, если имеется динамический IP-адрес; или выберите **Static IP Address** и введите, назначенный Интернет-провайдером IP-адрес в поле **IP Address**.

Табл. 7-1 Настройка WAN

ПОЛЕ	ОПИСАНИЕ
Connection (PPPoA and PPPoE encapsulation only) (Соединение (PPPoA и только инкапсуляция PPPoE)	Правило(а) планирования в меню 26 SMT имеет приоритет над настройками **Connection**.
Nailed-Up Connection (Полупостоянное соединение)	Выберите **Nailed-Up Connection**, если Вы хотите быть подключенным все время. Prestige попытается подключиться автоматически, если соединение разъединилось.
Connect on Demand (Соединение по запросу)	Выберите **Connect on Demand**, если Вы не хотите иметь постоянное соединение и установите время простоя в поле **Max Idle Timeout**.
Max Idle Timeout (Максимальное время простоя)	При выборе **Connect on Demand,** установите время простоя в поле **Max Idle Timeout**. Установкой по умолчанию является 0, что означает, что сеанс связи с Интернетом не должен прерваться.
PPPoE Pass Through (Пересылка PPPoE)	Это поле доступно, если Вы выберете инкапсуляцию **PPPoE**.
PPPoE + PPPoE_Client_PC (Клиент PC PPPoE + PPPoE) PPPoE encapsulation only) (только инкапсуляция PPPoE)	В дополнение к встроенному в Prestige клиенту PPPoE, можно включить пересылку PPPoE, допускающую наличие до десяти хостов в LAN, использующих PPPoE клиентское программное обеспечение на своих компьютерах для подключения к Интернет-провайдеру при помощи Prestige. Каждый хост может иметь отдельную учетную запись и общедоступный IP-адрес WAN. Пересылка PPPoE является вариантом использования NAT, где NAT не назначен. Отключите пересылку PPPoE, если нет необходимости допускать хосты в LAN, использующие клиентское программное обеспечение PPPoE на своих компьютерах, к подключению к Интернет-провайдеру

Табл. 7-1 Настройка WAN

ПОЛЕ	ОПИСАНИЕ
Subnet Mask (ENET ENCAP encapsulation only) (Маска подсети (только инкапсуляция ENET ENCAP)	Введите маску подсети в десятичном виде с разделительными точками. Для вычисления маски подсети см. Приложение *Организация подсетей* (если Вы их используете).
ENET ENCAP Gateway (Шлюз ENET ENCAP) (ENET ENCAP encapsulation only) (только инкапсуляция ENET ENCAP)	Если в поле **Encapsulation** Вы выбрали **ENET ENCAP,** необходимо определить IP-адрес шлюза (предоставляется Интернет-провайдером)
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения изменений.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

7.7 Переадресация трафика

Переадресация трафика пересылает трафик на резервный шлюз, если Prestige не может установить соединение с Интернетом. Пример показан на следующем рисунке.

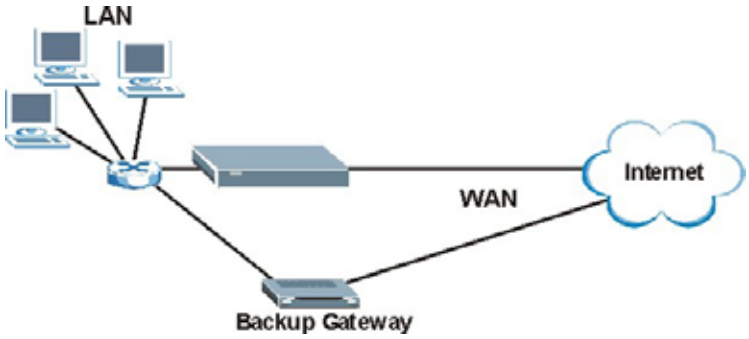


Рис. 7-3 Пример переадресации трафика

Следующая топология сети позволяет избежать образования треугольного маршрута, когда к LAN подключен резервный шлюз. Используйте псевдоним IP для разделения LAN на две или три логических сети, где Prestige выступает в качестве шлюза для каждой сети LAN. Поместите защищенную LAN в одну подсеть (Подсеть 1 на следующем рисунке), а резервный шлюз - в другую подсеть (Подсеть 2). Сконфигурируйте фильтры для пересылки пакетов из защищенной LAN (Подсеть 1) в резервный шлюз (Подсеть 2).

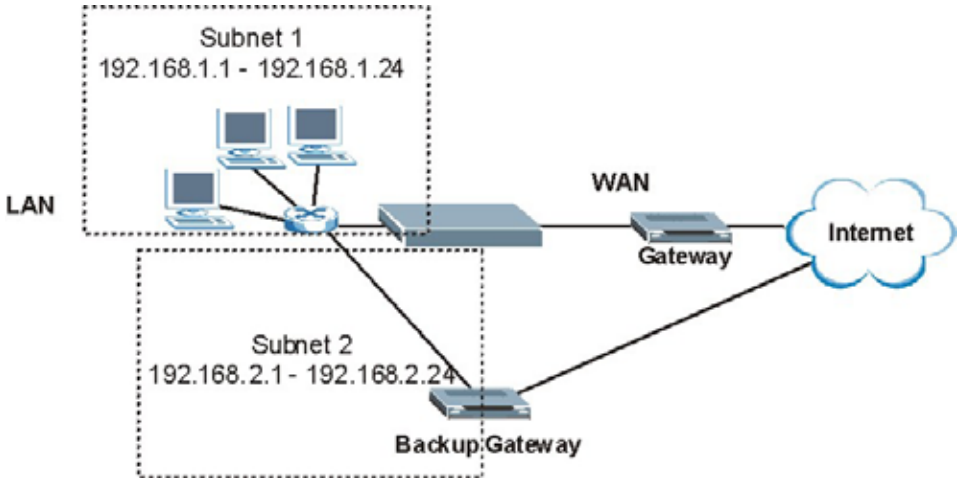


Рис. 7-4 Настройка LAN при переадресации трафика

7.8 Конфигурирование резервного соединения с WAN

Для изменения в Prestige настроек резервного сохранения WAN щелкните **WAN**, затем **WAN Backup** . Отобразится окно, указанное ниже.

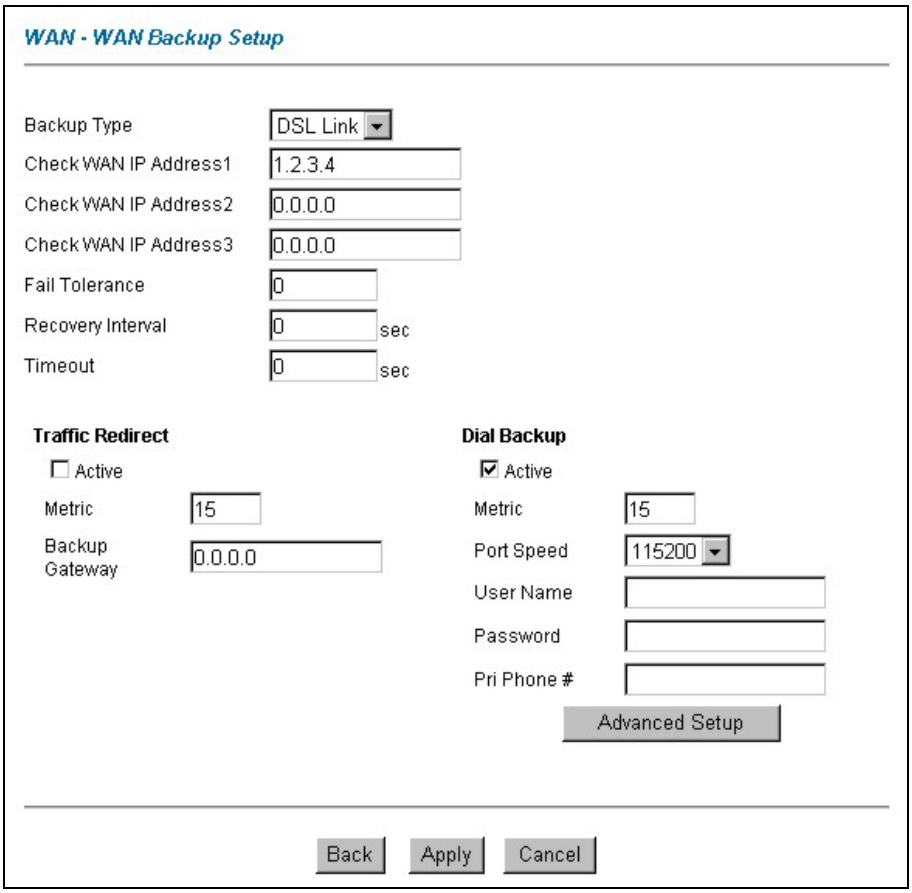


Рис. 7-5 Резервное соединение с WAN

В следующей таблице представлено описание полей данного экрана.

Табл. 7-2 Резервное соединение с WAN

ПОЛЕ	ОПИСАНИЕ
Backup Type (Тип резервирования)	Выберите метод, используемый Prestige для проверки соединения DSL. Выберите **DSL Link** для проверки Prestige физического уровня соединения DSL. Выберите **ICMP** для того, чтобы Prestige периодически посылал эхо-пакеты на IP-адреса, заданные в полях **Check WAN IP Address**.
Check WAN IP Address1-3 (Проверка IP-адресов 1-3 WAN)	Заполните это поле для проверки доступности WAN. Введите IP-адрес надежного близкого компьютера (напр., адрес сервера DNS Интернет-провайдера). При использовании дублирующего соединения с WAN, Prestige периодически посылает эхо-пакеты на заданные здесь адреса и использует другое дублирующее соединение с WAN (если сконфигурировано), если не получает ответа.
Fail Tolerance (Устойчивость к отказам)	Введите время в секундах (рекомендуется 2), в течение которого Prestige может посылать эхо-пакеты на IP-адреса, заданные в полях **Check WAN IP Address** без получения ответа до переключения на дублирующее соединение с WAN (или на другое дублирующее соединение с WAN).
Recovery Interval (Интервал восстановления)	Если Prestige использует соединение с более низким приоритетом (обычно дублирующее соединение с WAN), он периодически проверяет может ли он использовать соединения с более высоким приоритетом. Введите время в секундах (рекомендуется 30), которое Prestige может прибывать в ожидании между проверками. Допускается более длительный промежуток времени, если IP-адрес назначения справляется с обширным трафиком.
Timeout (Время простоя)	Введите время в секундах (рекомендуется 3), которое Prestige может пребывать в ожидании ответа эхо-пакета с одного из IP-адресов, заданных в полях **Check WAN IP Address** до окончания времени ответа. Соединение WAN считается "down" после того как Prestige израсходует время, указанное в поле **Fail Tolerance**. В данном поле используйте большее значение, в случае, если сеть занята или переполнена.
Traffic Redirect (Переадресация трафика)	
Active (Активно)	Поставьте галочку в этом поле для использования в Prestige переадресации трафика, если не удается установить нормальное подключение к WAN.

Табл. 7-2 Резервное соединение с WAN

ПОЛЕ	ОПИСАНИЕ
Metric (Метрика)	В этом поле устанавливается приоритет маршрута среди маршрутов, используемых Prestige. Метрика определяет "стоимость передачи". Маршрутизатор определяет лучший маршрут для передачи, выбирая траекторию с наименьшей "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве своего рода единицы стоимости, с минимальным значением равным "1" для прямого соединения. Число должно находиться в диапазоне от "1" до "15"; число больше "15" означает, что связь отсутствует. Чем меньше число, тем меньше "стоимость".
Backup Gateway (Резервный шлюз)	Введите IP-адрес резервного шлюза в десятичном виде с разделительными точками. Prestige автоматически пересылает трафик на этот IP-адрес, если прерывается подключение к Интернету.
Dial Backup (Резервное соединение)	
Active (Активно)	Поставьте галочку в этом поле для включения резервного соединения.
Metric (Метрика)	В этом поле устанавливается приоритет маршрута среди трех маршрутов, используемых Prestige (стандартный, переадресация трафика и резервное соединения). Введите число (от 1 до 15) для установления приоритета маршрута резервного соединения, используемого при передаче данных. Чем меньше число, тем выше приоритет. Если три маршрута имеют одинаковые значения метрик, то приоритет маршрутов выглядит следующим образом: **WAN**, **Traffic Redirect**, **Dial Backup**.
Port Speed (Скорость порта)	Из выпадающего списка выберите скорость соединения между портом резервного соединения и внешним устройством. Возможными являются: **9600**, **19200**, **38400**, **57600**, **115200** или **230400** бит/с.
User Name (Имя пользователя)	Введите регистрационное имя, назначенное Интернет-провайдером.
Password (Пароль)	Введите пароль, назначенный Интернет-провайдером.
Pri Phone # (Первичный телефон)	Введите первый (первичный) номер телефона, назначенный Интернет-провайдером для этого удаленного узла. Некоторые зоны требуют набора знака “решетки“ (#) перед номером телефона для местных вызовов. Если это требуется, используйте символ # в начале номера телефона.

Табл. 7-2 Резервное соединение с WAN

ПОЛЕ	ОПИСАНИЕ
Advanced Setup (Дополнительные настройки)	Щелкните по этой кнопке для отображения экрана **Advanced Setup** и отредактируйте остальные настройки резервного соединения с WAN.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения изменений.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

7.9 Конфигурирование дополнительных настроек резервного соединения с WAN

Для редактирования дополнительных настроек резервного соединения с WAN щелкните **WAN**, **WAN Backup**, а затем кнопку **Advanced Setup**. Отобразится окно, указанное ниже.

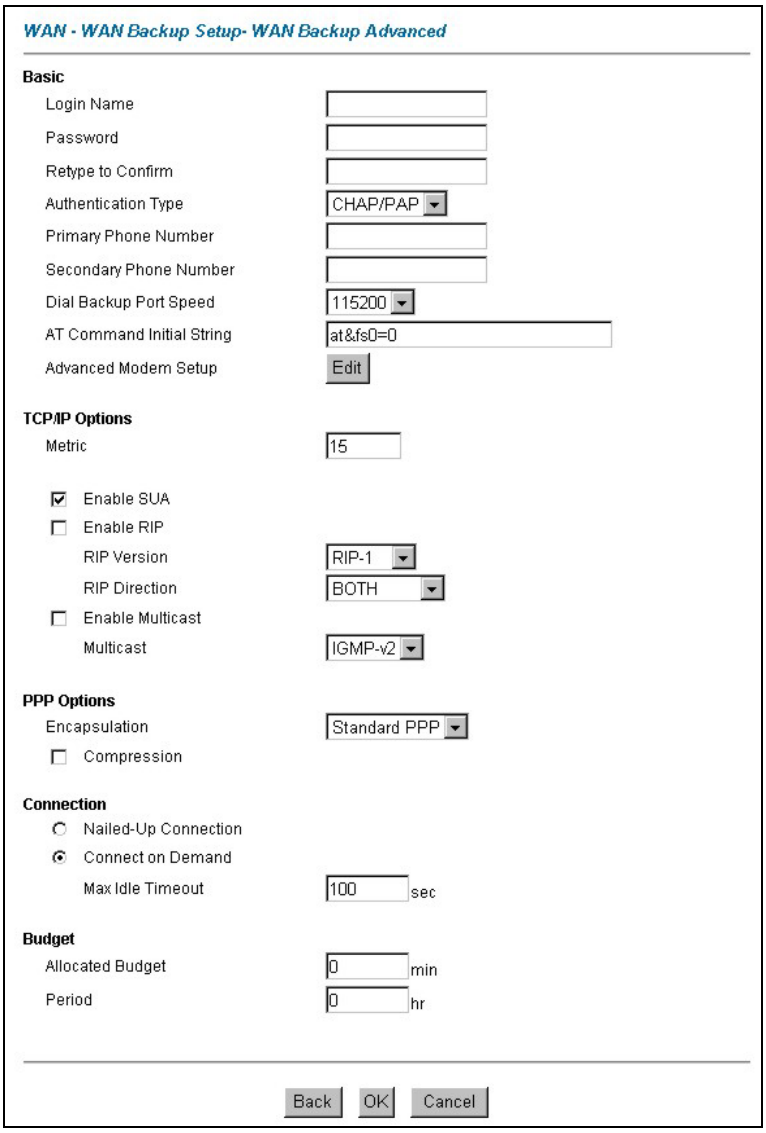


Рис. 7-6 Дополнительные настройки резервного соединения с WAN

В следующей таблице представлено описание полей данного экрана.

Табл. 7-3 Дополнительные настройки резервного соединения с WAN

ПОЛЕ	ОПИСАНИЕ
Basic (Основной)	
Login Name (Регистрационное имя)	Введите регистрационное имя, назначенное Интернет-провайдером.
Password (Пароль)	Введите пароль, назначенный Интернет-провайдером.
Retype to confirm (Подтверждение пароля)	Введите пароль еще раз, чтобы убедиться, что Вы правильно ввели пароль.
Authentication Type (Тип аутентификации)	Для выбора протокола аутентификации для исходящих звонков используйте выпадающий список. Опциями являются: **CHAP/PAP** - Prestige принимает CHAP или PAP при запросе этим удаленным узлом. **CHAP** - Prestige принимает только CHAP. **PAP** - Prestige принимает только PAP.
Primary/ Secondary Phone Number (Первый/Второй номер телефона)	Введите первый (первичный) номер телефона, назначенный Интернет-провайдером для этого удаленного узла. Если первичный телефонный номер занят или не отвечает, Prestige набирает второй телефонный номер, если он определен. Некоторые зоны требуют набора знака “решетки“ (#) перед номером телефона для местных вызовов. Если это требуется используйте символ # в начале номера телефона.
Dial Backup Port Speed (Скорость порта резервного соединения)	Из выпадающего списка выберите скорость связи между портом резервного соединения и внешним устройством. Возможными являются: **9600**, **19200**, **38400**, **57600**, **115200** или **230400** бит/с.
AT Command Initial String (Начальная строка AT-команды)	Введите строку AT-команды для инициализации устройства WAN. Для уточнения AT-команд см. инструкцию Вашего устройства резервного соединения.
Advanced Modem Setup (Дополнительная настройка модема)	Щелкните по кнопке **Edit** для отображения экрана **Advanced Modem Setup** и отредактируйте дополнительные настройки резервного соединения.

Табл. 7-3 Дополнительные настройки резервного соединения с WAN

ПОЛЕ	ОПИСАНИЕ
TCP/IP Options (Параметры TCP/IP)	
Metric (Метрика)	В этом поле устанавливается приоритет маршрута среди трех маршрутов, используемых Prestige (стандартный, переадресация трафика и резервное соединение). Введите число (от 1 до 15) для установления приоритета маршрута резервного соединения, используемого при передаче данных. Чем меньше число, тем выше приоритет. Если три маршрута имеют одинаковые метрики, то приоритет маршрутов выглядит следующим образом: **WAN**, **Traffic Redirect**, **Dial Backup**.
Enable SUA (Включить SUA)	Трансляция сетевых адресов (NAT) допускает трансляцию адреса межсетевого протокола (IP), используемого в одной сети, в другие IP-адреса, известные в другой сети. SUA (Single User Account/Учетная запись одиночного пользователя) является подмножеством NAT, поддерживающим два типа отображения: Много-в-один и “сервер“. Если Вы выбираете эту опцию, Prestige будет использовать Набор преобразования адресов 255 SMT (для более подробной информации см. раздел Меню 15.1).
Enable RIP (Включить RIP)	Поставьте галочку в этом поле для включения RIP (Routing Information Protocol/Протокол обмена информацией), позволяющий маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами.
RIP Version (Версия RIP)	Поле **RIP Version** управляет форматом и методом циркуляционной рассылки пакетов RIP, которые посылает Prestige (оба формата распознаются при получении). Выберите **RIP-1**, **RIP-2B** или **RIP-2M**. Формат **RIP-1** является общепринятым; но **RIP-2** содержит больше информации. Для большинства сетей подходит RIP-1, если только сеть не имеет какой-либо специфической топологии. Оба формата **RIP-2B** и **RIP-2M** осуществляют передачу данных маршрутизации в формате RIP-2; отличие заключается в том, что RIP-2B использует циркуляционную рассылку, а RIP-2M - многоадресную рассылку. Многоадресная рассылка может уменьшать нагрузку на машины, не являющиеся маршрутизаторами, так как они в основном не воспринимают адреса для многоадресной рассылки RIP и поэтому не получают пакетов RIP. Однако, если один маршрутизатор использует многоадресную рассылку, тогда все маршрутизаторы в сети должны также использовать многоадресную рассылку.

Табл. 7-3 Дополнительные настройки резервного соединения с WAN

ПОЛЕ	ОПИСАНИЕ
RIP Direction (Направление RIP)	Протокол обмена информацией (RIP) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Поле **RIP Direction** управляет приемом и передачей пакетов RIP. Выберите **Both**, **In Only** или **Out Only**. Если установлено **Both** или **Out Only**, Prestige будет периодически передавать свою таблицу маршрутизации. Если установлено **Both** или **In Only**, Prestige будет принимать данные RIP, которые он получает.
Enable Multicast (Включение многоадресной рассылки)	Поставьте галочку в этом поле, чтобы включить IGMP (Internet Group Multicast Protocol/Протокол управления группами). IGMP - это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки - он не предназначен для передачи пользовательских данных.
Multicast (Многоадресная рассылка)	Выберите **IGMP-v1** или **IGMP-v2**. Версия 2 IGMP (RFC 2236) является усовершенствованным вариантом версии 1 (RFC 1112), однако версия 1 IGMP все еще широко используется. Если Вы хотите узнать более подробную информацию о взаимодействии между версией 2 IGMP и версией 1, см. *разделы 4* и *5 RFC 2236*.
PPP Options (Параметры PPP)	
Encapsulation (Инкапсуляция)	Выберите **CISCO PPP** из выпадающего списка, если устройство резервного соединения с WAN использует инкапсуляцию **Cisco PPP**; или же выберите **Standard PPP**.
Compression (Сжатие)	Поставьте галочку в этом поле для включения сжатия.
Connection (Подключение)	
Nailed-Up Connection (Полупостоянное соединение)	Выберите **Nailed-Up Connection**, если Вы хотите иметь подключение все время. Prestige автоматически будет пытаться подключиться, если соединение разъединилось.
Connect on Demand (Соединение по запросу)	Выберите **Connect on Demand**, если Вы не хотите иметь постоянное соединение и установите время простоя в поле **Max Idle Timeout**.

Табл. 7-3 Дополнительные настройки резервного соединения с WAN

ПОЛЕ	ОПИСАНИЕ
Max Idle Timeout (Максимальное время простоя)	При выборе **Connect on Demand** установите время простоя в поле **Max Idle Timeout**. Установкой по умолчанию является 0, что означает, что сеанс связи с Интернетом не должен прерываться.
Budget (Бюджет)	Конфигурация в полях **Budget** имеет приоритет над настройками **Connection**.
Allocate Budget (Распределение бюджета)	Введите количество времени (в минутах), которое резервное соединение может использовать в течении периода времени, заданного в поле **Period**. Установите количество времени меньшее, чем период времени, заданный в поле **Period**. Если Вы установите 0 для **Allocated Budget**, то не сможете использовать резервное соединение.
Period (Период)	Введите период времени (в часах), чтобы установить как часто бюджет следует сбрасывать. Напр., для совершения звонков на этот удаленный узел в течение часа с максимальным 10 минутным интервалом, установите 10 (минут) для **Allocated Budget** и 1 (час) для **Period**. Если Вы установите 0 для **Period**, то управление бюджетом будет отключено и Prestige будет использовать настройки **Connection**.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
OK	Щелкните **OK** для возвращения к предыдущему окну, а затем **Apply** для сохранения изменений.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

7.10 Строки AT-команд

Для обычных телефонных линий параметр по умолчанию для строки набора “Dial” сообщает модему о том, что на линии используется тональный набор. “ATDT” - это команда для коммутатора, требующего тонального набора. Если коммутатор требует импульсного набора номера, следует заменить ее на “ATDP”.

Для линий ISDN существует гораздо больше протоколов и рабочих режимов. Следует проконсультироваться с документацией по используемому терминальному адаптеру. Возможно, потребуется ввести дополнительные команды в строки “Dial” и “Init”.

7.11 Сигнал DTR

Большинство устройств WAN по умолчанию завершают текущий вызов, когда DTE сбрасывает сигнал DTR (Data Terminal Ready/Готовность терминала данных). Если параметр “Drop DTR When

Hang Up" отмечен галочкой, Prestige в дополнение к команде отбоя "ATH" использует аппаратный сигнал для принудительного отбоя вызова устройством WAN.

7.12 Строки ответа

Строки ответа задают Prestige короткие сообщения или надписи, непосредственно предшествующие выводу различных параметров устройства WAN. Строки ответа не являются стандартными; следует проконсультироваться с документацией по используемому устройству WAN для определения соответствующих сообщений.

7.13 Конфигурирование дополнительных настроек модема

Для конфигурирования настроек модема для резервного соединения с WAN, щелкните **WAN**, **WAN Backup**, а затем кнопку **Advanced Setup**. В отобразившемся окне **Advanced Setup**, щелкните по кнопке **Edit** для вызова экрана **Advanced Modem Setup,** как показано ниже.

Для уточнения конкретных AT-команд см. инструкцию для Вашего устройства резервного соединения с WAN.

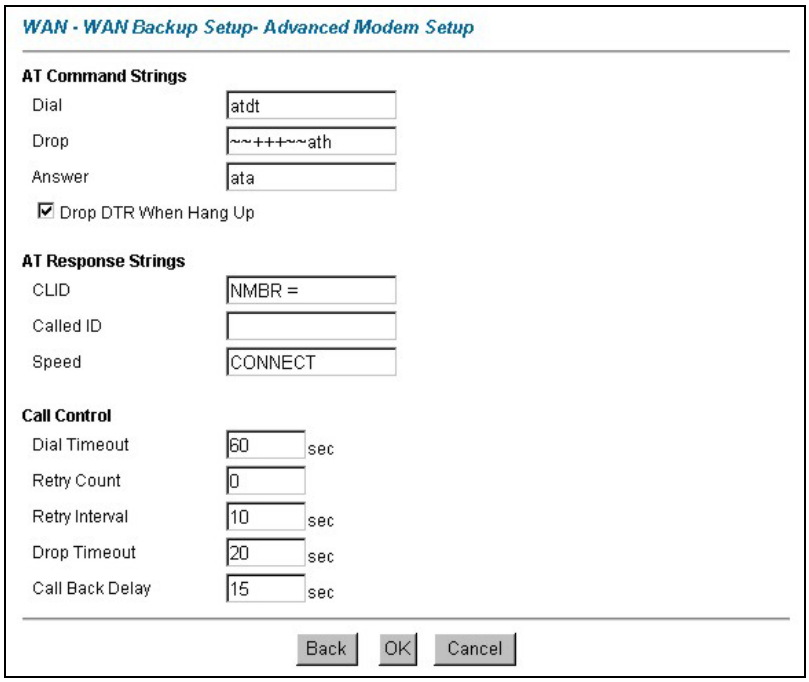


Рис. 7-7 Дополнительные настройки модема

В следующей таблице представлено описание полей данного экрана.

Табл. 7-4 Дополнительные настройки модема

ПОЛЕ	ОПИСАНИЕ
AT Command Strings (Строки AT-команд)	
Dial (Набор)	Введите строку AT-команды для осуществления вызова. Пример: atdt
Drop (Сброс)	Введите строку AT-команды для сброса вызова. "~" представляет ожидание в течение одной секунды, напр., "~~+++~~ath" может использоваться, если модем имеет низкую скорость отклика.
Answer (Ответ)	Введите строку AT-команды для ответа на вызов. Пример: ata

Табл. 7-4 Дополнительные настройки модема

ПОЛЕ	ОПИСАНИЕ
Drop DTR When Hang Up (Сброс DTR при снятии трубки)	Поставьте галочку в этом поле для сброса Prestige сигнала DTR (Data Terminal Ready/Готовность терминала данных) после отправки "AT Command String: Drop" .
AT Response Strings (Строки ответа AT)	
CLID	Введите ключевое слово, предшествующее CLID (Calling Line Identification/Идентификатор вызывающей линии) в строку ответа AT. Это позволяет Prestige собрать данные CLID в строку ответа AT, поступающие из устройства WAN. CLID требуется для аутентификации CLID. Пример: NMBR
Called ID (Идентификатор вызовов)	Введите ключевое слово, предшествующее набранному номеру.
Speed (Скорость)	Введите ключевое слово, предшествующее скорости соединения. Пример: CONNECT
Call Control (Управление вызовами)	
Dial Timeout (Задержка набора)	Введите время в секундах для того, чтобы Prestige попытался создать исходящий вызов до истечения времени. Пример: 60
Retry Count (Счетчик повторных попыток)	Введите число раз, которое Prestige снова будет пытаться набрать занятый или не отвечающий номер, прежде чем он будет внесен в черный список. Пример: 0
Retry Interval (Интервал повторных попыток)	Введите время в секундах для того, чтобы Prestige подождал перед повторной попыткой совершить звонок после сбоя. Используется до того, как номер помещен в черный список. Пример: 10
Drop Timeout (Задержка сброса)	Введите время в секундах для того, чтобы Prestige подождал перед сбрасыванием сигнала DTR, если он не получает положительное подтверждение об разъединении. Пример: 20

Табл. 7-4 Дополнительные настройки модема

ПОЛЕ	ОПИСАНИЕ
Call Back Delay (Задержка обратного вызова)	Введите время в секундах для того, чтобы Prestige подождал между сбросом запроса на обратный вызов и установлением соединения обратного вызова. Пример: 15
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
OK	Щелкните **OK** для возвращения к предыдущему окну, а затем щелкните **OK** для возвращения к следующему предыдущему окну и щелкните **Apply** для сохранения изменений.
Cancel (Отмена)	Щелкните **Cancel**, чтобы начать настройку заново.

Глава III:

NAT, динамический DNS и часовой пояс

В этой части описывается настройка NAT (Network Address Translation - Трансляция сетевых адресов), динамического DNS (Domain Name Server - Сервер имен доменов) а также настройку Времени и Даты.

Раздел 8
Окна настройки NAT (Трансляции сетевых адресов)

В данной главе описана настройка трансляции сетевых адресов (NAT) на Prestige.

8.1 Обзор трансляции сетевых адресов

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

8.1.1 Определения NAT

Внутренний/внешний означает местоположение хоста относительно Prestige, например, компьютеры Ваших абонентов являются внутренними хостами, тогда как web-серверы Интернет являются внешними хостами.

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

Следует отметить, что inside/outside относится к размещению хоста, а global/local к его IP-адресу, который используется в пакете. Таким образом, внутренний локальный адрес (ILA) - это IP-адрес внутреннего хоста в пакете, когда пакет находится в пределах локальной сети, тогда как внутренний глобальный адрес (IGA) - это IP-адрес того же внутреннего хоста, когда пакет находится в глобальной сети. В следующей таблице представлена данная информация в сжатом виде.

Табл. 8-1 Определения NAT

ПАРАМЕТР	ОПИСАНИЕ
Inside (Внутренний)	Относится к хосту локальной сети.
Outside (Внешний)	Относится к хосту глобальной сети.
Local (Локальный)	Относится к адресу пакета (источника или адресата) при пересылке пакета внутри локальной сети.

Global (Глобальный)	Относится к адресу пакета (источника или пункта назначения) при пересылке пакета по глобальной сети.

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

8.1.2 Что такое NAT

В простейшем случае NAT изменяет IP-адрес источника в пакете, принятом от абонента (внутренний локальный адрес) на другой (внутренний глобальный адрес) перед переадресацией пакета в глобальную сеть. При получении ответа, NAT переводит адрес назначения (внутренний глобальный адрес) обратно во внутренний локальный адрес перед переадресацией его исходному внутреннему хосту. Отметим, что IP-адрес (локальный или глобальный) внешнего хоста никогда не изменяется.

Глобальные IP-адреса внутренних хостов могут быть статическими или динамически назначаемыми Интернет-провайдером. Кроме того, Вы можете назначить серверы, например, web-сервер и сервер Telnet, находящиеся в Вашей локальной сети, и сделать их доступными для внешних пользователей.. Если Вы не назначаете серверы (для отображения "много-к-одному" и "много-ко-многим с перегрузкой" – см. *Табл. 8-2*), NAT предлагает дополнительное преимущество защиты брандмауэром. Если сервер не будет определен, все входящие запросы будут отфильтровываться Prestige, таким образом, предотвращается несанкционированный доступ в сеть. Дополнительные сведения о трансляции IP-адресов см. в *RFC 1631*, *"Трансляция сетевых IP-адресов (NAT)*".

8.1.3 Как функционирует NAT

Каждый пакет имеет два адреса – адрес источника и адрес назначения. Для исходящих пакетов, внутренний локальный адрес (ILA) является адресом источника в локальной сети, а внутренний глобальный адрес (IGA) - адресом источника в глобальной сети. Для входящих пакетов, ILA - это адрес назначения в локальной сети, а IGA - адрес назначения в глобальной сети. NAT преобразует частные (локальные) IP-адреса в уникальные глобальные, необходимые для связи с хостами других сетей. NAT заменяет исходный IP-адрес источника (и номера портов источника TCP или UDP для отображения Many-to-One (много-к-одному) и Many-to-Many Overload (много-ко-многим с перегрузкой) в каждом пакете и пересылает его в Интернет. Prestige сохраняет исходные адреса и номера портов, чтобы можно было восстановить исходные значения во входных ответных пакетах. Это иллюстрирует следующий рисунок.

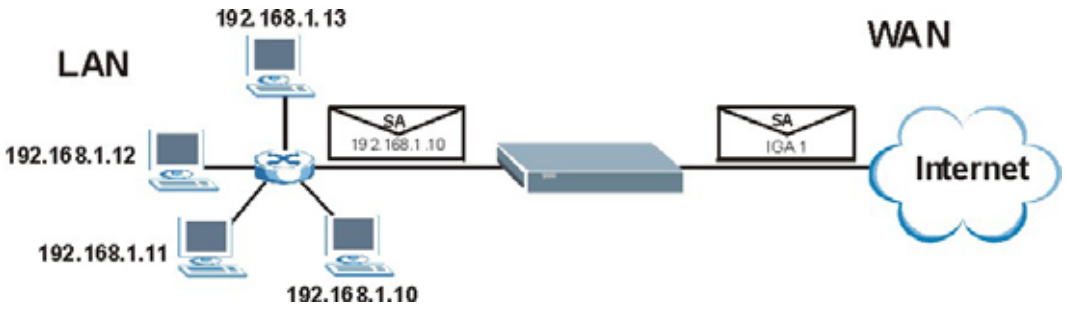


Рис. 8-1 Как функционирует NAT

8.1.4 Применение NAT

Следующий рисунок показывает возможное применение NAT, где три внутренних локальных сети (логические локальные сети, образованные при помощи псевдонимов IP), закрытые Prestige, могут взаимодействовать с тремя отдельными глобальными сетями. Другие примеры приведены в конце этой главы.

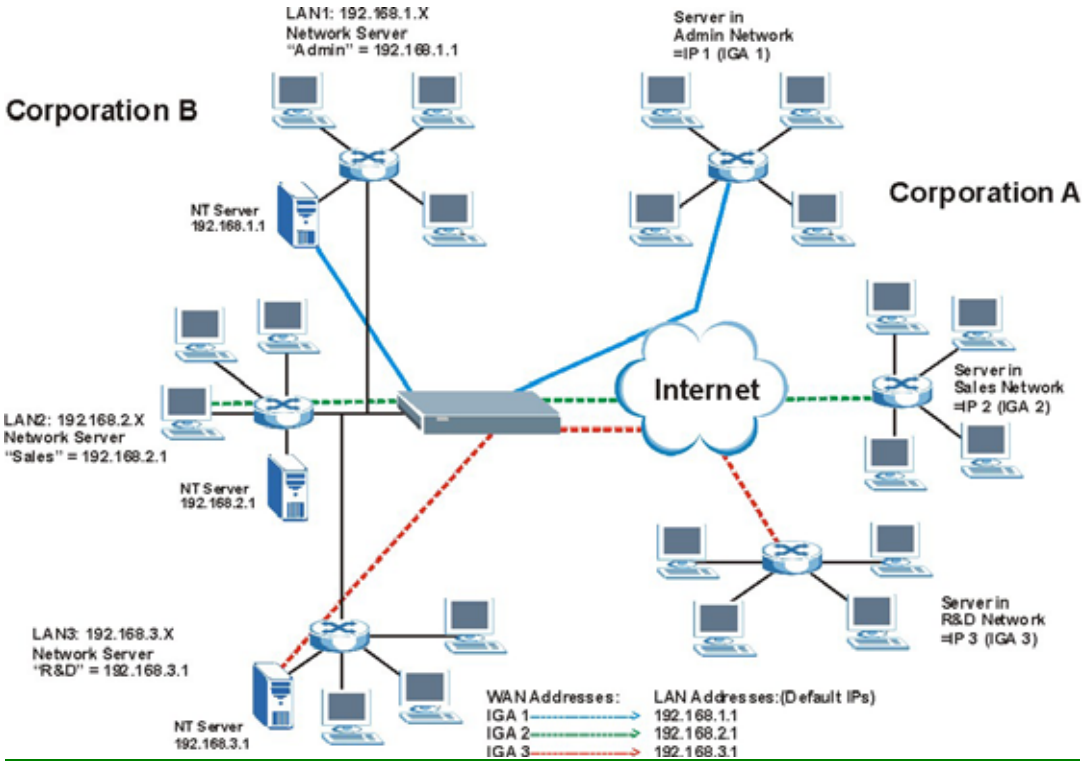


Рис. 8-2 Применение NAT с псевдонимами IP

8.1.5 Типы отображения NAT

NAT поддерживает пять типов отображения адресов IP - порт, а именно:

1. **One to One (один-к-одному)**: В режиме один-к-одному, Prestige преобразует один локальный IP-адрес в один глобальный IP-адрес.
2. **Many to One (много-к-одному)**: В режиме много-к-одному Prestige преобразует несколько локальных IP-адресов в один глобальный IP-адрес. Это эквивалент SUA (т. е., PAT - преобразование адресов портов), функциональной возможности получения учетной записи одиночного пользователя ZyXEL, которая поддерживалась в предыдущих моделях маршрутизаторов корпорации ZyXEL (опция **SUA Only (Только SUA)** в современных маршрутизаторах).
3. **Many to Many Overload (много-ко-многим с перегрузкой)**: В режиме много-ко-многим с перегрузкой, Prestige преобразует несколько локальных IP-адресов в общие глобальные IP-адреса.

4. **Many-to-Many No Overload (много-ко-многим без перегрузки)**: В режиме "много-ко-многим без перегрузки", Prestige преобразует каждый локальный IP-адрес в уникальный глобальный IP-адрес.
5. **Server (Сервер)**: Этот тип позволяет указать внутренние серверы различных служб, закрытые NAT, к которым предоставляется доступ для внешних пользователей.

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

В следующей таблице приведена обобщенная информация по этим типам.

Табл. 8-2 Типы отображения NAT

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

8.2 Сравнение SUA (Single User Account - учетная запись одиночного пользователя) и NAT

SUA (Single User Account - учетная запись одиночного пользователя) - это реализация в ZyNOS подмножества NAT, которая поддерживает два типа отображения, **много-к-одному** и **сервер**. Prestige 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. 8-2*.

1. **Выберите** SUA Only (Только SUA)**, если для Prestige установлено несколько общедоступных адресов глобальной сети.**

2. **Выберите** Full Feature (Полнофункциональная)**, если у Prestige существует несколько публичных IP-адресов в глобальной сети.**

8.3 Сервер SUA

Набор серверов SUA - это список внутренних (закрытых NAT в локальной сети LAN) серверов, например, web или FTP, которые можно сделать видимыми для внешних пользователей, несмотря на то, что SUA делает всю внутреннюю сеть видимой для внешних пользователей как один компьютер.

Вы можете задать один номер порта или диапазон номеров для пересылки, а также локальный IP-адрес требуемого сервера. Номер порта идентифицирует услугу; например, служба web занимает порт 80, а FTP - порт 21. В некоторых случаях, когда служба неизвестна или один сервер поддерживает более одной службы (например, FTP и служба web), возможно будет лучше указать диапазон номеров портов. Вы можете назначить IP-адрес сервера, соответствующий одному порту или набору 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 по умолчанию

Кроме серверов определенных видов служб NAT поддерживает IP-адрес сервера по умолчанию. Сервер по умолчанию принимает пакеты от портов, не указанных в этом окне.

Если Вы не назначили IP-адрес в Server Set 1 (сервер по умолчанию), все пакеты, полученные для портов, не указанных в этом пункте, или в remote management setup, будут сброшены.

8.3.1 Переадресация порта:услуги и номера портов

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

Табл. 8-3 Услуги и номера портов

УСЛУГА	НОМЕР ПОРТА
ECHO	7
FTP (Протокол передачи файлов)	21
SMTP (Простой протокол пересылки почты)	25

Табл. 8-3 Услуги и номера портов

УСЛУГА	НОМЕР ПОРТА
DNS (Служба имен доменов)	53
Finger	79
HTTP (Протокол передачи гипертекста или WWW - "всемирная паутина")	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

8.3.2 Конфигурирование серверов, закрытых SUA (пример)

Предположим, Вы хотите назначить порты 21-25 одному FTP,Telnet и SMTP серверу (A в примере), а порт 80 - другому серверу (B в примере), а также назначать IP-адрес сервера по умолчанию 192.168.1.35 третьему (C в примере). Вы назначаете IP адреса для локальной сети и провайдер выделяет IP адрес подключения к Интернет (WAN), как показано на следующем рисунке. Сеть с использованием NAT отображается в Интернет как один хост.

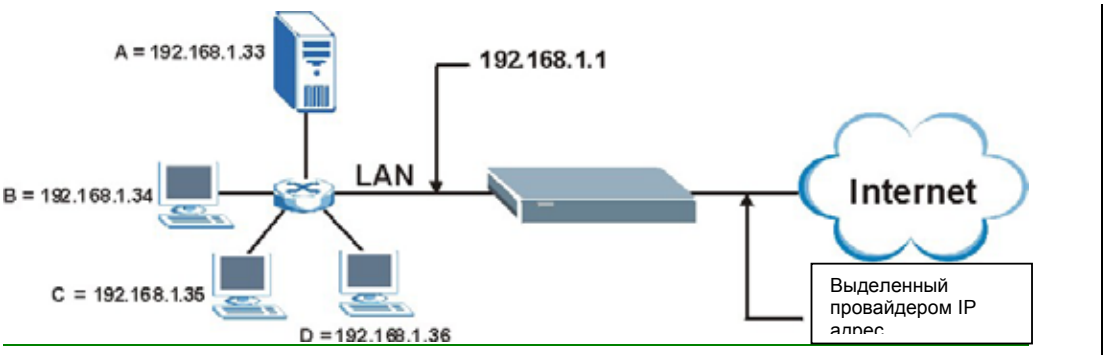


Рис. 8-3 Пример множества серверов, закрытых NAT

8.4 Выбор режима NAT

Чтобы направить трафик от глобальной сети через Prestige, необходимо, в дополнение к SUA/NAT, установить правила межсетевой защиты.

Для перехода к следующему окну щелкните на **NAT**.

Рис. 8-4 Окно NAT Mode

Следующая таблица описывает поля на этом экране.

Таблица 8-4 Окно NAT Mode

ПОЛЕ	ОПИСАНИЕ
None (Нет)	Выберите этот режим для отключения NAT.
SUA Only (Только SUA)	Выберите этот режим, если Вам выделен только один публичный IP-адрес в глобальной сети для Prestige. Prestige использует набор № 1 отображения адресов (Address Mapping Set 1) в окне **NAT - Edit SUA NAT Server Set**.
Edit Details (Подробное редактирование)	Щелкните по этой ссылке, чтобы перейти к экрану **NAT - Edit SUA NAT Server Set**.
Full Feature (Все функции)	Выберите этот режим, если у Prestige существует только один публичный IP-адрес в глобальной сети.
Edit Details (Подробное редактирование)	Щелкните по этой ссылке, чтобы открыть окно правил отображения адресов (**NAT - Address Mapping Rules**).
Apply (Применить)	Щелкните на кнопке **Apply**, чтобы сохранить конфигурацию.

8.5 Конфигурирование сервера SUA

Если Вы не назначили IP-адрес в Server Set 1 (сервер по умолчанию), все пакеты, полученные для портов, не указанных в этом пункте, или в remote management setup, будут сброшены.

Щелкните на **NAT**, выберите **SUA Only** и щелкните **Edit Details**, чтобы открыть следующее окно.

Номера портов, обычно используемых для конкретных служб, см. в *Табл. 8-2*.

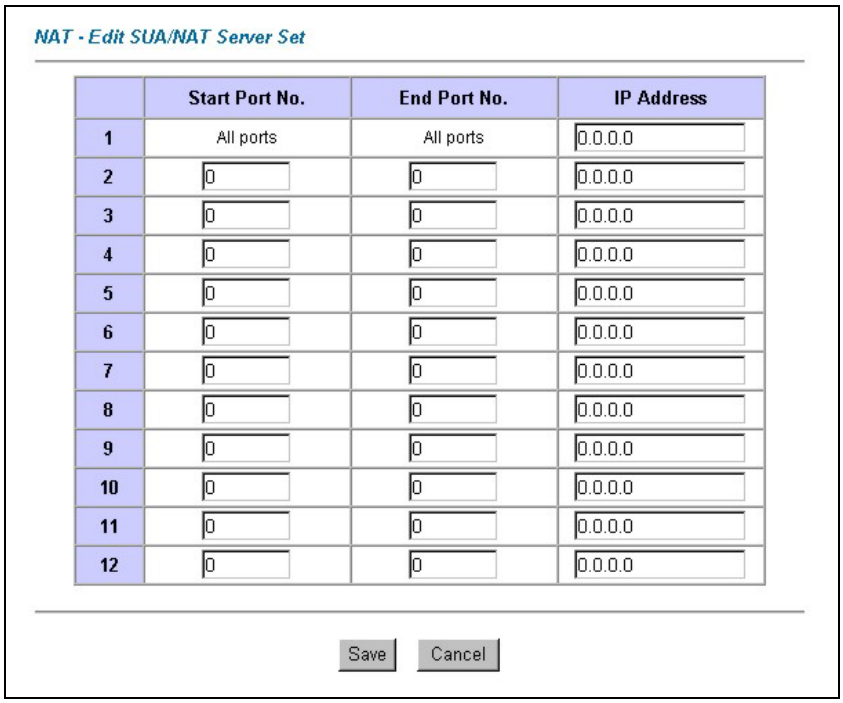


Рис. 8-5 Окно Edit SUA/NAT Server Set

В следующей таблице даны описания полей данного меню.

Таблица 8-5 Окно Edit SUA/NAT Server Set

ПОЛЕ	ОПИСАНИЕ

Таблица 8-5 Окно Edit SUA/NAT Server Set

ПОЛЕ	ОПИСАНИЕ
Start Port No. (Начальный номер порта)	Введите в данном поле номер порта. Для пересылки только одного порта, введите его номер еще раз в поле **End Port No (Конечный номер порта)**. Для пересылки набора последовательных портов, введите в этом поле начальный номер порта, а в поле **End Port No.** - конечный номер порта.
End Port No. (Конечный номер порта)	Введите в данном поле номер порта. Для пересылки только одного порта, введите его номер еще раз в расположенном выше поле **Start Port No.**, а затем еще раз введите его в этом поле. Для пересылки набора последовательных портов, введите в этом поле конечный номер порта в наборе, начинающемся с порта, номер которого указан в расположенном выше поле **Start Port No.**
Server IP Address (IP-адрес сервера)	Введите в этом поле IP-адрес сервера.
Save (Сохранить)	Щелкните на **Save** для сохранения настроек в Prestige.
Cancel (Отмена)	Щелкните на **Cancel**, чтобы вернуться к предыдущей конфигурации.

8.6 Конфигурирование преобразований адресов

Упорядочивание правил имеет большое значение, поскольку Prestige применяет правила в указанном Вами порядке. Когда текущий пакет подпадает под правило, Prestige производит соответствующие действия и прекращает обработку остальных правил. Если перед очередным заданным правилом имеются пустые, то это правило сдвигается на соответствующее количество пустых номеров. Например, если Вы уже задали правила с 1 по 6 в текущем наборе, а теперь зададите правило номер 9, в окне сводки набора правил новое правило будет иметь номер 7, а не 9. Если теперь Вы удалите правило номер 4, правила с 5 по 7 сдвинутся вверх на одно правило, и старые правила 5, 6 и 7 станут новыми правилами 4, 5 и 6.

Для изменения настроек преобразования адресов в Prestige щелкните на **NAT**, выберите **Full Feature** и щелкните на ссылке **Edit Details**, чтобы открыть следующее окно.

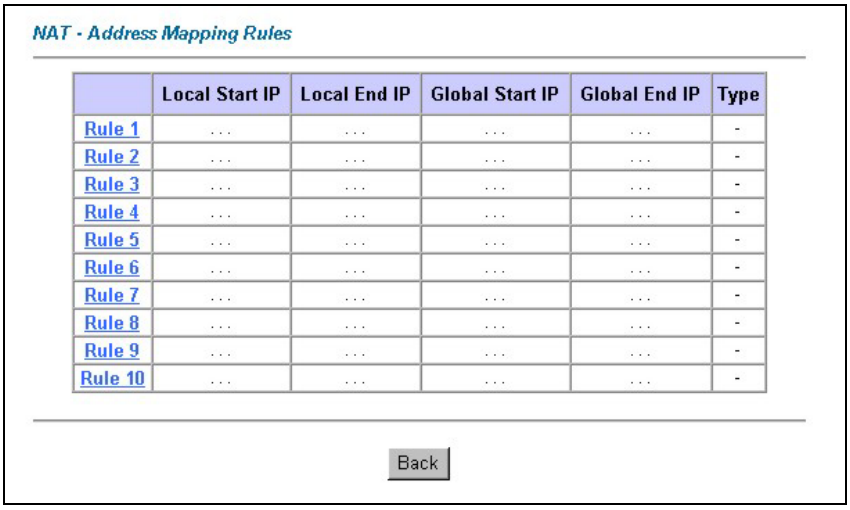


Рис. 8-6 Правила отображения адресов

В следующей таблице даны описания полей данного меню.

Табл. 8-6 Правила отображения адресов

ПОЛЕ	ОПИСАНИЕ
Local Start IP (Начальный локальный IP)	Это начальный внутренний локальный IP-адрес (ILA). Локальные IP-адреса для отображения порта **Server** недоступны (**N/A**).
Local End IP (Конечный локальный IP-адрес)	Это конечный внутренний локальный IP-адрес (ILA). Если правило действует для всех локальных IP-адресов, это поле отображает 0.0.0.0 в поле адреса **Local Start IP** и 255.255.255.255 в поле адреса **Local End IP**. Это поле отображает **N/A** (Недоступно) для типов **One-to-one** (один-к-одному) и **Server** (сервер).
Global Start IP (Начальный глобальный IP-адрес)	Это начальный внутренний глобальный IP-адрес (IGA). Введите в этом поле 0.0.0.0, если от Интернет-провайдера получен динамический IP-адрес. Это возможно только для типов **Many-to-One** (много-к-одному) и **Server** (сервер).
Global End IP (Конечный глобальный IP-адрес)	Это конечный внутренний глобальный IP-адрес (IGA). Это поле помечено **N/A** (Недоступно) для типов **One-to-one** (один-к-одному), **Many-to-One** (много-к-одному) и **Server** (сервер).

Табл. 8-6 Правила отображения адресов

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	**1-1**: В режиме один-к-одному один локальный IP-адрес преобразуется в один глобальный IP-адрес. Следует отметить, что при использовании типа преобразования One-to-One номера портов не меняются. **M-1**: В режиме много-к-одному несколько локальных IP-адресов преобразуются в один глобальный IP-адрес. Это эквивалентно SUA (т.е. PAT - трансляция адреса порта), функции "получение учетной записи одиночного пользователя", разработанной корпорацией ZyXEL, которая поддерживалась предыдущими версиями маршрутизаторов ZyXEL. **M-M Ov** (Overload): В этом режиме несколько локальных IP-адресов преобразуются в коллективные глобальные IP-адреса. **MM No** (No Overload): В этом режиме каждый локальный IP-адрес преобразуется в уникальный глобальный IP-адрес. **Server**: Этот режим позволяет назначить внутренние серверы различного типа в обход NAT и открыть к ним доступ со стороны внешнего мира.
Back (Назад)	Щелкните на кнопке **Back**, чтобы перейти к окну **NAT Mode**.

8.7 Редактирование правил преобразования адресов

Для редактирования правила преобразования адресов щелкните на ссылке на правило в окне **NAT Address Mapping Rules**, чтобы открыть следующее ниже окно.

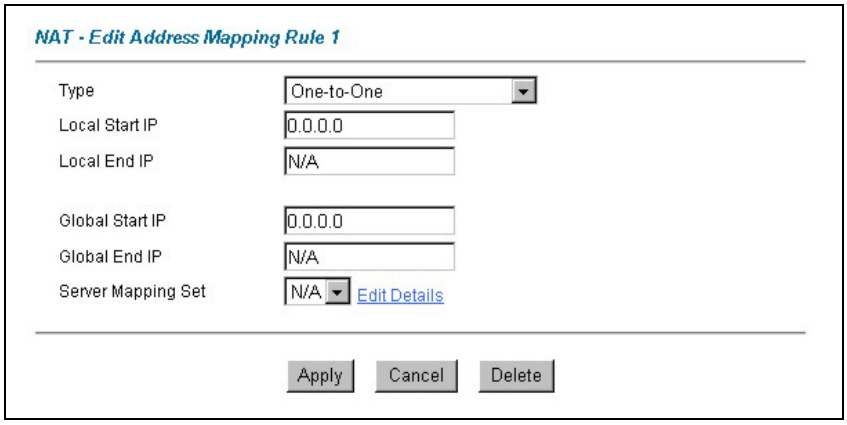


Рис. 8-7 Окно Address Mapping Rule Edit

В следующей таблице даны описания полей данного меню.

Таблица 8-7 Окно Address Mapping Rule Edit

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	Выберите один из следующих типов преобразования портов. 1. **One to One (один-к-одному)**: В режиме один-к-одному один локальный IP-адрес преобразуется в один глобальный IP-адрес. Следует отметить, что при использовании типа преобразования One-to-One номера портов не меняются. 2. **Many to One (много-к-одному)**: В режиме много-к-одному несколько локальных IP-адресов преобразуются в один глобальный IP-адрес. Это эквивалентно SUA (т.е. PAT - трансляция адреса порта), функции "получение учетной записи одиночного пользователя", разработанной корпорацией ZyXEL, которая поддерживалась предыдущими версиями маршрутизаторов ZyXEL. 3. **Many to Many Overload (много-ко-многим с перегрузкой)**: В этом режиме несколько локальных IP-адресов преобразуются в коллективные глобальные IP-адреса. 4. **Many to Many No Overload (много-ко-многим без перегрузки)**: В этом режиме каждый локальный IP-адрес преобразуется 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.
Local Start IP (Начальный локальный IP)	Это начальный локальный IP-адрес (ILA). Локальные IP-адреса для отображения порта **Server** недоступны (**N/A**).
Local End IP (Конечный локальный IP-адрес)	Это начальный локальный IP-адрес (ILA). Если данное правило действительно для всех локальных IP-адресов, введите 0.0.0.0 в поле адреса **Local Start IP** и 255.255.255.255 в поле адресе **Local End IP**. Это поле помечено **N/A** (Недоступно) для типов **One-to-one** (один-к-одному) и **Server** (сервер).
Global Start IP (Начальный глобальный IP-адрес)	Это начальный глобальный IP-адрес (IGA). Введите в этом поле 0.0.0.0, если от Интернет-провайдера получен динамический IP-адрес.
Global End IP (Конечный глобальный IP-адрес)	Это конечный глобальный IP-адрес (IGA). Это поле помечено **N/A** (Недоступно) для типов **One-to-one** (один-к-одному), **Many-to-One** (много-к-одному) и **Server** (сервер).

Server Mapping Set (Набор отображения серверов)	Доступно, только если поле **Type (Тип)** имеет значение **Server (Сервер)**. Выбрав число из раскрывающегося меню, выберите сервер из окна **NAT - Address Mapping Rules**.
Edit Details (Подробное редактирование)	Щелкните по этой ссылке, чтобы перейти к окну **NAT - Edit SUA NAT Server Set**, для редактирования настроек серверов, которые Вы выбрали в поле Server Mapping Set.
Apply (Применить)	Щелкните на **Apply** для сохранения настроек в Prestige.
Cancel (Отмена)	Щелкните на **Cancel**, чтобы вернуться к ранее сохраненным настройкам.
Удалить	Щелкните на **Delete**, чтобы выйти из окна без сохранения настроек

Раздел 9
Настройка динамического DNS

В этой главе обсуждается конфигурирование Prestige для использования динамической DNS (службы имен доменов).

9.1 Динамическая служба имен доменов (Dynamic DNS)

Динамическая DNS (Domain Name System - Служба имен доменов)делает возможным обновление текущего динамического IP-адреса одной или несколькими службами динамического DNS, чтобы любой мог связаться с Вами (через NetMeeting, CU-SeeMe и т. д.). Вы также можете получить доступ к своему серверу FTP или web-сайту на своем собственном компьютере, используя доменное имя (например, myhost.dhs.org, где myhost является любым именем на Ваш выбор), который никогда не изменится, вместо использования IP-адреса, который изменяется при каждом подключении. Ваши друзья и родственники всегда смогут связаться с Вами, даже если они не знают Вашего IP-адреса.

Прежде всего, Вам 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 службы динамического DNS выдает пароль или ключ.

9.1.1 Шаблоны DYNDNS

Включение функции шаблонов приводит к тому, что адреса вида *.yourhost.dyndns.org привязываются к тому же IP-адресу, что и yourhost.dyndns.org. Данная функция полена, если Вы хотите иметь возможность использовать, например, адрес www.yourhost.dyndns.org и при этом попадать на Ваш хост.

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

9.2 Конфигурирование динамического DNS

Для изменения Вашего Prestige DDNS, щелкните на **Dynamic DNS**. На экране появится следующее окно.

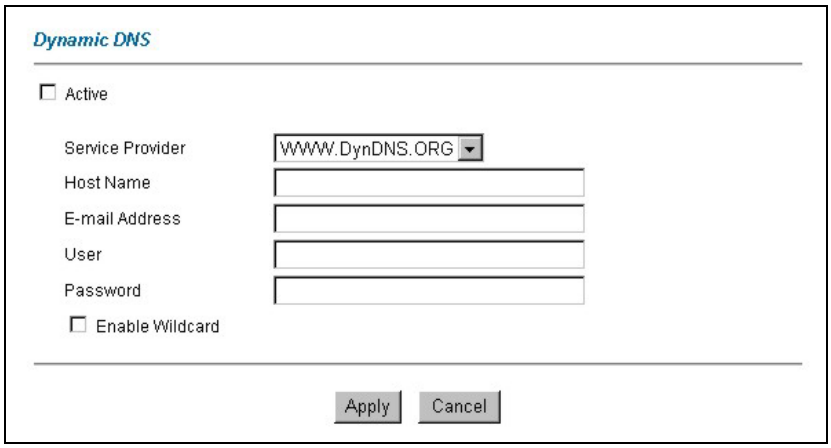


Рис. 9-1 Окно DDNS

В следующей таблице даны описания полей данного меню.

Таблица 9-1 Окно DDNS

ПОЛЕ	ОПИСАНИЕ
Active (Активно)	Поставьте флажок в этом окошке, чтобы использовать динамический DNS.
Service Provider (Провайдер услуг)	Это имя вашего провайдера услуг динамического DNS.
Host Names (Имена хостов)	Введите имя домена, назначенного Prestige провайдером услуг динамического DNS.
E-mail Address (адрес электронной почты)	Введите адрес Вашей электронной почты.
User (Пользователь)	Введите Ваше имя пользователя.
Password (Пароль)	Введите назначенный Вам пароль.
Enable Wildcard (Включить шаблоны)	Поставьте флажок в этом окошке, чтобы разрешить использование шаблонов DYNDNS.
Apply (Применить)	Щелкните на **Apply** для сохранения настроек в Prestige.
Cancel (Отмена)	Щелкните на **Cancel** чтобы начать конфигурировать это окно сначала.

Раздел 10
Время и дата (Часовой пояс)

Это окно доступно не на всех моделях. Это окно следует использовать для конфигурирования настроек времени суток и даты Prestige.

10.1 Конфигурирование времени и даты

Для изменения времени суток и даты в Prestige щелкните на **Time And Date**. На экране появится изображенное ниже окно. Используйте это окно для настройки системного времени Prestige в соответствии с Вашим часовым поясом.

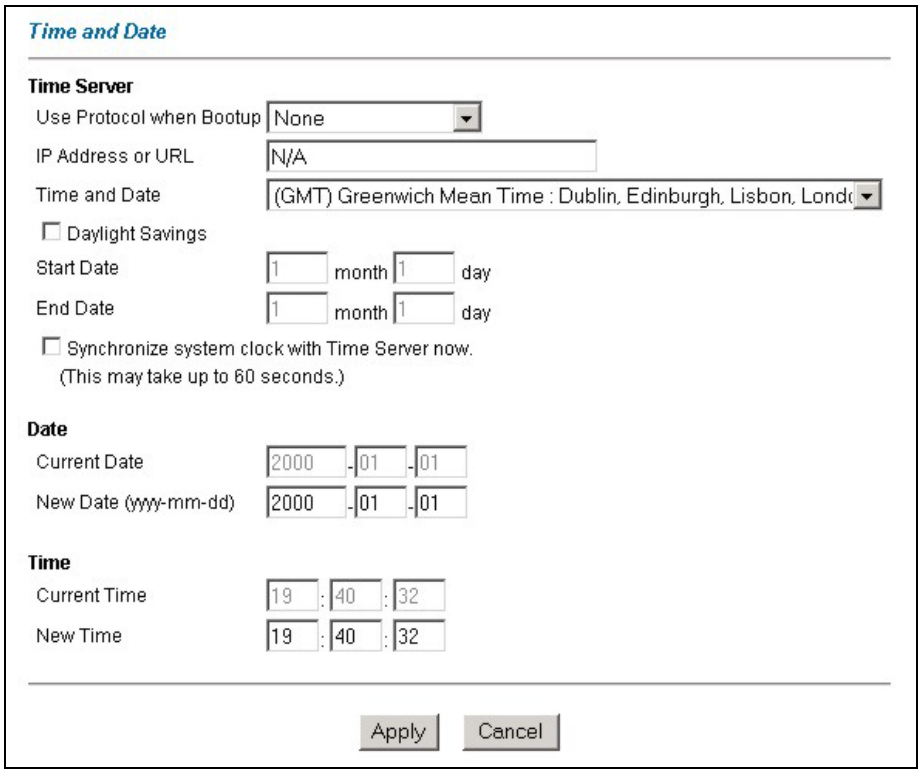


Рис. 10-1 Окно Time and Date

В следующей таблице даны описания полей данного меню.

Таблица 10-1 Окно Time and Date

ПОЛЕ	ОПИСАНИЕ
Time Server (Сервер времени)	
Use Protocol when Bootup (Использовать протокол сервиса времени при запуске)	Выберите протокол сервиса времени, который Ваш сервер времени посылает при включении Prestige. Не каждый сервер времени поддерживает все протоколы, поэтому следует сначала проконсультироваться с Интернет-провайдером/сетевым администратором или попытаться определить работающий протокол методом проб и ошибок. Основное различие между ними заключается в формате. Формат **Daytime (RFC 867)**: день/месяц/год/часовой пояс сервера. Формат **Time (RFC 868)** выдает 4-байтовое целое число, соответствующее полному числу секунд, прошедших с момента 00:00:00 01.01.1970. Формат по умолчанию, **NTP (RFC 1305)**, подобен формату Time (RFC 868). Выберите **None** для ввода времени и даты вручную.
IP Address or URL (IP-адрес или ссылка)	Введите IP-адрес или URL(ссылку) сервера времени. Если Вы не располагаете точной информацией, обратитесь к Интернет-провайдеру или системному администратору (адрес по умолчанию - tick.stdtime.gov.tw).
Time and Date (Часовой пояс)	Выберите свой часовой пояс. Это определит разницу во времени между Вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time, GMT).
Daylight Savings (Летнее время)	Выберите эту опцию, если Вы используете летнее время. Летнее время - это период с поздней весны до ранней осени, когда во многих странах стрелки часов переводятся на час вперед, чтобы добавить час светлого времени суток.
Start Date (Дата начала)	Если в окошке **Daylight Saving** стоит флажок, введите месяц и день начала действия летнего времени.
End Date (Дата окончания)	Если в окошке **Daylight Saving** стоит флажок, введите месяц и день окончания действия летнего времени.
Syncronize system clock with Time Server now (Установить системные часы по серверу времени)	Выберите этот пункт, чтобы Prestige установил по серверу времени (сконфигурированному Вами выше) свои внутренние системные часы. Пожалуйста подождите 60с пока Prestige обнаружит сервер времени. Если Prestige не сможет обнаружить сервер времени, пожалуйста, проверьте протокол сервера времени и его IP адрес. Если IP адрес был введен правильно, попытайтесь, например, выполнить команду ping для тестирования соединения.
Date (Дата)	
Current Date (Текущая дата)	В этом поле отображается дата, установленная в Prestige. При каждой перезагрузке этой страницы Prestige синхронизирует время с сервером времени.

Таблица 10-1 Окно Time and Date

ПОЛЕ	ОПИСАНИЕ
New Date (Новая дата в формате гггг-мм-дд)	В этом поле отображается последняя обновленная по серверу времени дата. Если Вы выбрали **None** в поле **Use Protocol when Bootup**, введите в этом поле новую дату и щелкните на **Apply**.
Time (Время)	
Current Time (Текущее время)	В этом поле отображается время, установленное в Prestige. При каждой перезагрузке этой страницы Prestige синхронизирует время с сервером времени.
New Time (Новое время)	В этом поле отображается последнее обновленное по серверу времени время. Если в поле **Use Protocol when Bootup** Вы выбрали **None**, введите в этом поле новое время и щелкните на **Apply**.
Apply (Применить)	Щелкните на **Apply** для сохранения настроек в Prestige.
Cancel (Отмена)	Щелкните на **Cancel** чтобы начать конфигурировать это окно сначала.

Глава IV:

Межсетевой экран и Контент-фильтр

В этой части содержится обзор различных типов межсетевых экранов и межсетевого экрана серии Prestige. Также рассматриваются пользовательские услуги, журнальные регистрации, представлены примеры правил межсетевого экрана и обзор контент-фильтрования.

Раздел 11
Межсетевые экраны

В этой части дается вводная информация о межсетевых экранах и ознакомление с межсетевым экраном серии Prestige.

11.1 Описание межсетевого экрана

Первоначально, происхождение термина *firewall* (дословно - "огненная стена") относится к строительному сооружению, предназначенному для предотвращения распространения огня из одного помещения в другое. В сетевой технике “firewall” приобрел значение “межсетевой экран”, под которым понимается система или группа систем, осуществляющих стратегию управления доступом между двумя сетями. Он также может быть определен как механизм, используемый для защиты безопасной сети от небезопасной сети. Безусловно, межсетевые экраны не могут разрешить все проблемы безопасности. Межсетевой экран является *одним* из механизмов, используемых с целью установления периметра сетевой безопасности для поддержки стратегии безопасности сети. Он никогда не будет *единственным* используемым механизмом или методом. Для того, чтобы межсетевой экран эффективно защищал, необходимо разработать и применить его соответствующим образом. Это требует объединения межсетевого экрана со всей стратегией информационной безопасности. Кроме того, определенные стратегии должны быть установлены в самом межсетевом экране.

11.2 Типы межсетевых экранов

Существует три основных типа межсетевых экранов:

1. Межсетевые экраны фильтрации пакетов
2. Межсетевые экраны прикладного уровня
3. Межсетевые экраны полнофункционального контроля

11.2.1 Межсетевые экраны фильтрации пакетов

Межсетевые экраны фильтрации пакетов ограничивают доступ, основанный на адресе отправитель/получатель пакета компьютерной сети и типе приложения.

11.2.2 Межсетевые экраны прикладного уровня

Межсетевые экраны прикладного уровня ограничивают доступ, используя в качестве proxy-серверов внешние серверы. Так как они используют программы, написанные для определенных Интернет услуг, таких как HTTP, FTP и telnet, они могут оценивать сетевые пакеты относительно достоверности данных, связанных с конкретным приложением. Шлюзы прикладного уровня имеют множество основных преимуществ перед режимом по умолчанию, допускающим поступление трафика непосредственно ко внутренним хостам:

i. Сокрытие информации препятствует узнаванию имен внутренних систем через DNS внешними системами, так как прикладные шлюзы представляют собой единственный хост, чье имя должно стать известным для внешних систем.

ii. Надежная аутентификация и журнальная регистрация ранее проверенного в подлинности трафика прикладного уровня, до того, как он достигнет внутреннего хоста, осуществляют защиту более эффективно, чем если бы она выполнялась с использованием стандартной регистрации хоста. Правила фильтрации при фильтрации пакетов маршрутизатора могут быть менее сложными, чем они могли бы быть, если бы маршрутизатору требовалось отфильтровать трафик прикладного уровня и направить его ко множеству конкретных систем. Маршрутизатору требуется только пропускать трафик прикладного уровня, адресованный прикладному шлюзу, и отбрасывать остальное.

11.2.3 Межсетевые экраны полнофункционального контроля

Межсетевые экраны полнофункционального контроля ограничивают доступ при помощи экранирования пакетов данных от определенных правил доступа. Они принимают решения об управлении доступом на основе IP-адреса и протокола. Они также "контролируют" данные сеанса связи для обеспечения целостности соединения и настройки динамического протокола. Эти межсетевые экраны в целом обеспечивают лучшую скорость и прозрачность, однако, они могут испытывать проблемы с детальностью управления доступом прикладного уровня или кэшированием, поддерживаемым некоторыми proxy-серверами. Для получения более подробной информации о полнофункциональном контроле см. *Раздел 11.5*.

Межсетевые экраны того или другого типа, становятся неотъемлемой частью стандартных решений безопасности для учреждений.

11.3 Введение в межсетевой экран корпорации ZyXEL

Межсетевой экран Prestige представляет собой межсетевой экран полнофункционального контроля, предназначенный, при его активации (в меню SMT 21.2 или в Web-конфигураторе), для защиты от атак *Отказ от обслуживания*. Целью Prestige является обеспечение безопасного подключения Локальной вычислительной сети (LAN) к Интернету. Prestige может использоваться для

предотвращения хищений, разрушения и модификации данных, а также для ведения записей журналов регистрации, которые могут быть необходимы для обеспечения безопасности сети. Prestige имеет также возможности фильтрации пакетов.

Prestige устанавливается между LAN и Интернетом. Это позволяет ему выступать в качестве шлюза системы безопасности для всех пересылаемых между Интернетом и LAN данных.

Prestige имеет один порт ISDN и один порт LAN Ethernet, которые физически разделяют сеть на две области.

- Порт ISDN подключается к Интернету.
- Порт LAN (Local Area Network/Локальная вычислительная сеть) подключается к сети компьютеров, которым необходима защита от внешнего мира. Эти компьютеры получают доступ к Интернет услугам, таким как электронная почта (e-mail), FTP, и “World Wide Web“. Однако, “входящий доступ” не будет позволен, если не сконфигурировано удаленное управление или не создано правило межсетевого экрана, позволяющее удаленному хосту использовать конкретную службу.

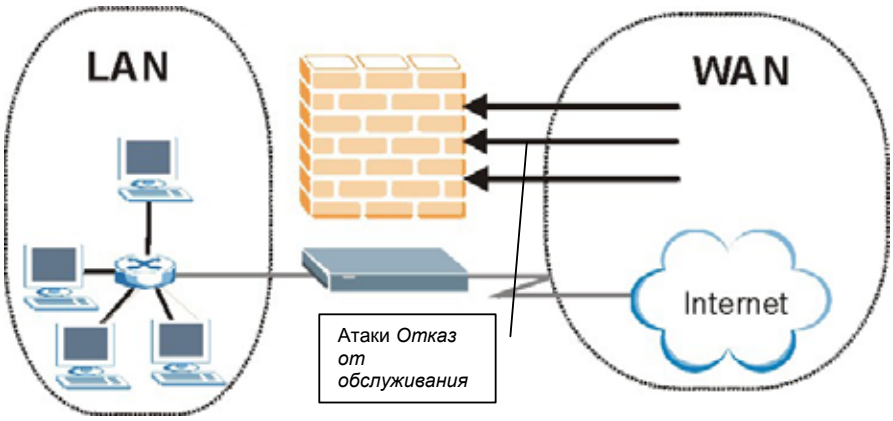


Рис. 11-1 Применение межсетевого экрана Prestige

11.4 Отказ от обслуживания

Атаки типа *Отказ от обслуживания* (DoS) направлены на устройства и сети, подключенные к Интернету. Их цель не украсть информацию, а отключить устройство или сеть с тем, чтобы

пользователи не могли больше иметь доступ к сетевым ресурсам. Prestige изначально сконфигурирован для автоматического обнаружения и предотвращения всех известных атак DoS.

11.4.1 Основы

Компьютеры рассылают информацию по Интернету, используя простой язык, называемый TCP/IP. TCP/IP, в свою очередь, является набором протоколов прикладного уровня, которые выполняют определенные функции. “Добавочный номер”, называемый "порт TCP" или "порт UDP" идентифицирует эти протоколы, а именно HTTP (Web), FTP (File Transfer Protocol/Протокол передачи файлов), POP3 (E-mail) и т.д. Напр., Web-трафик по умолчанию использует порт 80 TCP.

Когда компьютеры устанавливают связь с Интернетом, они используют модель клиент/сервер, где сервер "прослушивает" конкретный порт TCP/UDP относительно запросов информации с компьютеров удаленных клиентов в сети. Напр., Web-сервер типично прослушивает порт 80. Следует отметить, что хотя компьютер может быть предназначен для использования всего через один порт типа Web, другие порты также активны. Если конфигурирование или управление компьютером происходит неаккуратно, хакер может атаковать его через незащищенный порт.

Некоторые из наиболее распространенных IP-портов следующие:

Табл. 11-1 Распространенные IP-порты

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

11.4.2 Типы атак DoS

Существует четыре типа атак DoS:

1. Атаки, использующие ошибки в реализации TCP/IP.
2. Атаки, использующие слабости в спецификации TCP/IP.
3. Грубые атаки, заполняющие сеть неиспользуемыми данными.
4. Ложный IP-адрес.

1. Атаки"**Ping of Death**" и "**Teardrop**" используют ошибки в реализациях TCP/IP различных компьютеров и хост-систем.

1-a Атака Ping of Death использует утилиту "эхо-тестирование" для создания пакета IP, превышающего максимальное значение данных в 65536 байт, допущенных спецификацией IP. Затем этот огромный пакет посылается в ничего не подозревающую систему. Происходит ее полный отказ, зависание или перезагрузка.

1-b Атака Teardrop использует слабости в перекомпоновке фрагментов пакета IP. Поскольку данные передаются через сеть, пакеты IP часто разбиваются на более мелкие порции. Каждый фрагмент выглядит как исходный пакет IP, за исключением того, что он содержит поле смещения, которое выражает, напр., "Данный фрагмент переносит 200 байт начиная с 400 исходного (не фрагментированного) пакета IP". Программа Teardrop создает серии фрагментов IP с перекрыванием полей смещения. Когда эти фрагменты снова собираются в пункте назначения, некоторые системы полностью отказывают, зависают или перезагружаются.

2. Слабости в спецификации TCP/IP оставляют ее открытой для атак "**SYN Flood**" и "**LAND**". Эти атаки реализуются на этапе квитирования установления связи, инициирующего сеанс связи между двумя приложениями.

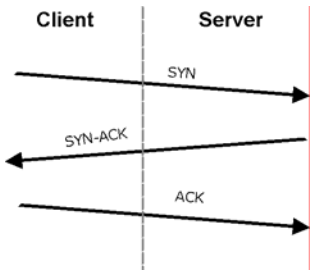


Рис. 11-2 Трехстороннее квитирование

При нормальных обстоятельствах, приложение, которое инициирует сеанс связи посылает пакет SYN (синхронизация) на принимающий сервер. Приемник отправляет назад пакет ACK (уведомление) и свой собственный SYN, а затем инициатор отвечает ACK (уведомление). После этого квитирования устанавливается соединение.

2-a Атака **SYN Attack** заполняет атакуемую систему серией пакетов SYN. Каждый пакет побуждает атакуемую систему выдавать ответ SYN-ACK. Пока атакуемая система ожидает ACK, которое следует за SYN-ACK, она отслеживает все ожидающие выполнения ответы SYN-ACK, известные как очередь журнала запросов. Очередь SYN-ACK сдвигается только тогда, когда приходит ответ ACK или когда внутренний таймер (который устанавливается на относительно длинные интервалы) прерывает трехстороннее квитирование. После того как очередь переполнена, система игнорирует все входящие запросы SYN, делая систему недоступной для легальных пользователей.

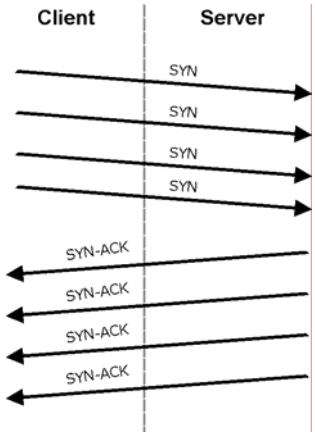


Рис. 11-3 Атака SYN Flood

2-b При атаке **LAND Attack** хакеры посылают пакеты SYN в сеть с ложным IP-адресом источника как у атакуемой системы. Это приводит к тому, что все выглядит так, как будто хост посылает пакеты самому себе, делая систему недоступной, в то время как атакуемая система пытается ответить самой себе.

3. **Грубая** атака типа атаки "Smurf", имеет целью функцию в спецификации IP, известную как целенаправленная или циркуляционная рассылка для подсети для быстрого заполнения атакуемой сети неиспользуемой информацией. Хакер Smurf заполняет маршрутизатор с протоколом (Internet Control Message Protocol/Протокол управляющих сообщений в сети Интернет) (ICMP) пакетами эхо-запросов (эхо-тестирование). Так как IP-адрес назначения каждого пакета представляет собой широковещательный адрес сети, маршрутизатор будет передавать пакет отклика ICMP запроса всем хостам в сети. Если существует множество хостов, это создаст большое количество трафика откликов ICMP на запросы и ответы. Если хакер выбирает ложный IP-адрес источника пакета отклика ICMP на запрос, итоговый трафик ICMP не только закупорит "промежуточную" сеть, но также перегрузит сеть ложного IP-адреса источника, известного как "жертвенная" сеть. Это затопление трафиком широковещательной рассылки забирает всю доступную пропускную способность, делая связь невозможной.

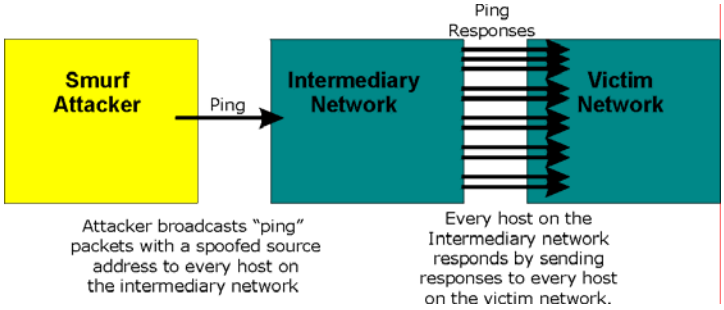


Рис. 11-4 Атака Smurf

- Уязвимость ICMP

ICMP - это сообщающий об ошибке протокол, работающий во взаимодействии с IP. Следующие типы ICMP предупреждают об опасности:

Табл. 11-2 Команды ICMP, предупреждающие об опасности

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Недопустимые команды (NetBIOS и SMTP)

Единственно допустимыми командами NetBIOS являются следующие - все остальные недопустимые.

Табл. 11-3 Допустимые команды NetBIOS

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

Все команды SMTP являются недопустимыми, за исключением команд, отображенных в следующей таблице.

Табл. 11-4 Допустимые команды SMTP

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

- Traceroute

Traceroute - это утилита, используемая для определения траектории пакета перемещающегося между двумя оконечными точками. Иногда, когда фильтр пакетов межсетевого экрана сконфигурирован неправильно, злоумышленник может отследить путь за межсетевым экраном, получая сведения о топологии сети за межсетевым экраном.

4. Часто, многие атаки DoS также применяют, как часть своей атаки метод, известный как "**IP Spoofing**" (ложный IP-адрес). Ложный IP-адрес может использоваться для вторжения в системы, с целью сокрытия подлинности хакера или усиления эффекта атаки DoS. Ложный IP-адрес это способ, используемый для получения неправомочного доступа к компьютерам путем обмана маршрутизатора или межсетевого экрана, заставляя его полагать, что связь происходит через правомочную сеть. Для включения ложного IP-адреса, хакеру необходимо изменить заголовок пакета, чтобы это выглядело так, как будто пакеты исходят из доверенного хоста и доступ через маршрутизатор или межсетевой экран будет разрешен. Prestige блокирует все попытки получения доступа обманным путем с использованием ложного IP-адреса.

11.5 Полнофункциональный контроль

При полнофункциональном контроле, поля пакетов сопоставляются с пакетами, которые уже известны как правомочные. Напр., если Вы имеете доступ к внешнему серверу, proxy-сервер запоминает подробности исходного запроса, такие как номер порта, отправитель и адреса назначения. Это “запоминание” называется *сохранение состояния.* Когда внешняя система отвечает на запрос, межсетевой экран сопоставляет полученные пакеты с сохраненным состоянием, чтобы определить позволен ли им доступ. Prestige использует полнофункциональный контроль пакетов для защиты частной LAN от хакеров и вандалов в Интернете. Установленный по умолчанию, полнофункциональный контроль Prestige допускает все средства связи в Интернете, которые исходят из LAN, и блокируют весь трафик в LAN, который исходит из Интернета. В итоге полнофункциональный контроль:

- Допускает все сеансы связи, исходящие из LAN (локальная сеть) в WAN (Интернет).
- Отвергает все сеансы связи, исходящие из WAN в LAN.

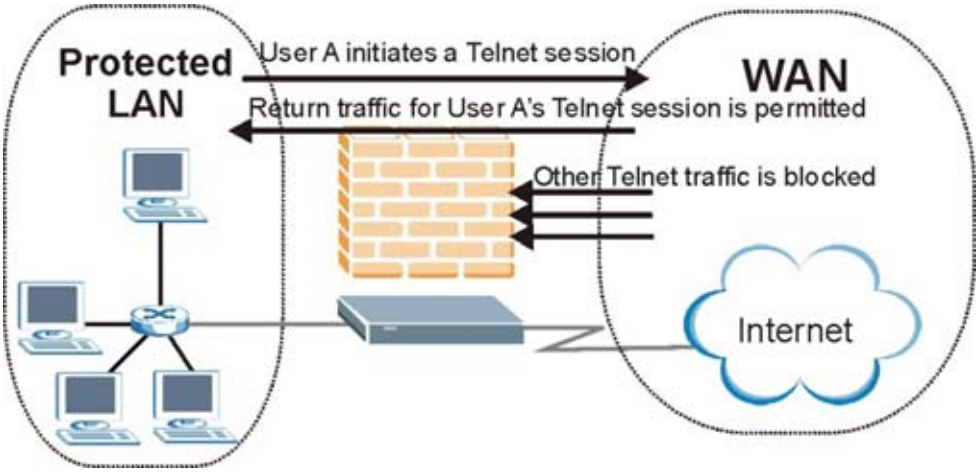


Рис. 11-5 Полнофункциональный контроль

Предыдущий рисунок демонстрирует правила по умолчанию межсетевого экрана Prestige в действии, а также показывает как работает полнофункциональный контроль. Пользователь A может инициировать сеанс связи Telnet из LAN и ответы на этот запрос допускаются. Однако, другой трафик Telnet, инициированный из WAN, блокируется.

11.5.1 Процесс полнофункционального контроля

В данном примере, происходит следующая последовательность событий, когда пакет TCP покидает сеть LAN через интерфейс WAN межсетевого экрана. Пакет TCP является первым в сеансе связи, а протокол прикладного уровня пакета конфигурируется для контролирующих правил межсетевого экрана:

1. Пакет перемещается из LAN с межсетевым экраном в WAN.
2. Пакет проверяется по списку существующих исходящих обращений через интерфейс, и пакету разрешается доступ (отвергнутый пакет просто удаляется к этому моменту).
3. Пакет обследуется по правилам межсетевого экрана для определения и записи информации о состоянии пакета. Эта информация записывается в новую таблицу записей состояния, созданную для нового соединения. Если не существует правила межсетевого экрана для этого пакета и это не является атакой, тогда поле **The default action for packets not matching following rules** (**Действие по умолчанию для пакетов не соответствующих следующим правилам**) (см. *Рис. 13-3*) определяет действие для этого пакета.

4. Основанное на полученной информации состояния, правило межсетевого экрана создает временный список записей доступа, которые вносятся в начало расширенного списка входящего доступа интерфейса WAN. Этот временный список записей доступа предназначается для разрешения входящим пакетам одинакового соединения, как и для только что проверенного исходящего пакета.
5. Исходящий пакет пересылается через интерфейс.
6. Далее, входящий пакет достигает интерфейса. Этот пакет является частью соединения, ранее установленного исходящим пакетом. Входящий пакет оценивается по отношению к списку входящего доступа и допускается, потому что список записей доступа создан ранее.
7. Пакет контролируется правилами межсетевого экрана, а записи таблицы состояния соединения обновляются по мере необходимости. Основанные на обновленной информации состояния, временные записи входящего списка расширенного доступа могут быть изменены, чтобы допустить только те пакеты, которые являются правомерными для текущего состояния соединения.
8. Любые дополнительные входящие или исходящие пакеты, относящиеся к этому соединению контролируются для обновления записи таблицы состояния и модификации временных записей списка входящего доступа по требованию и пересылки через интерфейс.
9. Когда соединение прерывается или заканчивается, удаляется запись таблицы состояния соединения, а также записи временного списка входящего доступа этого соединения.

11.5.2 Полнофункциональный контроль и Prestige

Могут быть определены дополнительные правила для расширения или игнорирования правил по умолчанию. Напр., может быть создано правило, которое будет:

i. Блокировать весь трафик определенного типа, как например, IRC (Internet Relay Chat/Интернетовские посиделки) из LAN в Интернет.

ii. Допускать определенные типы трафика из Интернета на конкретные хосты в LAN.

iii. Разрешать доступ к Web-серверу всем, кроме конкурентов.

iv. Ограничивать использование определенных протоколов, таких как, например, Telnet (теледоступ) санкционированным пользователям в LAN.

Эти пользовательские правила функционируют путем определения IP-адреса источника сетевого трафика, IP-адреса назначения, типа протокола IP, и сопоставления их с правилами, установленными администратором.

Возможность определять правила межсетевого экрана является очень мощным средством. Используя особые правила, можно отключить все

защиты межсетевого экрана или блокировать весь доступ в Интернет. Будьте очень осторожны при создании или удалении правил межсетевого экрана. Проверьте изменения после их создания, чтобы убедиться, что они работают надлежащим образом.

Ниже представлено краткое техническое описание того, как эти соединения отслеживаются. Соединения могут определяться или протоколами верхнего уровня (напр., TCP) или самим Prestige (как и в случае "виртуальных соединений", созданных для UDP и ICMP).

11.5.3 Безопасность TCP

Prestige использует информацию состояния, встроенную в пакеты TCP. Первый пакет любого нового соединения имеет свой установленный флаг SYN и свой очищенный флаг ACK; это пакеты - "инициаторы". Все пакеты, не имеющие этой структуры флагов, называются "последующими" пакетами, так как они представляют данные, возникающие далее в потоке TCP.

Если инициация пакета происходит в WAN, это означает, что кто-то пытается подсоединиться из Интернета в LAN. Эти пакеты сбрасываются и регистрируются. Исключение составляют несколько особых случаев (см. "Протокол верхнего уровня", представленный далее).

Если инициация пакета происходит в LAN, это означает, что кто-то пытается подсоединиться из LAN к Интернету. Полагая, что это является приемлемой частью политики безопасности (как это установлено в политике по умолчанию), соединение будет разрешено. Добавляется запись в кэш, которая включает информацию о подключении, а именно IP-адреса, порты TCP, порядковые номера и т.д.

Если Prestige получает последующий пакет (из Интернета или из LAN), то его информация о подключении извлекается и проверяется в зависимости от кэш. Для пересылки допускается только тот пакет, который соответствует правомерному соединению (т.е., если он является ответом на соединение, исходящее из LAN).

11.5.4 Безопасность UDP/ICMP

UDP (Протокол передачи дейтаграмм пользователя) и ICMP (Протокол управляющих сообщений в сети Интернет) сами по себе не содержат никакой информации о подключении (как например, порядковые номера). Однако, самое наименьшее, что они содержат, это пару IP-адресов (источника и назначения). UDP также содержит пары портов, а ICMP имеет информацию о типе и коде. Все эти данные должны быть проанализированы для создания "виртуальных соединений" в кэш.

Напр., любой пакет UDP, исходящий из LAN, создаст запись в кэш. Его IP-адрес и пары портов записываются. Через небольшой промежуток времени, пакетам UDP из WAN, которые имеют соответствие IP и UDP, информации будет разрешено вернуться через межсетевой экран.

Подобная ситуация существует и для ICMP, за исключением того, что для них Prestige является еще более сильным ограничителем. В частности, только для исходящих эхо-пакетов будет разрешен проход ответных входящих эхо-пакетов, исходящим запросам маски адреса будут разрешены входящие ответы маски адреса, а исходящим запросам метки времени будут разрешены соответствующие входящие ответы. Никаким другим пакетам ICMP не разрешается вход через сетевой экран, просто потому, что они слишком опасны и содержат слишком мало отслеживаемой информации. Напр., ICMP пересылает пакеты, не разрешенные для входа, так как они могут использоваться для перемаршрутизации трафика через атакуемые машины.

11.5.5 Протоколы верхнего уровня

Некоторые протоколы высшего уровня (такие как FTP и RealAudio) одновременно используют многочисленные сетевые соединения. В общих чертах, они обычно имеют "управление соединением", которое используется для отправки команд между оконечными точками, а также "соединение для данных", используемое для передачи массива информации.

Рассмотрим протокол FTP (Протокол передачи данных). Пользователь в LAN открывает *управление соединением* на сервере в Интернете и запрашивает файл. К этому моменту, удаленный сервер откроет соединение для данных из Интернета. Для того, чтобы FTP нормально функционировал, это соединение должно быть допущено к пересылке, даже если соединение из Интернета обычно отвергается.

Для достижения этого, Prestige контролирует данные FTP прикладного уровня. В частности, он разыскивает исходящую команду "PORT" и когда он находит ее, добавляет запись в кэш для подготовки к установлению соединения для данных. Это может быть сделано безошибочно, так как команда PORT содержит информацию об адресе и порте, используемую для однозначной идентификации соединения.

Любой протокол, действующий подобным образом, должен поддерживаться на базе *от случая к случаю*. Для этого можно использовать функцию Custom Ports Web-конфигуратора.

11.6 Руководящие принципы для усиления безопасности при использовании межсетевого экрана

1. Измените пароль по умолчанию при помощи SMT или Web-конфигуратора.
2. Ограничьте подключение к маршрутизатору через Telnet.
3. Не включайте никаких локальных служб (типа SNMP или NTP), если Вы их не используете. Любые включенные службы могу представлять потенциальный риск для безопасности. Некоторые хакеры могут найти оригинальные способы злоупотребления включенными службами для доступа к межсетевому экрану или сети.

4. Для включенных локальных служб должна применяться защита от злоупотребления. Установите защиту, сконфигурировав службы для связи только с одним конкретным клиентским устройством, и сконфигурировав правила для блокирования пакетов этих служб в конкретных интерфейсах.
5. Установите защиту от ложного IP-адреса, убедившись, что межсетевой экран в активен.
6. Храните межсетевой экран в надежном (закрытом) помещении.

11.6.1 Общая безопасность

Никогда нельзя быть полностью защищенным! Факторы за пределами межсетевого экрана, фильтрации или NAT могут вызвать несанкционированный доступ. Ниже представлены некоторые общие правила, которые помогут свести влияние этих факторов к минимуму.

1. Убедите Вашу компанию или организацию разработать комплексный план безопасности. Хорошее административное управление сетью принимает во внимание возможности хакеров и готовится к отражению атак. Лучшая защита от хакеров и взломщиков это информация. Проинструктируйте всех сотрудников о важности защиты и о том, как уменьшить риск. Создайте список наподобие этого.
2. DSL или соединения кабельного модема являются “всегда включенными“ соединениями и чрезвычайно уязвимыми, поэтому они представляют больше возможностей для хакеров, чтобы взломать систему. Выключайте компьютер, если он не используется.
3. Никогда не разглашайте пароль или любую секретную информацию на незапрошенный телефонный вызов или e-mail.
4. Никогда не отправляйте по электронной почте секретную информацию, а именно пароли, данные кредитных карт и т.д., перед этим не закодировав информацию.
5. Никогда не передавайте секретную информацию через web-страницу, если web-сайт не использует надежное соединения. Надежное соединение можно распознать по маленькой иконке “key” (ключ) в нижней части браузера (Internet Explorer 3.02 (или выше) или Netscape 3.0 (или выше)). Если web-сайт использует надежное соединение, можно с уверенностью говорить о надежной передаче информации. Надежные web-транзакции представляют большую сложность для взлома.
6. Никогда не показывайте Ваш IP-адрес или другую сетевую информацию людям не из Вашей компании. Будьте осторожны с файлами, полученными Вами по электронной почте от незнакомцев. Обычный способ получения BackOrifice в системе это вложить его в качестве троянского коня с другими файлами.
7. Регулярно меняйте пароли. Также, используйте пароли, которые не легко вычислить. Наиболее сложные для взламывания пароли это пароли с заглавными и строчными буквами, номерами и символами, как например % или #.

8. Регулярно обновляйте программное обеспечение. Большинство старых версий программного обеспечения, особенно web-браузеры, имеют хорошо известные недостатки в безопасности. При обновлении с последними версиями, Вы получаете новейшие вставки в программу и, соответственно, защиту.
9. Если Вы используете “chat rooms” или сеансы связи IRC, будьте осторожны с любой информацией, которую Вы представляете незнакомцам.
10. Если система начинает выказывать странное поведение, свяжитесь с Интернет-провайдером. Некоторые хакеры обладают таким мастерством, что это приводит к тому, что система понемногу становится неустойчивой или не пригодной для использования.
11. Всегда уничтожайте конфиденциальную информацию, особенно о компьютере, перед тем как ее выбросить. Некоторые хакеры копаются в мусоре компаний или отдельных людей в поисках информации, которая может быть им полезна для совершения атак.

11.7 Фильтрация пакетов в сравнении с межсетевым экраном

Ниже представлены некоторые сравнения между функциями фильтрации Prestige и функциями межсетевого экрана.

11.7.1 Фильтрация пакетов:

- Маршрутизатор фильтрует пакеты, когда они проходят через интерфейс маршрутизатора согласно установленным правилам фильтра.
- Фильтрация пакетов представляет собой мощное средство, однако может быть сложность в конфигурировании и сохранении, особенно, если необходима сводка правил для фильтрации услуги.
- Фильтрация пакетов проверяет только часть заголовка пакета IP.

Когда использовать фильтрацию

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

11.7.2 Межсетевой экран

- Межсетевой экран контролирует содержимое пакетов, а также их адреса отправителя и назначения. Межсетевой экран этого типа использует контрольный модуль, подходящий ко всем протоколам, который понимает, что данные в пакете предназначаются для других уровней, с сетевого уровня (IP-заголовки) до прикладного уровня.
- Межсетевой экран производит полнофункциональный контроль. Он принимает во внимание состояние соединений, которыми он управляет, таким образом, напр., легальный входящий пакет должен совпадать с исходящим запросом, для которого пакет допускается. Напротив, нелегально проникающий входящий пакет в качестве ответа на несуществующий исходящий запрос должен блокироваться.
- Межсетевой экран использует сеанс связи фильтрования, т.е., интеллектуальные правила, которые исправляют процесс фильтрования и контролируют сеанс связи сети, вместо того, чтобы контролировать индивидуальные пакеты в сеансе связи.
- Межсетевой экран предоставляет услугу электронной почты для извещения о текущих сообщениях, а также при появлении извещений.

Когда использовать межсетевой экран

1. Для предотвращения атак типа DoS и предотвращения взламывания сети хакерами.
2. Диапазон отправителя и IP-адресов назначения, а также номера портов, могут быть определены в одном правиле межсетевого экрана, делая межсетевой экран лучшей альтернативой, когда необходимы сложные правила.
3. Для выборочного блокирования/разрешения входящего или исходящего трафика между внутренним хостом/сетями и внешним хостом/сетями. Помните, что фильтры не могут различать по IP-адресу трафик, начинающийся из внутреннего или внешнего хоста.
4. Межсетевой экран работает лучше, чем фильтрация, если необходимо проверить много правил.
5. Используйте межсетевой экран, если необходимы текущие сообщения электронной почты о системе или необходимы извещения о произошедшей атаке.
6. Межсетевой экран может блокировать конкретный трафик URL, который может встречаться в будущем. URL может сохраняться в базе данных Списка контроля доступа (ACL).

Основные графичемские обозначения

 Prestige	 Компьютер (PC)	 Переносной компьютер (Notebook)
 Сервер	 Операторское DSL оборудование (DSLAM)	 Межсетевой экран (Firewall)
 Телефон	 Коммутатор (Switch)	 Маршрутизатор (Router)
 Беспроводной сигнал (Wireless Signal)		

В следующем разделе приведена вводная информация о DSL. Переходите к *Разделу 1* если вы хотите начать работать с Вашим модемом прямо сейчас.

Раздел 12
Конфигурирование межсетевого экрана

В этой главе описывается включение и конфигурирование межсетевого экрана Prestige.

12.1 Дистанционное управление и межсетевой экран

Если дистанционное управление сконфигурировано для разрешения управления (см. главу *Дистанционное управление*) и межсетевой экран включается:

- Межсетевой экран блокирует дистанционное управление из WAN, если не сконфигурировано правило межсетевого экрана, разрешающее такое управление.
- Межсетевой экран допускает дистанционное управление из LAN.

12.2 Включение межсетевого экрана

Щелкните **Firewall**, а затем **Config** для отображения следующего экрана. Поставьте галочку в поле **Firewall Enabled** и щелкните **Apply** для включения (активации) межсетевого экрана.

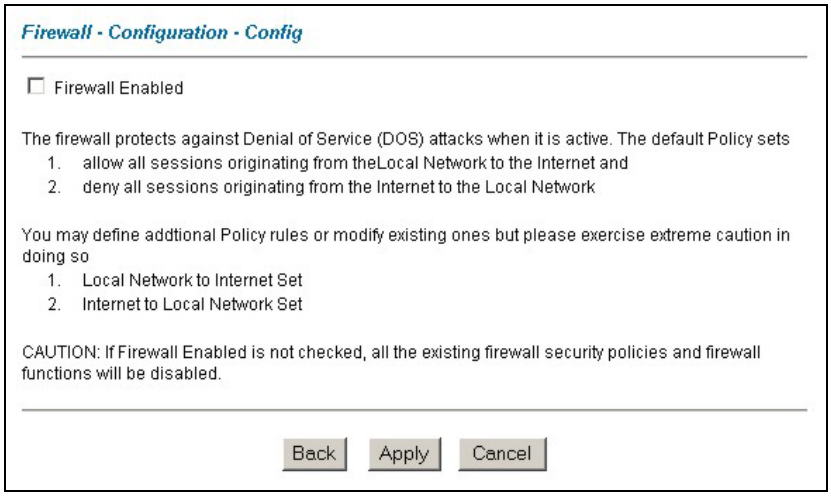


Рис. 12-1 Включение межсетевого экрана

12.3 Извещение об атаке

Извещение об атаке - это сообщение в реальном масштабе времени об атаках типа DoS. В окне, представленном далее, можно выбрать *вывести извещение*, если атака выявлена. Для атак типа DoS, Prestige использует пороги, определяющие, когда необходимо удалить сеанс связи, установленный не полностью. Эти пороги универсально применяются для всех сеансов связи.

Можно использовать значения порога, установленные по умолчанию, или изменить их до значений, более подходящих к требованием безопасности.

12.3.1 Извещения

Извещения представляют собой сообщения о событиях, таких как атаки, о которых необходимо знать немедленно. Можно выбрать в окне **Alert** *вывести извещение,* если атака выявлена *(Рис. 12-2 -* поставьте галочку в поле **Generate alert when attack detected**) или когда совпадает правило в окне **Edit Rule** (см. *Рис. 13-4)*. Если событие создает извещение, сообщение незамедлительно отправляется по адресу электронной почты, который Вы определяете в экране **Log Settings** (см. Главу о журнальной регистрации).

12.3.2 Значения порога

Подстройте эти параметры, если что-нибудь не работает и после того, как проверены счетчики межсетевого экрана. Эти значения, установленные по умолчанию, хорошо подходят для небольших офисов. Факторы, влияющие на опции для значений порога, следующие:

1. Максимальное число открытых сеансов связи.
2. Минимальная производительность сервера журнала запросов в локальной сети.
3. Мощность CPU (центральных процессоров) серверов в локальной сети.
4. Пропускная способность сети.
5. Тип трафика для определенных серверов.

Если сеть медленнее, чем средние значения любого из этих факторов (особенно, если имеются сервера, которые медленно работают или обрабатывают много задач и часто заняты), тогда значения по умолчанию необходимо изменить.
Необходимо произвести изменения в значениях порога до того, как Вы продолжите конфигурирование правил межсетевого экрана.

12.3.3 Полуоткрытые сеансы связи

Необычно высокое число полуоткрытых сеансов связи (конкретное число или измеренное как интенсивность входного потока) может указывать на то, что совершается атака типа *Отказ от обслуживания*. Для TCP, "полуоткрытый" означает, что сеанс связи не достиг установленного состояния - трехстороннее квитирование TCP еще не завершено (см. *Рис. 11-2*). Для UDP, "полуоткрытый" означает, что межсетевой экран не обнаружил обратного трафика.

Prestige измеряет как общее число существующих полуоткрытых сеансов связи, так и интенсивность попыток установления сеанса связи. Полуоткрытые сеансы связи TCP и UDP подсчитываются по общему числу и интенсивности. Измерения производятся раз в минуту.

Когда число существующих полуоткрытых сеансов связи превышает верхний допустимый предел (**max-incomplete high**), Prestige начинает удалять полуоткрытые сеансы связи по требованию для осуществления новых запросов соединения. Prestige продолжает удалять полуоткрытые запросы по мере необходимости, до тех пор, пока число существующих полуоткрытых сеансов связи не упадет ниже другого допустимого предела (**max-incomplete low**).

Когда интенсивность попыток нового соединения превышает допустимый предел (**one-minute high**), Prestige начинает удалять полуоткрытые сеансы связи по требованию для осуществления новых запросов соединения. Prestige продолжает удалять полуоткрытые сеансы связи по мере необходимости, до тех пор, пока интенсивность попыток нового соединения не упадет ниже другого допустимого предела (**one-minute low**). Интенсивность - это число новых попыток, обнаруженных за последний одноминутный выборочный период.

Максимум неполных TCP и время блокирования

Необычно высокое число полуоткрытых сеансов связи с одинаковым адресом целевого хоста может указывать на то, что против хоста осуществляется атака *Отказ от обслуживания*.

Всякий раз, когда число полуоткрытых сеансов связи с одинаковым адресом целевого хоста превышает допустимый предел (**TCP Maximum Incomplete**) (**Максимум неполных TCP**), Prestige начинает удалять полуоткрытые сеансы связи согласно одному из следующих методов:

1. Если интервал простоя **Blocking Time** (**Время блокирования**) равен 0 (по умолчанию), тогда Prestige удаляет самые старые существующие полуоткрытые сеансы связи хоста для каждого нового запроса соединения в хосте. Это обеспечивает ситуацию, что число полуоткрытых сеансов связи, заданных хосту, никогда не превысит допустимого предела.
2. Если интервал простоя **Blocking Time** (**Время блокирования**) выше, чем 0, тогда Prestige блокирует все новые запросы соединения к хосту, предоставляя серверу время на обработку текущих соединений. Prestige продолжает блокировать все новые запросы соединения до тех пор, пока не истечет **Blocking Time** (**Время блокирования**).

Prestige также посылает извещения, всякий раз, когда превышено значение **TCP Maximum Incomplete**. Общие значения, определенные для допустимого предела и интервала простоя, применимы ко всем TCP соединениям. Щелкните **Firewall** и **Alert** для открытия следующего окна.

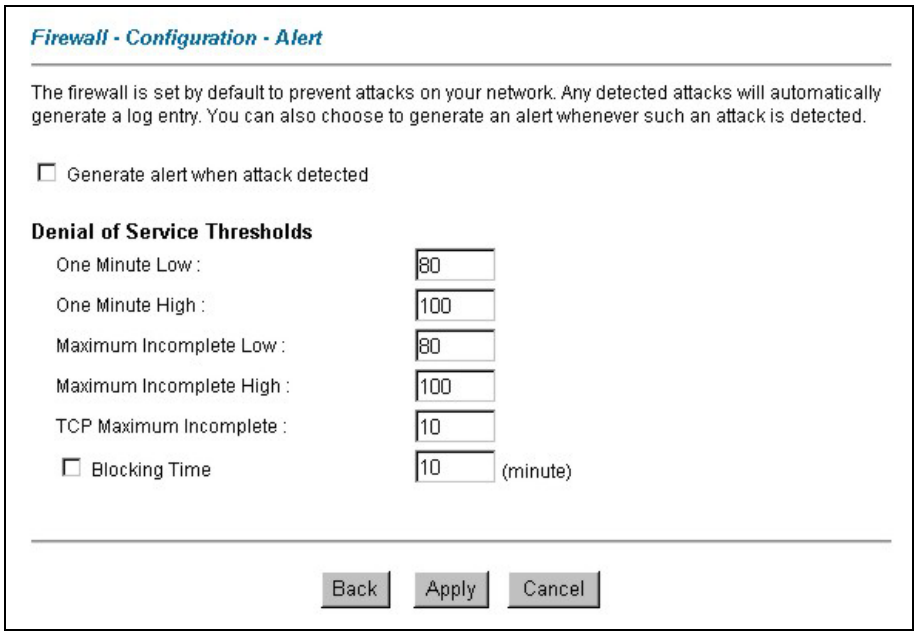


Рис. 12-2 Извещение

В приводимой ниже таблице, представлены описания полей данного окна.

Табл. 12-1 Извещение

ПОЛЕ	ОПИСАНИЕ
Generate alert when attack detected (Вывести извещение при обнаружении атаки)	Поставьте галочку в этом поле для вывода извещения всякий раз при обнаружении атаки.
Denial of Services Thresholds (Допустимый предел атаки типа *Отказ от обслуживания*)	

Табл. 12-1 Извещение

ПОЛЕ	ОПИСАНИЕ
One Minute Low (Одноминутный минимум)	В этом поле отображается интенсивность новых полуоткрытых сеансов связи, обуславливающая межсетевой экран прекратить удаление полуоткрытых сеансов связи. Prestige продолжает удалять полуоткрытые сеансы связи по мере необходимости, до тех пор, пока интенсивность новых попыток соединения не упадет до этого значения. "80" по умолчанию.
One Minute High (Одноминутный максимум)	В этом поле отображается интенсивность новых полуоткрытых сеансов связи, обуславливающая межсетевой экран начать удаление полуоткрытых сеансов связи. По умолчанию - "100". Когда интенсивность попыток нового соединения превышает это число, Prestige начинает удалять полуоткрытые сеансы связи по мере поступления требований на осуществление новых соединений. Prestige прекращает удалять полуоткрытые сеансы связи, если интенсивность становится меньше, чем **One Minute Low.**
Maximum Incomplete Low (Минимум неполных)	В этом поле отображается число существующих полуоткрытых сеансов связи (по умолчанию "80"), обуславливающее межсетевой экран прекратить удаление полуоткрытых сеансов связи. Prestige продолжает удалять полуоткрытые сеансы связи по мере необходимости, до тех пор, пока число существующих полуоткрытых сеансов связи не упадет ниже этого значения.
Maximum Incomplete High (Максимум неполных)	В этом поле отображается число существующих полуоткрытых сеансов связи (по умолчанию "100"), обуславливающее межсетевой экран начать удаление полуоткрытых сеансов связи. Когда число существующих полуоткрытых сеансов связи превышает это значение, Prestige начинает удалять полуоткрытые сеансы связи по мере поступления требований на осуществление новых соединений. Prestige прекращает удалять полуоткрытые сеансы связи, если число становится меньше, чем **Max Incomplete Low**. Не устанавливайте **Maximum Incomplete High** меньше, чем текущее значение **Max Incomplete Low**.
TCP Maximum Incomplete (Максимум неполных TCP)	В этом поле отображается число существующих полуоткрытых сеансов связи TCP (по умолчанию "10") с одинаковым IP-адресом целевого хоста, обуславливающее межсетевой экран начать удаление полуоткрытых сеансов связи с тем же самым IP-адресом целевого хоста. Введите число в диапазоне от **1** до **256**. Основное правило: необходимо выбрать меньшее число для меньшей сети, медленной системы или ограниченной пропускной способности.

Табл. 12-1 Извещение

ПОЛЕ	ОПИСАНИЕ
Blocking Time (Время блокирования)	Когда достигнуто **Maximum Incomplete**, можно выбрать разрешен ли следующий сеанс связи или заблокирован. Если Вы выбираете **Blocking Time**, любой новый сеанс связи будет блокирован на отрезок времени, определенный в следующем поле **(minute),** и все старые незаконченные сеансы связи будут очищены в течение этого периода. Если требуется твердая защита, тогда лучше всего заблокировать трафик на короткое время, так как это предоставит серверу некоторое время для упорядочения загрузки.
(minute) (минута)	Введите длину **Blocking Time** в минутах (1-256). По умолчанию - "0".
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения пользовательских настроек и выхода из этого окна.
Cancel (Отмена)	Щелкните **Cancel** для возвращения к ранее сохраненным настройкам.

Раздел 13
Создание пользовательских правил

В этой главе содержатся инструкции по определению правил локальной сети, а также правил Интернета.

13.1 Описание правил

Правила межсетевого экрана подразделяются на правила “Локальной сети” и правила “Интернет”. По умолчанию, пакет полнофункционального контроля Prestige допускает все соединения в Интернет, которые исходят из местной сети, и блокирует весь трафик в LAN, который исходит из Интернета. Можно определить дополнительные правила и установить или модифицировать существующие, но соблюдайте крайнюю осторожность в выполнении этого.

Вы можете неумышленно подвергнуть межсетевой экран и защищенную сеть небезопасному риску, если попытаетесь сконфигурировать правила без полного осмысления того, как они работают. Убедитесь, что Вы протестировали правила после того, как Вы их сконфигурировали.

Напр., можно создать правила для:

- Блокирования определенных типов трафика, как например IRC (Интернетовские посиделки) из LAN в Интернет.
- Разрешения определенных типов трафика, как например синхронизация базы данных Lotus Notes из конкретных хостов в Интернет для конкретных хостов в LAN.
- Разрешения доступа к Web-серверу всем, кроме Ваших конкурентов.
- Ограничения использования определенных протоколов, как например, Telnet (теледоступ) санкционированным пользователям в LAN.

Эти пользовательские правила функционируют при помощи сопоставления IP-адреса источника сетевого трафика, IP-адреса назначения, типа протокола IP с правилами, установленными администратором. Правила, установленные пользователем, имеют очередность и могут игнорироваться правилами Prestige, установленными по умолчанию.

13.2 Обзор логики правил

Тщательно изучите эти пункты до того, как конфигурировать правила.

13.2.1 Контрольный список правил

1. Сформулируйте цель правила. Напр., “Это ограничивает весь доступ IRC из LAN в Интернет.” Или, “Это разрешает удаленному серверу Lotus Notes синхронизировать через Интернет внутренний сервер Notes.”
2. Цель правила заключается в пересылке или блокировании трафика?
3. Каково направление соединения: из LAN в Интернет или из Интернета в LAN?
4. Какие будут задействованы службы IP?
5. Какие компьютеры задействованы в LAN (если таковые имеются)?
6. Какие компьютеры будут задействованы в Интернете? Чем более конкретно, тем лучше. Напр., если трафик разрешается из Интернета в LAN, то лучше всего разрешить доступ в LAN только определенным машинам в Интернете.

13.2.2 Рамификация безопасности

После того, как логика правила определена, необходимо рассмотреть рамификацию безопасности, созданную правилом:

1. Блокирует ли это правило доступ пользователей LAN к важным ресурсам в Интернете? Напр., если IRC блокируется, существуют ли пользователи, которым требуется эта услуга?
2. Возможно ли модифицировать правило так, чтобы оно было более конкретным? Напр., если IRC блокировано для всех пользователей, не будет ли правило, которое блокирует определенных пользователей, более эффективным?
3. Не создаст ли правило, которое разрешает пользователем Интернета доступ к ресурсам в LAN, слабые места в защите? Напр., если порты FTP (TCP 20, 21) открыты из Интернета в LAN, пользователи Интернетом смогут подключиться к компьютерам, управляемым серверами FTP.
4. Не будет ли это правило вступать в противоречие с другими существующими правилами?

После того, как ответы на все вопросы даны, прибавление правил это просто вопрос занесения информации в соответствующие поля в экране **Rules** Web-конфигуратора.

13.2.3 Основные поля для конфигурирования правил

Действие

Какое должно быть действие **Block** или **Forward**?

"Block" означает, что межсетевой экран сбрасывает пакет без уведомления.

Услуга

Выберите услугу из прокручиваемого окна списка **Service**. Если услуга не содержится в списке, то вначале необходимо ее определить. Для получения более подробной информации о предопределенных услугах см. *Раздел 13.5*.

Адрес источника

Какой адрес источника соединения; находится он в LAN или в WAN? Это единичный IP, диапазон адресов IP или подсеть?

Адрес назначения

Какой адрес назначения соединения; находится он в LAN или в WAN? Это единичный IP, диапазон адресов IP или подсеть?

13.3 Направление соединения

В этом разделе рассказывается о конфигурировании правил межсетевого экрана для соединений, проходящих через межсетевой экран из LAN в WAN и из WAN в LAN.

13.3.1 Правила из LAN в WAN

Правило по умолчанию для трафика из LAN в WAN состоит в том, что всем пользователям в LAN разрешается неограниченный доступ в WAN. При конфигурировании правила из LAN в WAN, по существу, Вы хотите ограничить некоторым или всем пользователям доступ к определенным услугам в WAN. См. следующий рисунок.

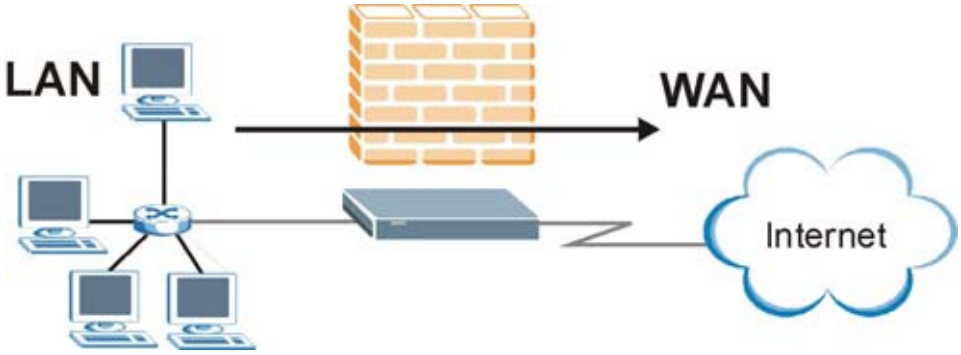


Рис. 13-1 Трафик из LAN в WAN

13.3.2 Правила из WAN в LAN

Правило по умолчанию для трафика из WAN в LAN блокирует все входящие соединения (WAN в LAN). Если Вы хотите разрешить определенным пользователям WAN иметь доступ к LAN, то для этого потребуется создать пользовательские правила.

См. следующий рисунок.

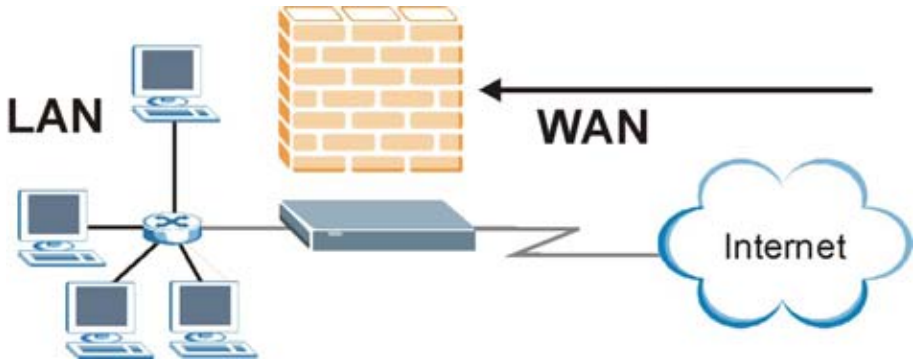


Рис. 13-2 Трафик из WAN в LAN

13.4 Сводка правил

Поля в экранах Rule Summary **идентичны для** установок из локальной сети в Интернет **и для** установок из Интернет в локальную сеть**, поэтому представленные ниже рассуждения относятся к ним обоим.**

Щелкните по **Firewall**, затем **Rule Summary** для отображения следующего экрана. Этот экран представляет собой сводку существующих правил. Обратите внимание на порядок, в котором перечислены правила.

Порядок следования правил очень важен, так как правила применяются по очереди.

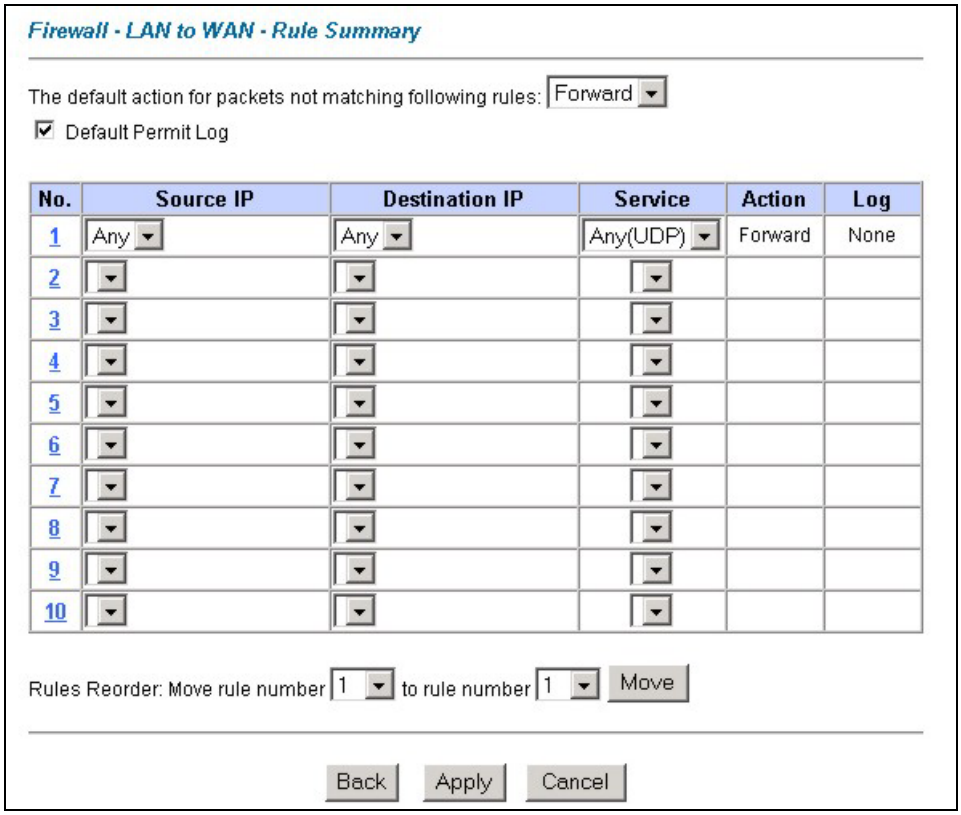


Рис. 13-3 Сводка правил межсетевого экрана: Первый экран

В приводимой ниже таблице, даются описания полей данного окна.

Табл. 13-1 Сводка правил межсетевого экрана: Первый экран

ПОЛЕ	ОПИСАНИЕ
The default action for packets not matching following rules (Действие по умолчанию для пакетов, не соответствующих следующим правилам)	Используйте выпадающий список для выбора **Block** (**Блокировать**) (сброс без уведомления) или **Forward** (**Переслать**) (разрешить пересылку) пакетов, не соответствующих следующим правилам.
Default Permit Log (Разрешение журнальной регистрации по умолчанию)	Поставьте галочку в этом поле для регистрации всех правил, совпадающих с настройкой по умолчанию.
Следующие поля суммируют созданные правила. Обратите внимание, что эти поля используются только для чтения. Щелкните по закладке в верхней части прямоугольника, чтобы расположить правила согласно этой закладке.	
No.	Это - номер правила межсетевого экрана. Порядок следования правил важен, так как правила применяются по очереди. Поле **Move** внизу разрешает переупорядочивание правил. Щелкните по номеру правила для его редактирования.
Source IP (IP-адрес источника)	В этом поле отображается адрес источника пакета. Следует отметить, что пустое поле источника или адреса назначения равнозначно **Any (Любой)**.
Destination IP (IP-адрес назначения)	В этом поле отображается адрес назначения пакета. Следует отметить, что пустое поле источника или адреса назначения равнозначно **Any (Любой)**.
Service (Услуга)	В этом поле отображается услуга, в которой применяется правило. Для получения более подробной информации см. *Табл. 13-2*.
Action (Действие)	В этом поле отображается конкретное действие для правила: **Block** (сбросить) или **Forward** (разрешить пересылку) пакетов.
Log (Журнальная регистрация)	В этом поле отображается регистрируются ли пакеты, для которых произошло совпадение с правилом (**Match**), не произошло совпадения с правилом (**Not Match**), все пакеты регистрируются (**Both**) или пакеты не регистрируются (**None**).

Табл. 13-1 Сводка правил межсетевого экрана: Первый экран

ПОЛЕ	ОПИСАНИЕ
Rules Reorder (Переупорядочивание правил)	Можно переупорядочить правила, используя эту функцию. Из выпадающего списка выберите номер правила, который Вы хотите передвинуть. Порядок следования правил важен, так как правила применяются по очереди.
To Rule Number (Управление номером)	Из выпадающего списка выберите куда Вы хотите передвинуть правило.
Move (Передвижение)	Щелкните **Move** для передвижения правила.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel** для возвращения к ранее сохраненным настройкам.

13.5 Предопределенные услуги

Окно списка **Available Services** в экране **Edit Rule** (см. *Рис. 13-4*) отображает все предопределенные услуги, которые Prestige уже обеспечивает. Рядом с наименованием услуги, два поля отображаются в скобках. Первое поле указывает тип протокола IP (TCP, UDP или ICMP). Второе поле указывает номер порта IP, который определяет услугу. (Следует отметить, что может существовать больше, чем один тип протокола IP. Напр., взгляните на конфигурацию по умолчанию с обозначением "(**DNS**)". **(UDP/TCP:53)** означает UDP порт 53 и TCP порт 53. Возможно до 128 вхождений. Пользовательские услуги также могут быть сконфигурированы с использованием функции **Custom Ports,** рассматриваемой далее.

Табл. **13-2** Предопределенные услуги

УСЛУГА	ОПИСАНИЕ
AIM/NEW_ICQ(TCP:5190)	Сервис сообщений Интернет AOL, используемый в качестве "слушающего" порта при помощи ICQ.
AUTH(TCP:113)	Протокол аутентификации, используется некоторыми серверами.
BGP(TCP:179)	Протокол пограничного шлюза.
BOOTP_CLIENT(UDP:68)	Клиент DHCP.
BOOTP_SERVER(UDP:67)	Сервер DHCP.

Табл. **13-2** Предопределенные услуги

УСЛУГА	ОПИСАНИЕ
CU-SEEME(TCP/UDP:7648, 24032)	Популярное решение для видеоконференцсвязи от White Pines Software.
DNS(UDP/TCP:53)	Сервер имен доменов - услуга, определяющая соответствие web имен (напр. www.zyxel.com) номерам IP.
FINGER(TCP:79)	Указатель - это команда, связанная с UNIX или Интернетом, может использоваться для выяснения зарегистрирован ли пользователь.
FTP(TCP:20.21)	Программа передачи файлов - программа позволяющая быструю передачу файлов, включая большие файлы, которые невозможно отправить по электронной почте.
H.323(TCP:1720)	Этот протокол использует Net Meeting.
HTTP(TCP:80)	Протокол передачи гипертекста - протокол клиент/сервер для "Всемирной паутины".
HTTPS	HTTPS - это надежный сеанс связи http, часто используемый в электронной коммерции.
ICQ(UDP:4000)	Это популярная дискуссионная программа Интернета.
IPSEC_TRANSPORT/TUNNEL(AH:0)	Эту услугу использует протокол туннелирования IPSEC AH (Аутентификация заголовка).
IPSEC_TUNNEL(ESP:0)	Эту услугу использует протокол туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).
IRC(TCP/UDP:6667)	Это еще одна популярная дискуссионная программа Интернета.
MSN Messenger(TCP:1863)	Этот протокол использует сетевой сервис сообщений Microsoft.
MULTICAST(IGMP:0)	Широковещательный протокол взаимодействия групп в сети Интернет -используется при пересылке пакетов в конкретную группу хостов.
NEWS(TCP:144)	Протокол для групп новостей.
NFS(UDP:2049)	Сетевая файловая система (NFS) - представляет собой услугу клиент/сервер по распространению файлов, обеспечивающую совместное прозрачное использование файлов в сетевой среде.
NNTP(TCP:119)	Сетевой протокол передачи новостей - это механизм доставки для услуги сетевой телеконференции USENET.
PING(ICMP:0)	Packet INternet Groper (“Ощупыватель“ Интернет пакетами) - это протокол, который посылает эхо-запросы ICMP для проверки

Табл. **13-2** Предопределенные услуги

УСЛУГА	ОПИСАНИЕ
	достижимости удаленного хоста.
POP3(TCP:110)	Почтовый протокол версии 3 позволяет клиентским компьютерам получать электронную почту с сервера POP3 через временное соединение (TCP/IP или другие).
PPTP(TCP:1723)	Протокол Point-to-Point Tunneling обеспечивает безопасную передачу данных через корпоративные сети. Это канал управления.
PPTP_TUNNEL(GRE:0)	Протокол Point-to-Point Tunneling обеспечивает безопасную передачу данных через корпоративные сети. Это канал данных.
RCMD(TCP:512)	Услуга удаленных команд.
REAL_AUDIO(TCP:7070)	Услуга прямого воспроизведения звука, обеспечивает передачу звука в реальном времени через web.
REXEC(TCP:514)	Дистанционное выполнение Daemon.
RLOGIN(TCP:513)	Удаленная регистрация.
RTELNET(TCP:107)	Удаленный теледоступ.
RTSP(TCP/UDP:554)	Протокол воспроизведения в реальном времени (управление средой передачи) (RTSP) - это удаленное управление для мультимедиа в Интернете.
SFTP(TCP:115)	Простой протокол передачи файлов.
SMTP(TCP:25)	Простой протокол электронной почты - это стандарт обмена сообщениями для Интернета. SMTP позволяет перемещать сообщения с одного сервера электронной почты на другой.
SNMP(TCP/UDP:161)	Простая программа управления сетью.
SNMP-TRAPS (TCP/UDP:162)	Прерывания для совместного использования с SNMP (RFC:1215).
SQL-NET(TCP:1521)	Язык структурированных запросов представляет собой интерфейс для доступа к данным на различных типах систем баз данных, включая универсальные вычислительные машины, средние системы, системы UNIX и сетевые серверы.
SSDP(UDP:1900)	Протокол упрощенной службы обнаружения (SSDP) - это услуга обнаружения, отыскивающая устройства типа Plug and Play в Вашей домашней сети или шлюзы в Интернете для передачи данных при помощи порта 1900 протокола UDP.

Табл. **13-2** Предопределенные услуги

УСЛУГА	ОПИСАНИЕ
SSH(TCP/UDP:22)	Программа по обеспечению надежной удаленной регистрации.
STRMWORKS(UDP:1558)	Протокол передачи данных.
SYSLOG(UDP:514)	Системный журнал - позволяет посылать журнальные регистрации системы на сервер UNIX.
TACACS(UDP:49)	Протокол регистрации хоста, используемый для TACACS - Контроллер доступа терминалов управления доступом системы.
TELNET(TCP:23)	Telnet представляет собой регистрацию и протокол эмуляции терминала, распространенный в Интернете и в среде UNIX. Он управляется через сети TCP/IP. Его основная функция - разрешить пользователям зарегистрироваться на удаленной хост-системе.
TFTP(UDP:69)	Упрощенный протокол передачи файлов - это протокол передачи файлов Интернет, подобный FTP, но использующий UDP (Протокол передачи дейтаграмм пользователя), а не TCP (Протокол управления передачей).
VDOLIVE(TCP:7000)	Другое решение для видеоконференцсвязи.

13.6 Создание/редактирование правил межсетевого экрана

Для создания нового правила щелкните в последнем представленном окне по номеру (**No.**) для отображения следующего экрана.

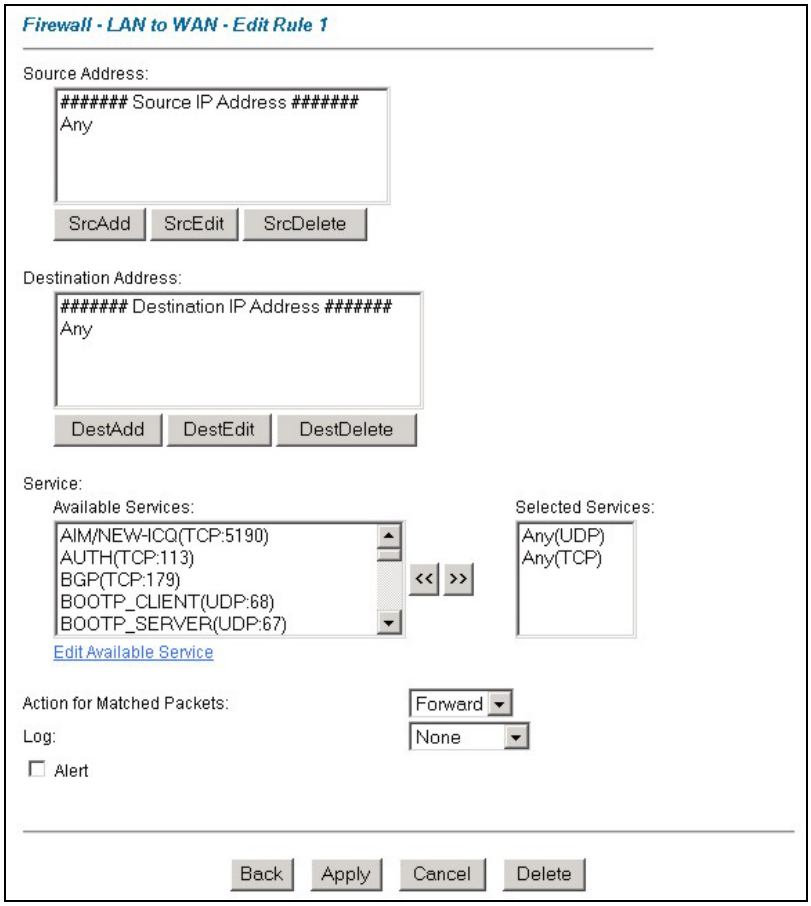


Рис. 13-4 Создание/редактирование правил межсетевого экрана

В приводимой ниже таблице, даны описания полей данного окна.

Табл. 13-3 Создание/редактирование правил межсетевого экрана

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

Табл. 13-3 Создание/редактирование правил межсетевого экрана

ПОЛЕ	ОПИСАНИЕ
Destination Address (Адрес назначения)	Щелкните **DestAdd** для добавления нового адреса, **DestEdit** для редактирования существующего адреса или **DestDelete** для удаления адреса.
Services (Услуги)	Выберите услугу в прямоугольнике **Available Services** слева, затем щелкните **>>** для выбора. Выбранная услуга отобразится в прямоугольнике **Selected Services** справа. Для удаления услуги щелкните по ней в прямоугольнике **Selected Services** справа, затем щелкните **<<**.
Edit Available Service (Редактирование доступной услуги)	Щелкните по этой кнопке для вызова экрана **Customized Services**. Для дополнительной информации см. *Раздел 14*.
Action for Matched Packets (Действие при совпадении пакетов)	Из выпадающего списка выберите **Block** (сброс без уведомления) или **Forward** (разрешение пересылки) пакетов, для которых произошло совпадение с правилом.
Log (Журнальная регистрация)	В этом поле определяется регистрируются ли пакеты, для которых произошло совпадение с правилом (**Match**), не произошло совпадения с правилом (**Not Match**), все пакеты регистрируются (**Both**) или пакеты не регистрируются (**None**).
Alert (Извещение)	Поставьте галочку в поле **Alert** для установления, что это правило выводит извещение при совпадении с правилом.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel** для выхода из этого окна без сохранения.
Delete (Удалить)	Щелкните **Delete** для удаления текущего правила.

13.6.1 Адреса источника и отправителя

Для добавления нового адреса источника или отправителя щелкните **SrcAdd** или **DestAdd** в предыдущем экране. Для редактирования существующего адреса источника или отправителя выберите его из прямоугольника и щелкните **SrcEdit** или **DestEdit** в предыдущем экране. В результате этого отобразится следующий экран.

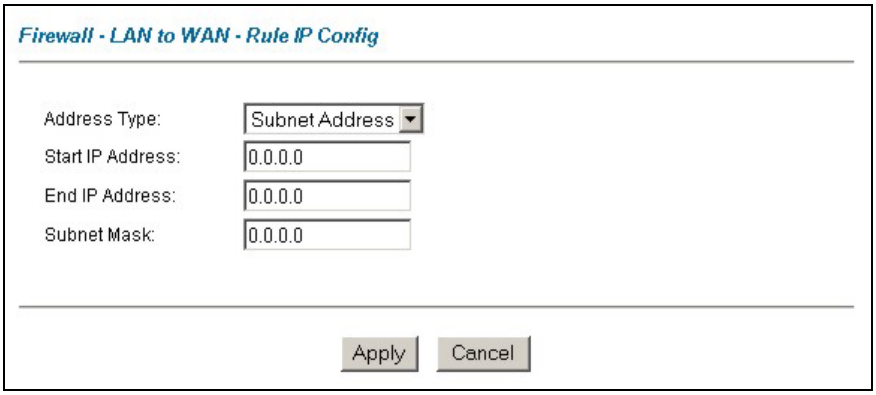


Рис. 13-5 Добавление/редактирование адресов источника и назначения

В приводимой ниже таблице, даны описания полей данного окна.

Табл. 13-4 Добавление/редактирование адресов источника и назначения

ПОЛЕ	ОПИСАНИЕ
Address Type (Тип адреса)	Вы хотите, чтобы правило применялось к пакетам с индивидуальным (единичным) IP-адресом, диапазону IP-адресов (напр., 192.168.1.10 до 192.169.1.50), подсети или любому IP-адресу? Выберите опцию из выпадающего списка, который включает: **Single Address**, **Range Address**, **Subnet Address** и **Any Address.**
Start Address (Начальный IP-адрес)	Введите единичный IP-адрес или начальный IP-адрес из диапазона адресов.
End Address (Конечный IP-адрес)	Введите последний IP-адрес из диапазона адресов.
Subnet Mask (Маска подсети)	Введите маску подсети, если применяется.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel** для возвращения к ранее сохраненным настройкам.

13.7 Время простоя

Поля экрана Timeout **идентичны для параметров соединений из** локальной сети в Интернет **и** для параметров соединений из Интернет в локальную сеть, **поэтому представленные ниже рассуждения относятся к ним обоим.**

13.7.1 Факторы, влияющие на опции для значений времени простоя

Факторы, влияющие на опции для значений времени простоя, идентичны факторам, влияющим на опции для значений допустимого предела – см. *Раздел 12.3.2*. Щелкните **Timeout** для **Local Network to Internet Set** или **Internet to Local Network Set**.

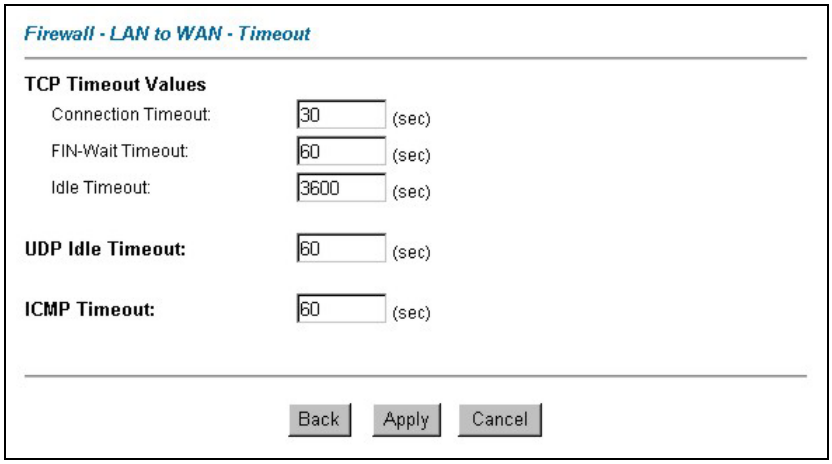


Рис. 13-6 Время простоя

В приводимой ниже таблице, даны описания полей данного окна.

Табл. 13-5 Время простоя

ПОЛЕ	ОПИСАНИЕ
TCP Timeout Values (Значения времени простоя TCP)	

Табл. 13-5 Время простоя

ПОЛЕ	ОПИСАНИЕ
Connection Timeout (Время простоя соединения)	Введите время в секундах (по умолчанию - 30), чтобы Prestige подождал установления сеанса связи TCP перед сбрасыванием сеанса связи.
FIN-Wait Timeout (Время простоя FIN-Wait)	Введите время в секундах (по умолчанию - 60) для того, чтобы сеанс связи TCP оставался открытым после того, как межсетевой экран обнаружит FIN-обмен (указывающий на конец сеанса связи TCP).
Idle Timeout (Время простоя)	Введите время в секундах (по умолчанию - 3600) для того, чтобы неактивное соединение TCP оставалось открытым до того, как Prestige рассмотрит закрытое соединение.
UDP Idle Timeout (Время простоя UDP)	Введите время в секундах (по умолчанию - 60) для того, чтобы неактивное соединение UDP оставалось открытым до того, как Prestige осуществит закрытие соединения.
ICMP Timeout (Время простоя ICMP)	Введите время в секундах (по умолчанию - 60) для того, чтобы сеанс связи ICMP подождал ответа ICMP.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения пользовательских настроек и выхода из этого окна.
Cancel (Отмена)	Щелкните **Cancel** для возвращения к предыдущей конфигурации.

Раздел 14
Пользовательские услуги

В этой главе описывается создание, просмотр и редактирование пользовательских услуг.

14.1 Введение в пользовательские услуг

Конфигурирование пользовательских услуг и номеров порта не предписано Prestige (см. *Рис. 13-4)*. Посетите Web-сайт IANA (Агентство по назначению имен и уникальных параметров протоколов Интернет), на котором представлен полный перечень номеров портов и услуг. Для получения подробной информации по этим услугам см. *Раздел 13.5*. Для конфигурирования пользовательских услуг щелкните **Edit Available Service** в экране редактирования правил для отображения следующего окна.

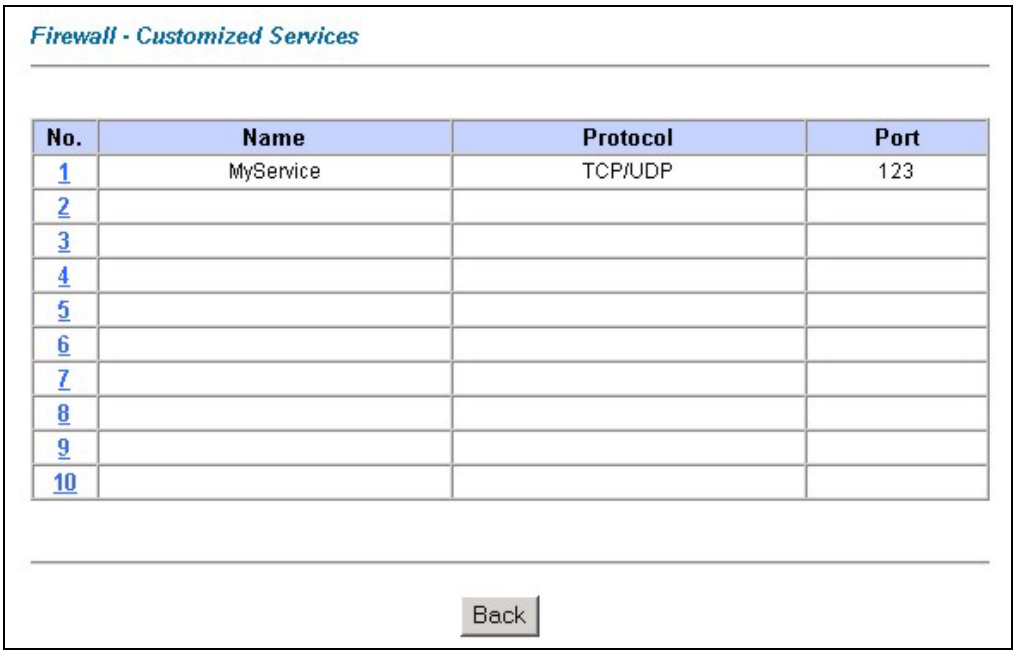


Рис. 14-1 Пользовательские услуги

В приводимой ниже таблице, даны описания полей данного окна.

Табл. 14-1 Пользовательские услуги

ПОЛЕ	ОПИСАНИЕ
Customized Services (Пользовательские услуги)	
No.	В этом поле отображается номер пользовательского порта. Щелкните номер правила услуги для вызова экрана **Firewall Customized Services Config** для конфигурирования или редактирования пользовательской услуги.
Name (Имя)	В этом поле отображается название пользовательской услуги.
Protocol (Протокол)	В этом поле отображается протокол IP (**TCP**, **UDP** или **TCP/UDP**), который определяет пользовательскую услугу.
Port (Порт)	В этом поле отображается номер порта или диапазон, определяющий пользовательскую услугу.
Back (Назад)	Щелкните **Back** для возвращения к экрану **Firewall Edit Rule**.

14.2 Создание/редактирование пользовательской услуги

Щелкните номер правила в предыдущем экране для создания нового пользовательского порта или редактирования существующего. В результате этого отобразится следующий экран.

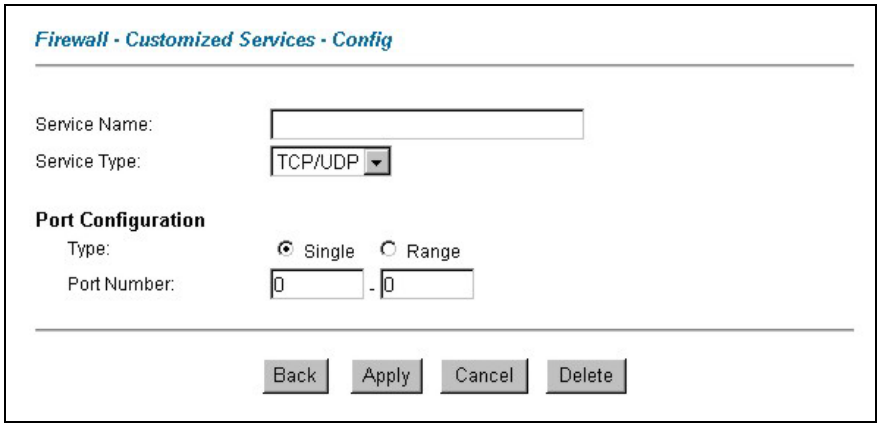


Рис. 14-2 Создание/редактирование пользовательской услуги

В приводимой ниже таблице, даны описания полей данного окна.

Табл. 14-2 Создание/редактирование пользовательской услуги

ПОЛЕ	ОПИСАНИЕ
Service Name (Имя услуги)	Введите уникальное имя для пользовательского порта.
Service Type (Тип услуги)	Из выпадающего списка выберите порт IP (**TCP**, **UDP** или **TCP/UDP**), который определяет пользовательский порт.
Port Configuration (Конфигурирование порта)	
Type (Тип)	Щелкните **Single** для установления только одного порта или **Range** для установления диапазона портов, которые определяют пользовательскую услугу.
Port Number (Номер порта)	Введите единичный номер порта или диапазон номеров порта, которые определяют пользовательскую услугу.
Back (Назад)	Щелкните **Back** для возвращения к экрану **Firewall Customized Services**.
Apply (Применить)	Щелкните **Apply** для сохранения пользовательских настроек и выхода из этого окна.
Cancel (Отмена)	Щелкните **Cancel** для возвращения к ранее сохраненным настройкам.
Delete (Удалить)	Щелкните **Delete** для удаления текущего правила.

14.3 Пример правила пользовательской услуги межсетевого экрана

Следующий пример правила межсетевого экрана Интернета позволяет гипотетическое соединение “My Service” (Моя услуга) из Интернета.

Step 10. Щелкните по Сводке правил под установкой соединений из Интернет в локальную сеть.

Step 11. Щелкните по номеру правила для вызова экрана редактирования правила.

Step 12. Щелкните **Any** в прямоугольнике **Source Address**, а затем щелкните **ScrDelete**.

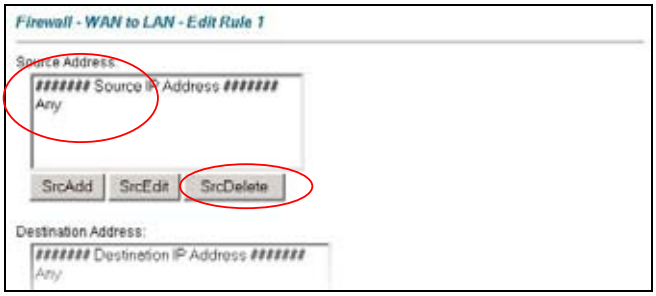


Рис. 14-3 Пример редактирования правила

Step 13. Щелкните **ScrAdd** для вызова экрана **Rule IP Config**. Сконфигурируйте его следующим образом и щелкните **Apply**.

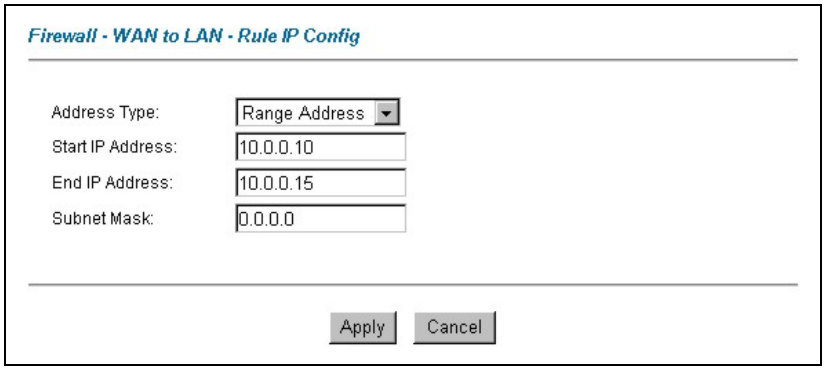


Рис. 14-4 Пример конфигурирования источника IP

Step 14. Щелкните **Edit Available Service** в экране **Edit rule**, а затем щелкните по номеру правила для отображения экрана **Firewall Customized Services Config**. Сконфигурируйте его следующим образом.

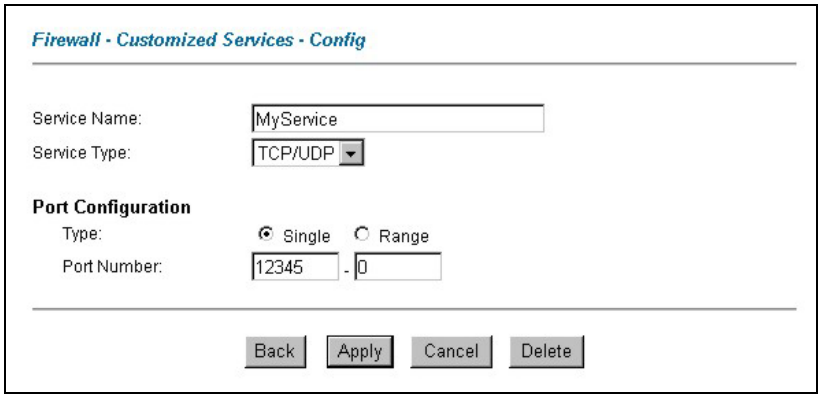


Рис. 14-5 Пример пользовательской услуги для MyService

Пользовательские услуги отображаются с символом “*” перед их названием в списке Services и в списке Rule Summary. Щелкните Apply **после создания пользовательской услуги.**

Step 15. Следуйте методике, описанной ранее в этой главе, для конфигурирования остальных правил. Заполните экран конфигурирования правил как представлено ниже и примените его.

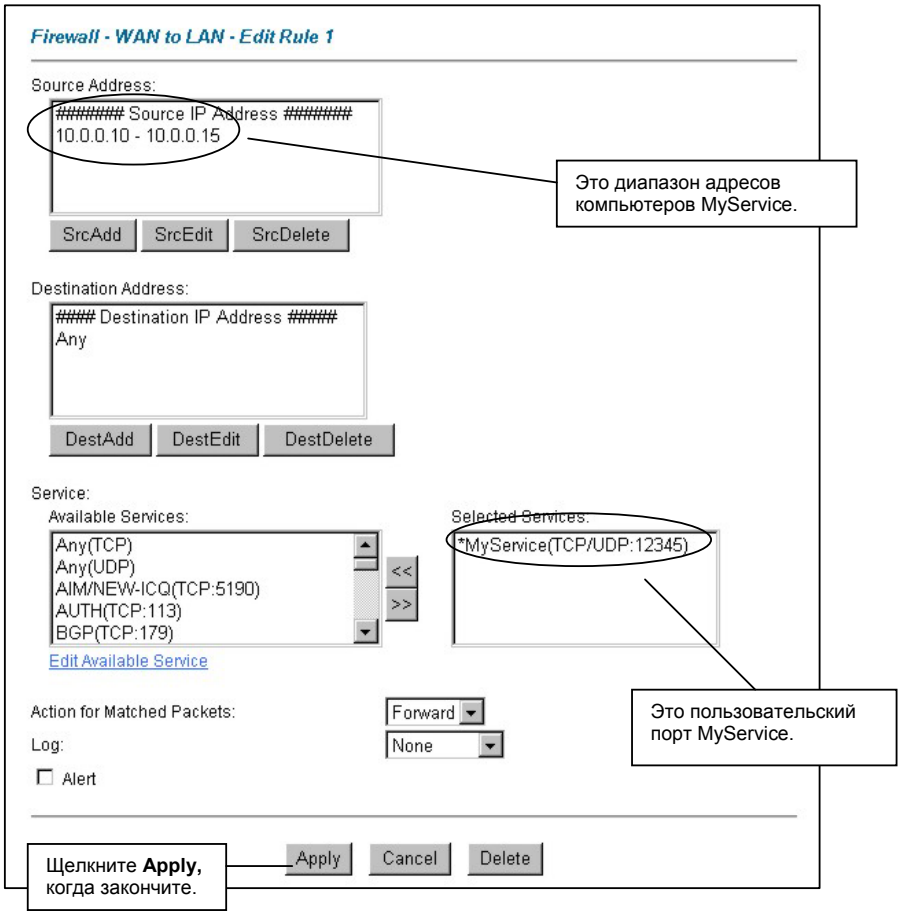


Рис. 14-6 Пример конфигурирования правила системного журнала

Step 16. По завершении процедуры конфигурирования для этих правил межсетевого экрана Интернет, экран **Rule Summary** должен выглядеть следующим образом. Не забудьте щелкнуть **Apply** по завершении конфигурирования правил для сохранения настроек в Prestige.

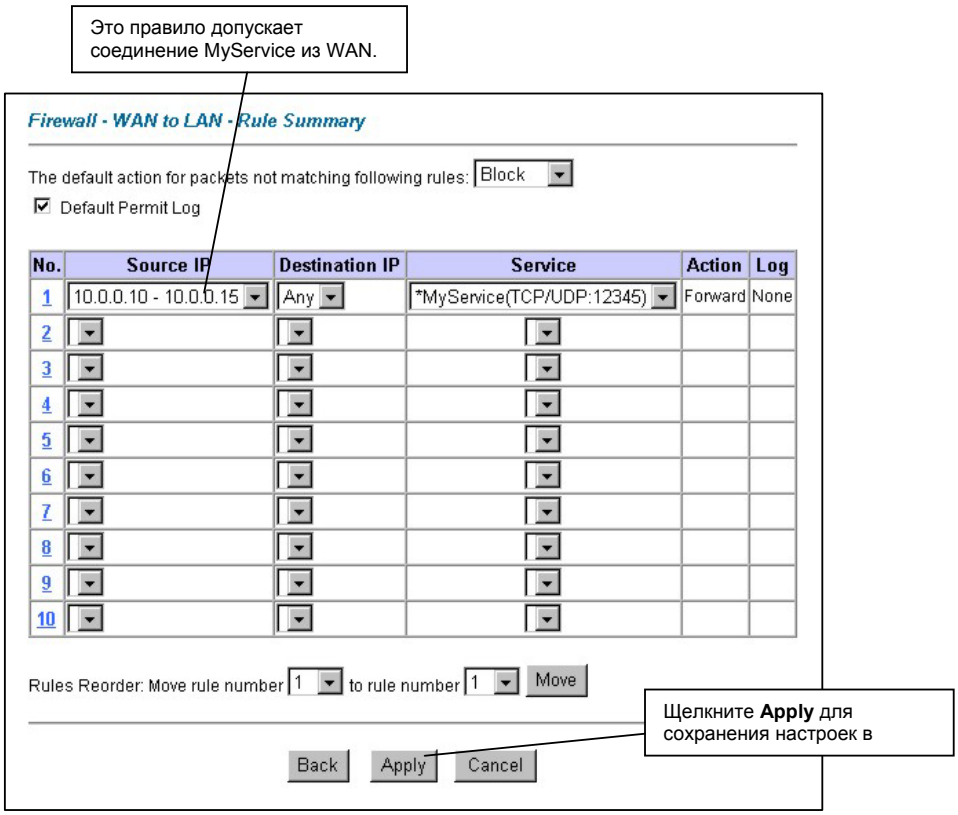


Рис. 14-7 Пример Сводки правил

Раздел 15
Контент-фильтрование

В этой части дается обзор конфигурирования контент-фильтрования.

15.1 Обзор контент-фильтрования

Контент-фильтрование Интернета позволяет создать и осуществить стратегии доступа в Интернет согласно Вашим потребностям. Контент-фильтрование предоставляет возможность блокировать Web-сайты, содержащие ключевые слова (которые устанавливаете Вы) в URL. Можно составить план, когда Prestige будет выполнять контент-фильтрование. Также можно установить правомочные IP-адреса в LAN, для которых Prestige не будет производить контент-фильтрование.

15.2 Конфигурирование блокировки по ключевым словам

Используйте этот экран для блокирования сайтов, содержащих определенные ключевые слова в URL. Напр., если Вы включаете ключевое слово "bad", Prestige блокирует все сайты содержащие это ключевое слово, включая URL http://www.website.com/bad.html, даже, если оно не входит в Список фильтра.

Для того, чтобы Prestige блокировал Web-сайты, содержащие ключевые слова в своих URL, щелкните **Content Filter** и **Keyword**. Отобразится окно, указанное ниже.

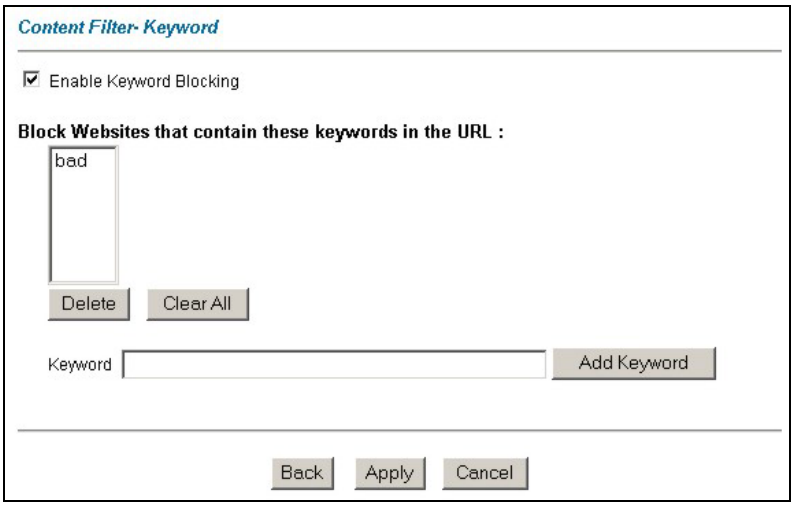


Рис. 15-1 Контент-фильтр: Ключевое слово

В приводимой ниже таблице, даны описания полей данного окна.

Табл. 15-1 Контент-фильтр: Ключевое слово

ПОЛЕ	ОПИСАНИЕ
Enable Keyword Blocking (Включение блокировки по ключевым словам)	Поставьте галочку в этом поле для включения этой функции.
Block Websites that contain these keywords in the URL: (Блокирование Web-сайтов, содержащих эти ключевые слова в URL)	Это поле содержит список всех ключевых слов, которые Вы сконфигурировали в Prestige для блокировки.
Delete (Удалить)	Выделите ключевое слово в прямоугольнике и щелкните **Delete** для его удаления.
Clear All (Очистить все)	Щелкните **Clear All** для удаления всех ключевых слов из этого списка.

Табл. 15-1 Контент-фильтр: Ключевое слово

ПОЛЕ	ОПИСАНИЕ
Keyword (Ключевое слово)	Введите в это поле ключевое слово. Допускается использование любых символов (до 64 символа). Знаки препинания не разрешаются.
Add Keyword (Добавить ключевое слово)	Щелкните **Add Keyword** после того, как Вы ввели ключевое слово. Повторите эту процедуру для добавления других ключевых слов. Допускается до 127 ключевых слов. При попытке доступа к web-странице, содержащей ключевое слово, Вы получите сообщение, в котором говорится, что контент-фильтр блокирует этот запрос.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel** для возвращения к ранее сохраненным настройкам.

15.3 Конфигурирование плана

Для установки даты и времени, когда Prestige будет производить контент-фильтрование щелкните **Content Filter** и **Schedule**. Отобразится окно, указанное ниже.

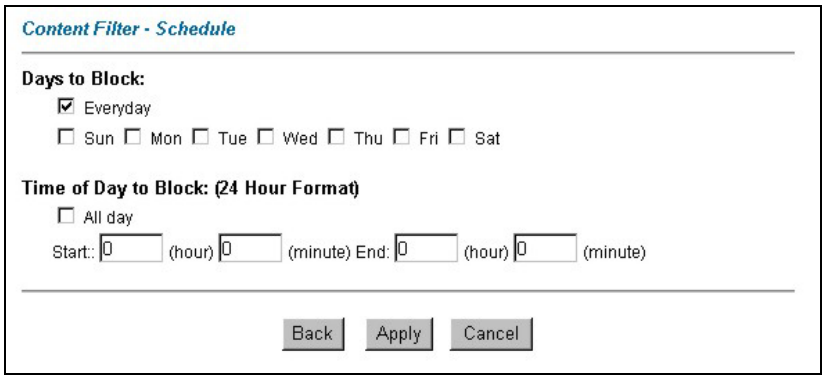


Рис. 15-2 Контент-фильтр: План

В приводимой ниже таблице, даны описания полей данного окна.

Табл. 15-2 Контент-фильтр: План

ПОЛЕ	ОПИСАНИЕ
Days to Block: (Дни для блокирования)	Поставьте галочку в этом поле, чтобы установить в какие дни недели (или каждый день) необходимо проводить контент-фильтрование.
Time of Day to Block: (Время дня для блокирования)	Используйте суточный формат, чтобы установить в какое время дня (или поставьте галочку в поле **All day**) необходимо проводить контент-фильтрование.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения изменений.
Cancel (Отмена)	Щелкните **Cancel** для возвращения к ранее сохраненным настройкам.

15.4 Настройка списка компьютеров, пользующихся доверием

Для исключения диапазона пользователей в LAN из контент-фильтрования в Prestige щелкните **Content Filter** и **Trusted**. Отобразится окно, указанное ниже.

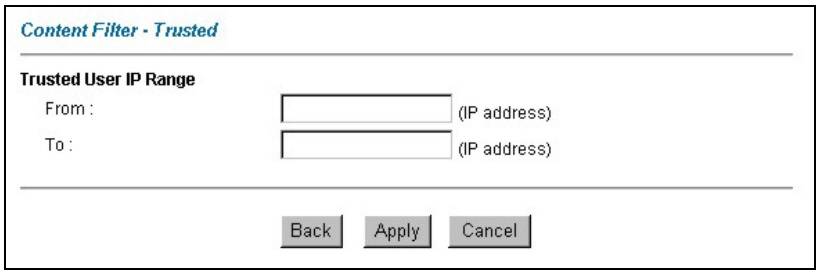


Рис. 15-3 Контент-фильтр: Правомочный

В приводимой ниже таблице, даны описания полей данного окна.

Табл. 15-3 Контент-фильтр: Правомочный

ПОЛЕ	ОПИСАНИЕ
Trusted User IP Range (Диапазон правомочных пользователей IP)	
From (Из)	Введите IP-адрес компьютера (или начальный IP-адрес конкретного диапазона компьютеров) в LAN, который Вы хотите исключить из контент-фильтрования.
To (В)	Введите конечный IP-адрес конкретного диапазона пользователей в LAN, которых Вы хотите исключить из контент-фильтрования. Оставьте это поле не заполненным, если Вы хотите исключить отдельный компьютер.
Back (Назад)	Щелкните **Back** для возвращения к предыдущему окну.
Apply (Применить)	Щелкните **Apply** для сохранения изменений в Prestige.
Cancel (Отмена)	Щелкните **Cancel** для возвращения к ранее сохраненным настройкам.

Глава V:

Дистанционное управление, UPnP и журналы

В этой части содержится информация о конфигурировании Prestige для дистанционного управления, настройке универсальной функции "Plug and Play" (UPnP), а также организации и отображении журналов.

Раздел 16
Конфигурирование дистанционного управления

В этой главе содержится информация о конфигурировании дистанционного управления.

16.1 Обзор дистанционного управления

Дистанционное управление позволяет определить, какие службы/протоколы и с каких компьютеров могут получить доступ к определенным интерфейсам Prestige .

При конфигурировании дистанционного управления, разрешающего управление из глобальной сети, Вы должны также сконфигурировать правило межсетевого экрана, разрешающее доступ. Подробную информацию о конфигурировании правил межсетевых экранов см. в главах, описывающих межсетевые экраны.

Вы можете управлять Prestige из удаленного пункта из:

- Интернет (WAN only - только из WAN)
- LAN only (только из LAN),
- ALL (отовсюду) (из LAN и WAN)
- Neither (Disable) (Ниоткуда (Отключено))

При выборе опции WAN only **или** ALL **(LAN & WAN), необходимо также сконфигурировать правило межсетевого экрана, разрешающее доступ.**

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

Единовременно возможна только одна сессия удаленного управления. Prestige автоматически разрывает сессию удаленного управления более низкого приоритета в момент старта сессии удаленного управления с большим приоритетом. Приоритеты для разных типов сессий удаленного управления следующие:

1. Telnet
2. HTTP

16.1.1 Ограничения дистанционного управления

Дистанционное управление через LAN или WAN не будет работать, когда:

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

2. Эта услуга отключена в одном из окон дистанционного управления.
3. IP-адрес в поле **Secured Client IP** не совпадает с IP-адресом клиента. В случае несовпадения Prestige немедленно закрывает сеанс связи.
4. Уже установлена сеанс дистанционного управления с равным или большим приоритетом. Одновременно возможен только один сеанс дистанционного управления.
5. Существует правило межсетевого экрана, которое блокирует такое соединение.

16.1.2 Дистанционное управление и NAT

При использовании NAT:

- При конфигурировании через глобальную сеть следует использовать IP-адрес Prestige в глобальной сети.
- При конфигурировании через локальную сеть следует использовать IP-адрес Prestige в локальной сети.

16.1.3 Системная задержка

Существует задержка бездействия управления системой длительностью в пять минут (триста секунд). Prestige автоматически отключает вас, если сессия управления остается бездействующей в течении времени более системной задержки, за исключением случая, когда постоянно обновляется окно статистики.

16.2 Telnet

Вы можете настроить удаленный доступ к Prestige через Telnet, как показано ниже.

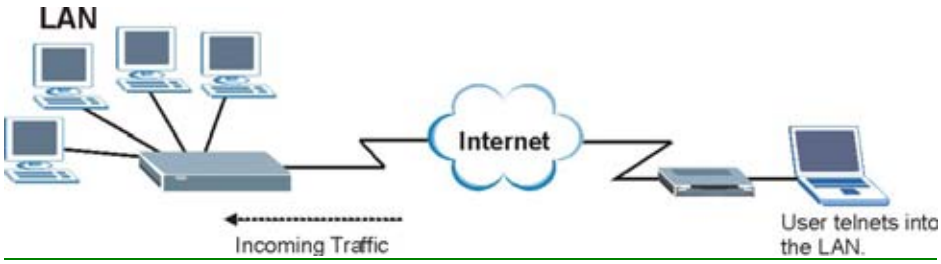


Рис. 16-1 Конфигурирование Telnet в сети TCP/IP

16.3 FTP

При помощи FTP Вы можете загружать и выгружать файлы микропрограммного обеспечения и конфигурации Prestige. Для использования данной функции на Вашем компьютере должен быть установлен FTP-клиент.

16.4 Web

Для конфигурирования и управления файлами можно использовать встроенный Web-конфигуратор Prestige. Подробности см. в оперативной справке.

16.5 Конфигурирование дистанционного управления

Для перехода к следующему окну щелкните на **Remote Management**.

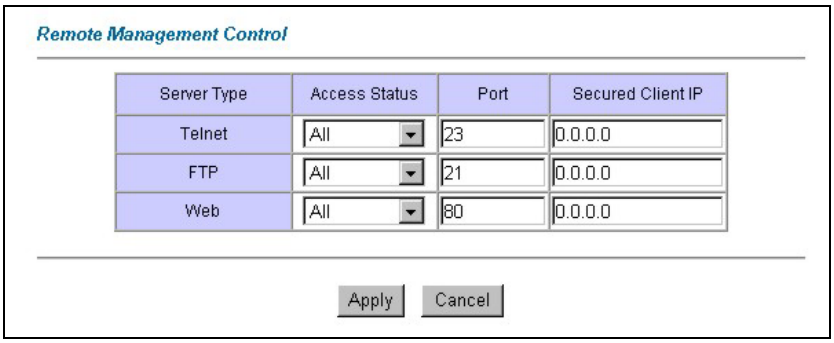


Рис. 16-2 Дистанционное управление

В следующей таблице даны описания полей данного меню.

Таблица 16-1 Дистанционное управление

ПОЛЕ	ОПИСАНИЕ
Server Type (Тип сервера)	Каждая из этих надписей обозначает службу, которую Вы можете использовать при дистанционном управлении Prestige.
Access Status (Статус доступа)	Выберите интерфейс доступа. Варианты выбора: **All**, **LAN Only**, **WAN Only** и **Disable**.
Port (Порт)	В данном поле показан номер порта для службы дистанционного управления. В этом поле Вы можете сменить номер порта службы, но Вы должны использовать такой же номер порта для использования службы при дистанционном управлении.
Secured Client IP (Защищенный клиентский IP-адрес)	По умолчанию используется 0.0.0.0, что позволяет любому клиенту использовать данную функцию для дистанционного управления Prestige. Введите IP-адрес для предоставления доступа только клиентам с совпадающим IP-адресом.
Apply (Применить)	Щелкните на **Apply** для сохранения настроек в Prestige.
Cancel (Отмена)	Щелкните на **Cancel**, чтобы начать настройку заново.

Раздел 17
Универсальная функция Plug and Play (UPnP)

В данной главе содержится вводная информация по функции UPnP в Web-конфигураторе.

17.1 Введение в Универсальную функцию Plug and Play

Универсальная функция Plug and Play (UPnP) - это распределенный открытый сетевой стандарт, использующий TCP/IP для возможности подключения устройств в одноранговой сети. Устройство UPnP может динамически присоединяться к сети, получать IP-адрес, передавать свои функциональные возможности и собирать информацию о других устройствах сети. В свою очередь, устройство может беспрепятственно и автоматически покидать сеть, когда оно больше не используется.

17.1.1 Как узнать, используется ли UPnP?

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

17.1.2 Прохождение NAT

Прохождение NAT (NAT Transversal) с поддержкой UPnP автоматизирует процесс работы приложения через NAT. Сетевые устройства, совместимые с UPnP, могут автоматически настроить сетевые адреса, объявить о своем присутствии в сети другим устройствам UPnP и включить обмен простыми описаниями продукта и услуг. Прохождение NAT позволяет следующее:

- Динамическое отображение портов
- Изучение общедоступных IP-адресов
- Назначение времени аренды отображениям

Windows Messenger является примером приложения, поддерживающего NAT Traversal и UPnP.

Подробнее о NAT см. в главе *Трансляция сетевых адресов (NAT)*.

17.1.3 Предупреждения по использованию UPnP

Сущность автоматизации приложений NAT Traversal заключается в установлении собственных служб и открытии портов брандмауэра, что может оказать влияние на сетевую безопасность. Сетевая

информация и конфигурация может быть получена и изменена пользователями в некоторых сетевых средах.

Все UPnP-совместимые устройства могут свободно взаимодействовать друг с другом без дополнительной настройки. Отключите UPnP, если Вы не собираетесь ее использовать.

17.2 UPnP и ZyXEL

Корпорация ZyXEL получила сертификат UPnP от Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). Реализация UPnP корпорации ZyXEL поддерживает IGD 1.0 (Internet Gateway Device - устройство Интернет-шлюза). На момент написания документа реализация UPnP корпорации ZyXEL поддерживает Windows Messenger 4.6 и 4.7, в то время как Windows Messenger 5.0 и Xbox еще тестируются.

Широковещательные рассылки UPnP разрешены только в пределах локальной сети.

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

17.2.1 Конфигурирование UPnP

В подменю **Site Map** главного меню щелкните на **UPnP** в разделе **Advanced Setup (Дополнительные настройки)** для перехода к следующему экрану.

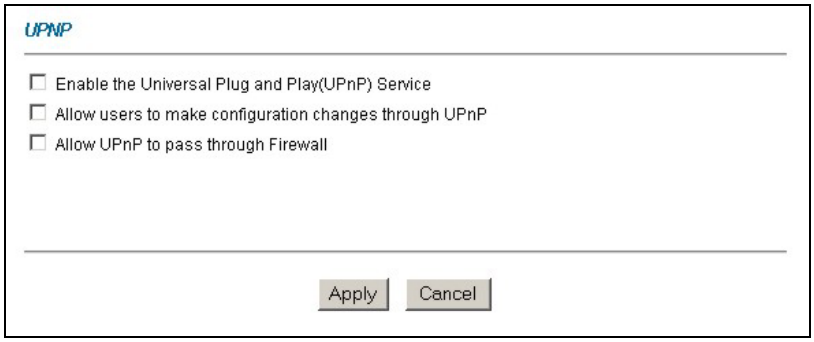


Рис. 17-1 Конфигурирование UPnP

В следующей таблице даны описания полей данного меню.

Табл. 17-1 Конфигурирование UPnP

ПОЛЕ	ОПИСАНИЕ

Табл. 17-1 Конфигурирование UPnP

ПОЛЕ	ОПИСАНИЕ
Enable the Universal Plug and Play (UPnP) Service (Включить службу UPnP)	Установите флажок для активирования UPnP. Помните, что каждый может использовать приложения UPnP, чтобы открыть окно ввода пароля Web-конфигуратора, не вводя IP-адрес Prestige (хотя для доступа к Web-конфигуратору остается необходимым ввод пароля).
Allow users to make configuration changes through UPnP (Позволить пользователям вносить изменения в конфигурацию через UPnP)	Установите флажок, чтобы разрешить UPnP-совместимым приложениям автоматически конфигурировать Prestige, чтобы связываться через Prestige. Например, используя NAT Traversal, приложения UPnP автоматически резервируют порт переадресации NAT, чтобы иметь возможность общаться с другим UPnP-совместимым устройством; это предотвращает необходимость ручной настройки порта пересылки для UPnP-совместимых приложений.
Allow UPnP to pass through Firewall (Позволить UPnP проходить через межсетевой экран)	Установите флажок, чтобы разрешить трафику от UPnP-совместимых приложений обходить межсетевой экран. Снимите флажок, чтобы обеспечить блокировку межсетевым экраном всех пакетов от UPnP-совместимых приложений (например, MSN-пакетов).
Apply (Применить)	Щелкните **Apply (Применить)** для сохранения настроек Prestige.
Cancel (Отмена)	Щелкните на **Cancel**, чтобы вернуться к ранее сохраненным настройкам.

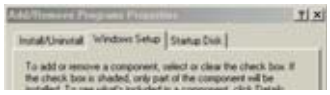
17.3 Пример установки UPnP в Windows

В данном разделе показано, как установить UPnP в Windows Me и Windows XP.

Установка UPnP в Windows Me

Выполните следующие действия для установки UPnP в Windows Me.

Step 17. Щелкните **Start (Пуск)**, **Control Panel (Панель управления)**. Дважды щелкните **Add/Remove Programs (Установка и удаление программ)**.



Step 18. Щелкните закладку **Windows Setup (Установка компонентов Windows)** и выберите **Communication (Связь)** в поле **Components (Компоненты)**. Щелкните **Details (Дополнительно)**.

Step 19. В окне **Communications (Связь)** установите флажок **Universal Plug and Play** в поле **Components (Компоненты)**.

Step 20. Щелкните **OK** для возврата в окно **Add/Remove Programs Properties (Свойства установки/удаления программ)** и щелкните **Next (Далее)**.

Step 21. После появления соответствующего сообщения перезапустите компьютер.

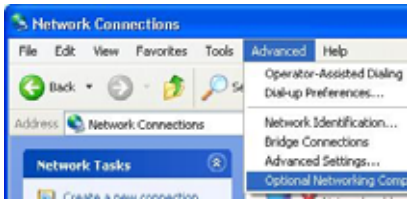
Установка UPnP в Windows XP

Выполните следующие действия для установки UPnP в Windows XP.

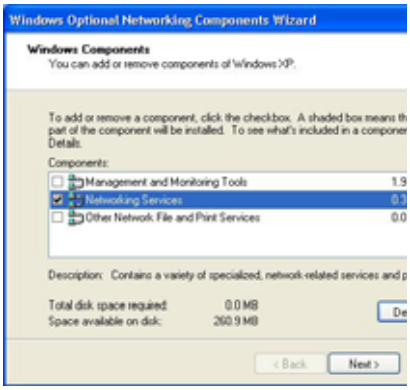
Step 1. Щелкните **Start** (Пуск), **Control Panel** (Панель управления).

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

Step 3. В окне Network Connections (Сетевые подключения) щелкните Advanced (Дополнительно) в главном меню и выберите Optional Networking Components … (Дополнительные сетевые компоненты...). Появится окно Windows Optional Networking Components Wizard (Мастер дополнительных сетевых компонентов Windows).

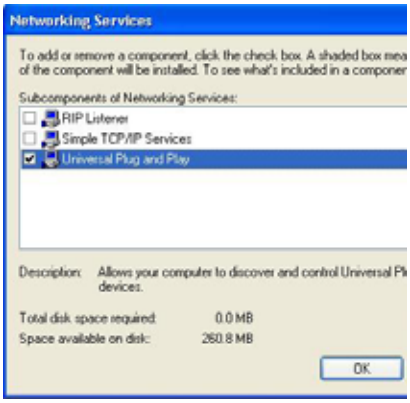


Step 4. Выберите **Networking Service (Сетевая служба)** в поле **Components (Компоненты)** и щелкните **Details (Дополнительно)**.



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

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



17.4 Пример использования UPnP в Windows XP

В этом разделе показано, как использовать функцию UPnP в Windows XP. Вы уже должны установить UPnP в Windows XP и активировать UPnP на Prestige.

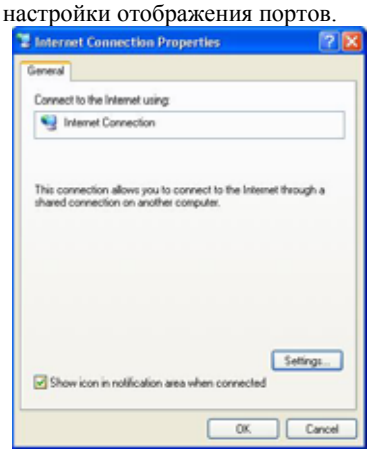
Следует убедиться, что компьютер подключен к порту локальной сети Prestige. Включить компьютер и Prestige.

Автоматическое обнаружение Вашего UPnP-совместимого сетевого устройства

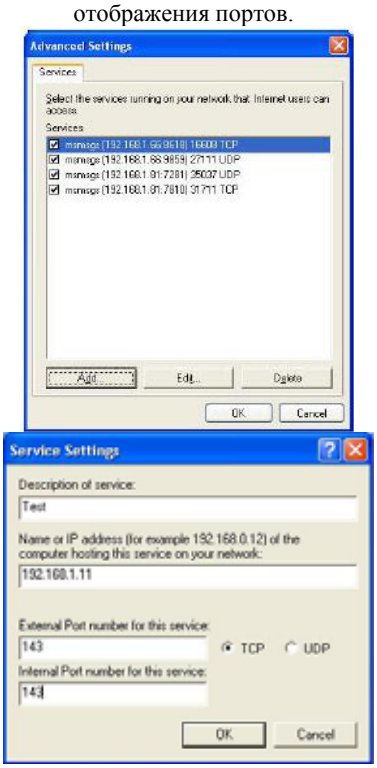
Step 7. Щелкните **Start (Пуск)**, **Control Panel (Панель управления)**. Дважды щелкните на **Network Connections (Сетевые подключения)**. В разделе Internet Gateway (Шлюз в Интернет) отображается иконка.

Step 8. Щелкните правой кнопкой мыши на иконке и выберите **Properties (Свойства)**.

Step 9. В окне **Internet Connection Properties (Свойства подключения к Интернет)**, щелкните **Settings (Настройки)**, чтобы просмотреть автоматически созданные настройки отображения портов.

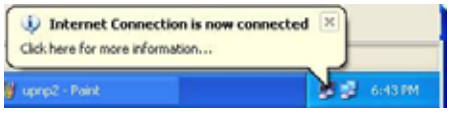


Step 10. Вы можете редактировать или удалять отображения портов, или щелкнуть **Add (Добавить)**, чтобы вручную добавить отображения портов.



При отключении UPnP-совместимого устройство от компьютера все отображения портов автоматически стираются.

Step 1. Выберите Show icon in notification area when connected (Отображать значок при подключении) и щелкните OK. Иконка отображается на системной панели



Step 2. Дважды щелкните иконку для отображения текущего состояния подключения к Интернету.

Простой доступ к Web-конфигуратору

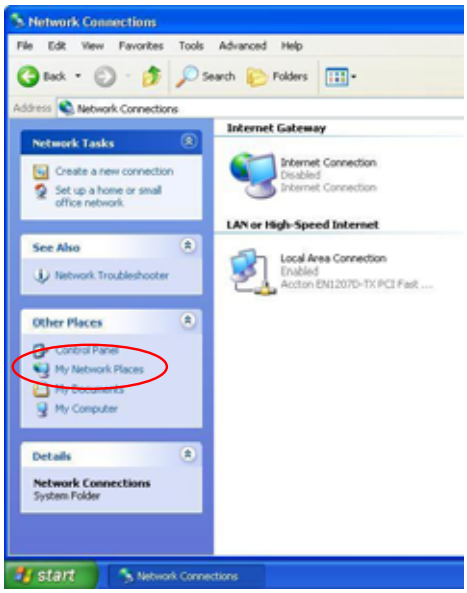
С помощью UPnP вы можете получить доступ к программе конфигурирования Prestige на основе Web без предварительного выяснения его IP-адреса. Это может оказаться полезным, если Вы не знаете IP-адрес Prestige.

Выполните следующие действия для доступа к Web-конфигуратору.

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

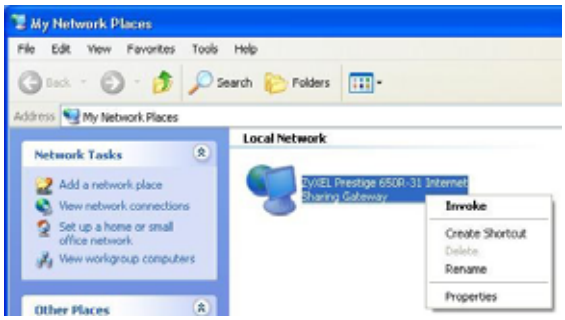
Step 2. Дважды щелкните на **Network Connections (Сетевые подключения)**.

Step 3. Выберите **My Network Places (Мое сетевое окружение)** в разделе **Other Places (Другие места)**.



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

Step 5. Щелкните правой кнопкой мыши на иконке Prestige и выберите **Invoke (Запустить)**. Появится окно ввода пароля Web-конфигуратора.



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

Раздел 18
Окна журналов

В этой главе содержится информация о конфигурировании общих настроек журналов и просмотре журнальных записей Prestige. В *приложении приводятся примеры расшифровки журнальных записей.*

18.1 Обзор журналов

Web-конфигуратор позволяет выбирать категории событий и/или предупреждений, заносимых в журнал, а также выводить журнальные записи или отсылать их из устройства Prestige администратору (по указанному адресу электронной почты) или на сервер системного журнала.

18.1.1 Предупреждения и журнальные записи

Предупреждения требуют более серьезного внимания, чем другие журнальные записи. В их число входят сообщения о системных ошибках, атаках (управлении доступом) и попытках доступа к заблокированным web-сайтам. Некоторые категории - например, **System Errors** (**Системные ошибки**) - включают как журнальные записи, так и предупреждения. Отличить их можно по цвету записи в окне **View Log**. Предупреждения отображаются красным цветом, а журнальные записи - черным.

18.2 Конфигурирование настроек журналов

Окно **Log Settings** используется для конфигурирования адресов, по которым Prestige отправляет журнальные записи, а также составления расписания отправки Prestige журнальных записей и определения того, какие журнальные записи и/или предупреждения Prestige должен регистрировать.

Для изменения настроек журналов Prestige щелкните на **Logs**, затем на **Log Settings**. На экране появится изображенное ниже окно.

Предупреждения отправляются по электронной почте по мере их появления. Журналы могут отправляться по электронной почте по заполнению журнала(см. **Log Schedule (график журнала)**). Выбор многих предупреждений и/или категорий журналов (особенно **Access Control** (контроль доступа)) может привести к отправке большого числа сообщений электронной почты.

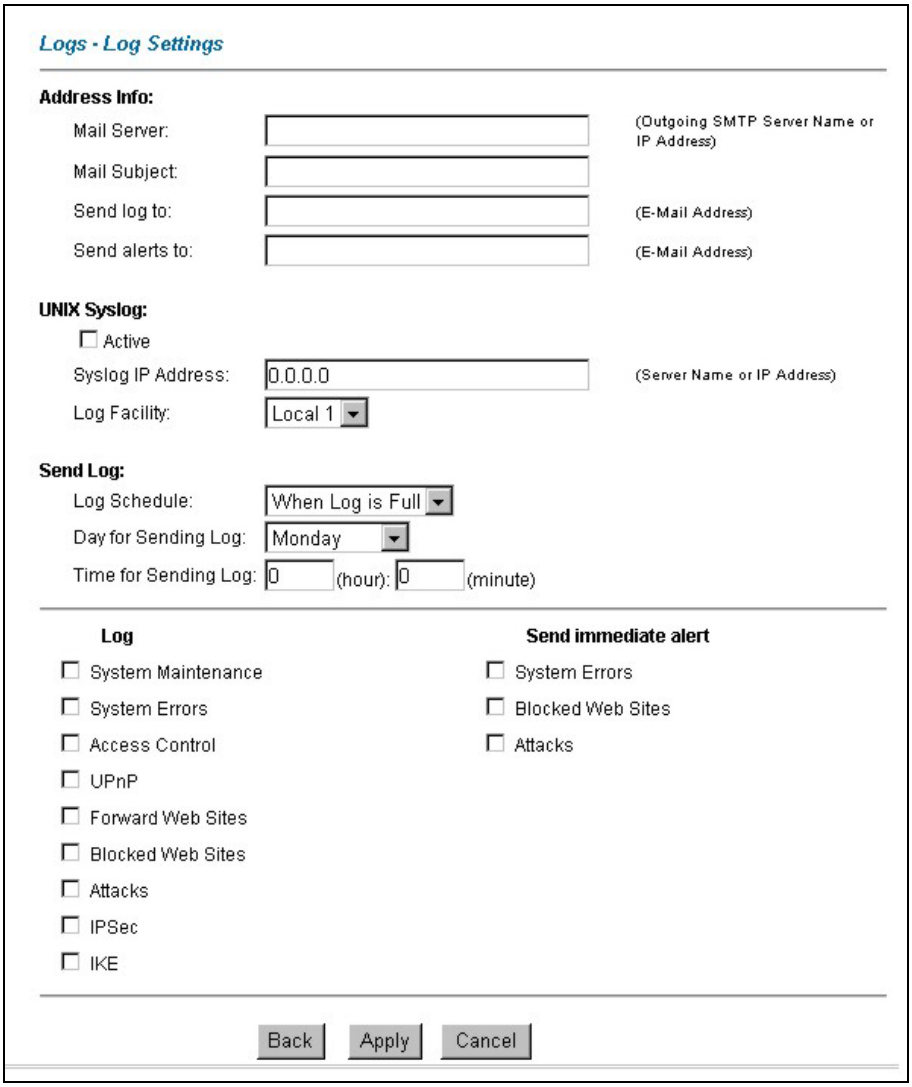


Рис. 18-1 Настройки журналов

В следующей таблице даны описания полей данного меню.

Табл. 18-1 Настройки журналов

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, журнальные записи и предупреждающие сообщения не будут высылаться по электронной почте.
Mail Subject (Тема сообщения)	Введите заголовок, который будет использоваться в качестве темы сообщений электронной почты с журнальными записями, отправляемыми Prestige.
Send log to (Адрес отправки журнала)	Журнальные записи отправляются на адрес электронной почты, указанный в данном поле. Если не заполнять это поле, журнальные записи не будут высылаться по электронной почте.
Send log to (Адрес отправки предупреждающих сообщений)	Предупреждающие сообщения отправляются на адрес электронной почты, указанный в данном поле. Если не заполнять это поле, предупреждающие сообщения не будут высылаться по электронной почте.
UNIX Syslog (Системный журнал UNIX)	Системный журнал отправляет журнал на внешний Syslog сервер, используемый для хранения журналов.
Active (Активно)	Щелкните на **Active**, чтобы включить системный журнал.
Syslog IP Address (IP-адрес системного журнала)	Введите имя или IP-адрес сервера системного журнала, который будет регистрировать выбранные категории журнальных записей.
Log Facility (Функция журнальной регистрации)	Выберите местонахождение из раскрывающегося списка. Функция журнальной регистрации дает возможность регистрировать сообщения в различных файлах на сервере системного журнала. Дополнительную информацию см. в руководстве вашей программы системного журнала.
Send Log (Отправка журнала)	
Log Schedule (План журнальной регистрации)	В этом раскрывающемся меню задается частота отправки журнальных записей по электронной почте: • **Daily (ежедневно)** • **Weekly (еженедельно)** • **Hourly (ежечасно)** • **When Log is Full (когда журнал заполнен)** • **None (никогда).** При выборе опции **Weekly** или **Daily** необходимо указать время суток для рассылки сообщений электронной почты. При выборе опции **Weekly** также необходимо указать день недели для рассылки сообщений. При выборе опции **When Log is Full** сообщение посылается только, когда журнал заполнен. При выборе **None** сообщения не высылаются.
Day for Sending Log (День рассылки журнала)	Выберите из раскрывающегося списка день недели, в который должны посылаться журнальные записи.
Time for Sending Alerts (Время рассылки журнальных записей)	Введите время суток в 24-часовом формате (например, 23:00 означает 11:00 пополудни), в которое должна производиться рассылка журнальных записей.

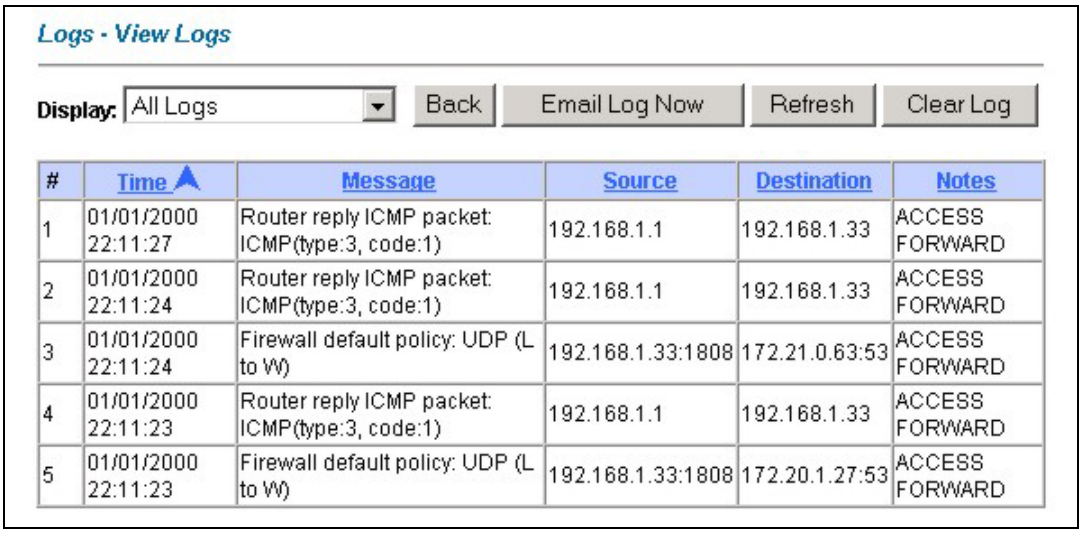
Табл. 18-1 Настройки журналов

ПОЛЕ	ОПИСАНИЕ
Log (Журнал)	Выберите категории журнальных записей для регистрации. Предупреждения входят в число журнальных записей.
Send Immediate Alert (Немедленная отправка предупреждений)	Выберите категории предупреждений, сообщения о которых Prestige должен немедленно высылать по адресу электронной почты, указанному в поле **Send Alerts To**.
Back (Назад)	Щелкните на **Back**, чтобы перейти к предыдущему окну.
Apply (Применить)	Щелкните на **Apply**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отмена)	Щелкните на **Cancel**, чтобы вернуться к ранее сохраненным настройкам.

18.3 Отображение журнальных записей

Щелкните на **Logs** и на **View Log**, чтобы открыть окно **View Logs**. Окно **View Logs** используется для просмотра журналов, принадлежащих к категориям, выбранным в окне **Log Settings** (см. *раздел 18.2*).

Красный цвет журнальной записи указывает на предупреждающее сообщение. После заполнения журнала новые записи производятся на месте старых, которые удаляются. Щелкните на заголовке столбца для упорядочивания содержащихся в нем записей. Треугольник указывает на возрастающий или убывающий порядок расположения записей.



#	Time	Message	Source	Destination	Notes
1	01/01/2000 22:11:27	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
2	01/01/2000 22:11:24	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
3	01/01/2000 22:11:24	Firewall default policy: UDP (L to W)	192.168.1.33:1808	172.21.0.63:53	ACCESS FORWARD
4	01/01/2000 22:11:23	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
5	01/01/2000 22:11:23	Firewall default policy: UDP (L to W)	192.168.1.33:1808	172.20.1.27:53	ACCESS FORWARD

Рис. 18-2 Просмотр журналов

В следующей таблице даны описания полей данного меню.

Таблица 18-2 Просмотр журналов

ПОЛЕ	ОПИСАНИЕ
Display (Отображение)	Категории, выбранные в окне **Log Settings** (см. *раздел 18.2*) отображаются в раскрывающемся списке. Выберите категорию журнальных записей для просмотра; для просмотра всех журналов из всех категорий, выбранных в окне **Log Settings**, выберите опцию **All Logs**.
Time (Время)	В этом поле отображается время регистрации записи. Информацию о настройке времени и даты в Prestige см. в главе о сопровождении системы и системной информации.
Message (Сообщение)	В этом поле указывается причина возникновения записи.
Source (Источник)	В этом поле указывается IP-адрес и номер порта источника входящего пакета.
Destination (Адресат)	В этом поле указывается IP-адрес и номер порта адресата входящего пакета.
Notes (Примечания)	В этом поле указывается дополнительная информация о журнальной записи.
Back (Назад)	Щелкните на **Back**, чтобы перейти к предыдущему окну.
Email Log Now (Отправить журнал)	Щелкните на **Email Log Now**, чтобы отправить окно журнала по адресу электронной почты, определенному в окне **Log Settings** (проверьте, что поля **Address Info** в окне **Log Settings** заполнены, см. *раздел 18.2*).
Refresh (Обновить)	Щелкните на **Refresh**, чтобы обновить окно журнала.
Clear Log (Очистить журнал)	Щелкните на **Clear Log**, чтобы удалить все записи.

18.4 Сообщения об ошибках SMTP

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

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

Таблица 18-3 Сообщения об ошибках SMTP

-1 означает, что Prestige выключен из сети
-2 означает ошибку tcp SYN fail
-3 означает ошибку smtp server OK fail
-4 означает ошибку HELO fail
-5 означает ошибку MAIL FROM fail

Таблица 18-4 Сообщения об ошибках SMTP

-6 означает ошибку RCPT TO fail
-7 означает ошибку DATA fail
-8 означает ошибку mail data send fail

18.4.1 Пример журнала, высылаемого по E-mail

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

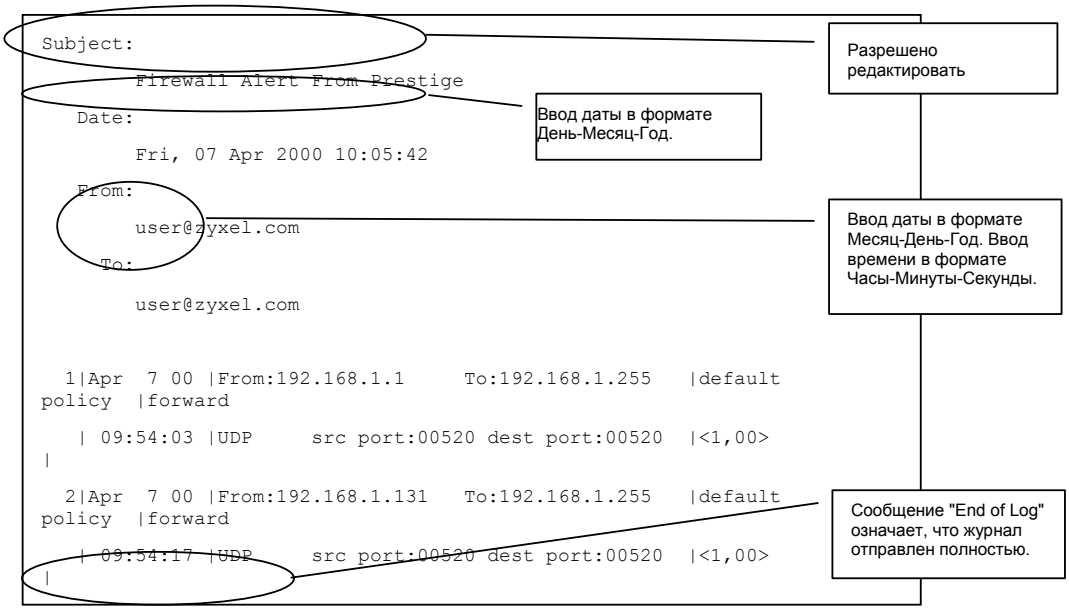


Рис. 18-3 Пример журнала, высланного по электронной почте

Глава VI:

Управление пропускной способностью

В этой части содержится информация о функциях и конфигурировании системы управления пропускной способностью.

Раздел 19
Управление пропускной способностью

эта глава описывает функции и конфигурацию системы управления пропускной способностью.

19.1 Обзор управления пропускной способностью

Управление пропускной способностью позволяет распределить выходную производительность интерфейса по конкретным типам трафика. Оно также помогает обеспечить перенаправление Prestige определенных типов трафика (в частности, приложений, работающих в режиме реального времени) с минимальной задержкой. По мере расширения использования приложений, работающих в режиме реального времени - например, систем Voice-over-IP (VoIP), потребности в распределении пропускной способности также растут.

Управление пропускной способностью решает следующие вопросы:

- Кто и в каком количестве получает доступ к определенным приложениям?
- Какие уровни приоритета следует присваивать различным типам трафика?
- Доставка какого трафика должна быть гарантирована?
- Какая пропускная способность должна быть выделена под гарантированную доставку?

Управление пропускной способностью также позволяет конфигурировать возможный выходной поток интерфейса в соответствии с возможностями сети. Это помогает уменьшить задержки и потери пакетов на следующем устройстве маршрутизации. Например, Вы можете установить скорость интерфейса WAN на 1000 Кбит/с, если соединение ADSL имеет скорость исходящего потока, равную 1000 Кбит/с. Все значения в конфигурационных окнах измеряются в Кбит/с (килобитах в секунду), но в настоящем *Руководстве пользователя* для краткости также используются Мбит/с (мегабиты в секунду).

19.2 Классы и фильтры пропускной способности

Классы и дочерние классы пропускной способности используются для распределения конкретных объемов (бюджетов) пропускной способности. Конфигурация фильтра пропускной способности определяет класс (или дочерний класс) пропускной способности, соответствующий конкретному приложению и/или подсети. Закладка **Class Configuration** (см. *раздел 19.9.1*) используется для определения имени класса пропускной способности, распределения пропускной способности и фильтра пропускной способности. Для каждого класса пропускной способности Вы можете сконфигурировать не более одного фильтра пропускной способности. Вы можете также конфигурировать классы пропускной способности без фильтров пропускной способности. Для классов, сконфигурированных без фильтров, однако, рекомендуется сконфигурировать дочерние классы, имеющие фильтры. Prestige оставляет бюджет пропускной способности для класса, который не имеет ни фильтра, ни дочерних классов с фильтрами, распределенным и неиспользуемым.

Просмотреть сконфигурированные классы и дочерние классы пропускной способности можно в закладке **Class Setup** (подробности см. в *разделе 19.9*).

Сумма сконфигурированных бюджетов пропускной способности всех дочерних классов не может быть больше, чем сконфигурированная пропускная способность родительского класса.

19.3 Пропорциональное распределение пропускной способности

Управление пропускной способностью позволяет определять пропускную способность, выделяемую каждому классу; однако, реальная пропускная способность, которую может использовать каждый класс, уменьшается пропорционально доступной пропускной способности.

19.4 Примеры использования управления пропускной способностью

В этих примерах показано управление пропускной способностью на интерфейсе WAN, настроенном на 640 Кбит/с.

19.4.1 Пример управления пропускной способностью с учетом приложений

Классы пропускной способности в следующем примере созданы только с учетом приложений. Каждому класс пропускной способности (VoIP, Web, FTP, E-mail и Video) выделено по 128 Кбит/с.

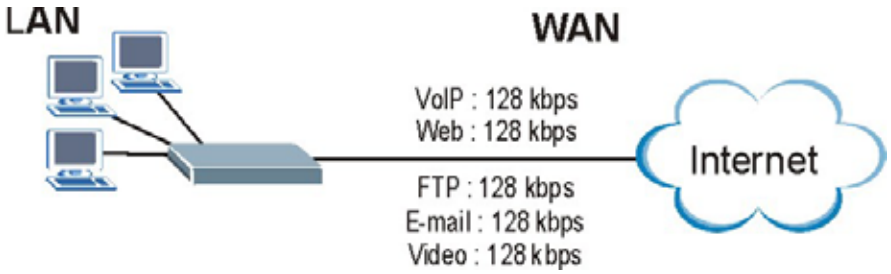


Рис.19-1 Пример управления пропускной способностью с учетом приложений

19.4.2 Пример управления пропускной способностью с учетом подсетей

Классы пропускной способности в следующем примере созданы только с учетом подсетей LAN. Каждому классу пропускной способности (Подсеть A и Подсеть B) выделено по 320 Кбит/с.

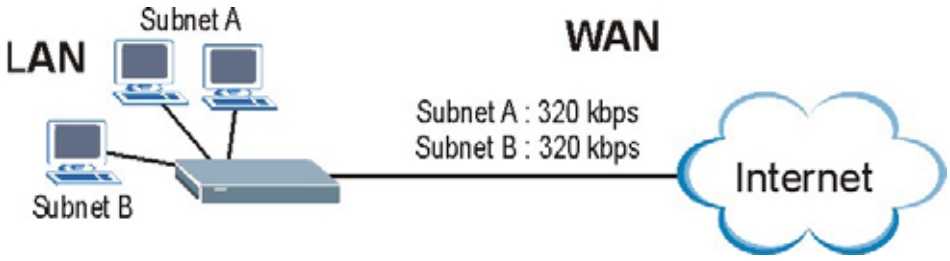


Рис.19-2 Пример управления пропускной способностью с учетом подсетей

19.4.3 Пример управления пропускной способностью с учетом приложений и подсетей

Классы пропускной способности в следующем примере созданы с учетом подсетей LAN и приложений (пропускная способность выделяется конкретным приложениям в каждой подсети).

Таблица 19-1Пример управления пропускной способностью с учетом 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

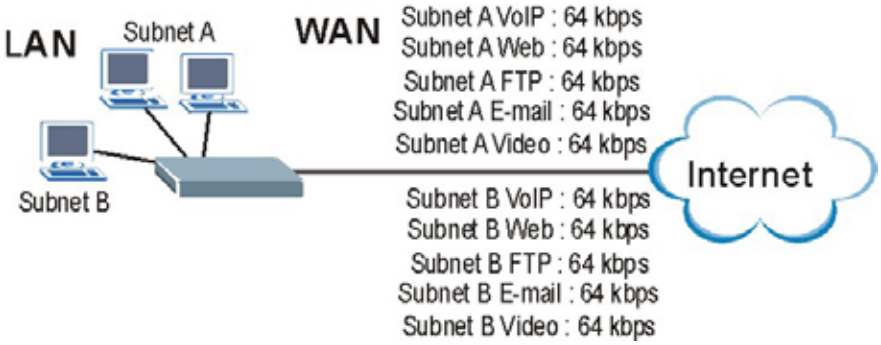


Рис.19-3 Пример управления пропускной способностью с учетом приложений и подсетей

19.5 Планировщик

Планировщик распределяет пропускную способность интерфейса между классами пропускной способности. В Prestige имеются два типа планировщиков: на принципе равнодоступности и опирающийся на приоритеты.

19.5.1 Планировщик, базирующийся на приоритетах

При помощи планировщика, базирующегося на приоритетах, Prestige пересылает трафик из классов пропускной способности в соответствии с присвоенными им приоритетами. Чем больше число, определяющее приоритет класса пропускной способности, тем выше приоритет. Приложениям, работающим в режиме реального времени (например, использующим аудио или видеосигналы) следует назначать более высокий приоритет для обеспечения их бесперебойной работы.

19.5.2 Планировщик на принципе равнодоступности

При использовании планировщика на принципе равнодоступности Prestige распределяет пропускающую способность между классами пропускной способности поровну; это исключает использование одним классом пропускной способности всей пропускной способности интерфейса.

19.6 Максимизация использования пропускной способности

Опция максимизации использования пропускной способности (см. *Рис. 19-7*) позволяет Prestige распределить всю доступную пропускную способность интерфейса (включая нераспределенную пропускную способность и любую распределенную пропускную способность, не используемую классом) между классами пропускной способности, которым требуется дополнительная пропускная способность.

При включении этой опции, Prestige сначала проверяет использование каждым классом пропускной способности всей выделенной ему пропускной способности. Затем Prestige распределяет доступную пропускную способность интерфейса (пропускную способность, которая осталась нераспределенной или не используется классами) в зависимости от количества классов пропускной способности, которым требуется дополнительная пропускная способность, и уровней их приоритета . Если дополнительная пропускная способность требуется только одному классу, Prestige предоставляет дополнительную пропускную способность этому классу.

Если дополнительная пропускная способность требуется нескольким классам, Prestige в первую очередь предоставляет доступную пропускную способность классам с самым высоким приоритетом (в необходимом им количестве, если имеется достаточно доступной пропускной способности), а затем - классам с более низким приоритетом, если пропускная способность еще остается. Классам с одинаковым уровнем приоритета Prestige распределяет равное количество пропускной способности.

19.6.1 Резервирование пропускной способности для трафика вне классов пропускной способности

Для конфигурирования в Prestige возможности выделения пропускной способности для трафика, не определенного в фильтре пропускной способности, следует выполнить следующие три операции.

1. Оставить часть пропускной способности интерфейса не приписанной.
2. Не включать опцию **Maximize Bandwidth Usage** интерфейса.
3. Не включать заимствование пропускной способности для дочерних классов, родительским классом которых является корневой класс (см. *раздел 19.7*).

19.6.2 Пример максимизации использования пропускной способности

В приведенном примере функция максимизации использования пропускной способности Prestige включена на интерфейсе. На первой схеме показаны бюджет пропускной способности и приоритет каждого класса пропускной способности. Классы организованы в соответствии с подсетями. Интерфейс настроен на 10 Мбит/с. Каждой подсети выделено 2 Мбит/с. Нераспределенные 2 Мбит/с позволяют организовывать исходящий трафик, не определенный в фильтрах пропускной способности, если опция максимизации использования пропускной способности отключена.

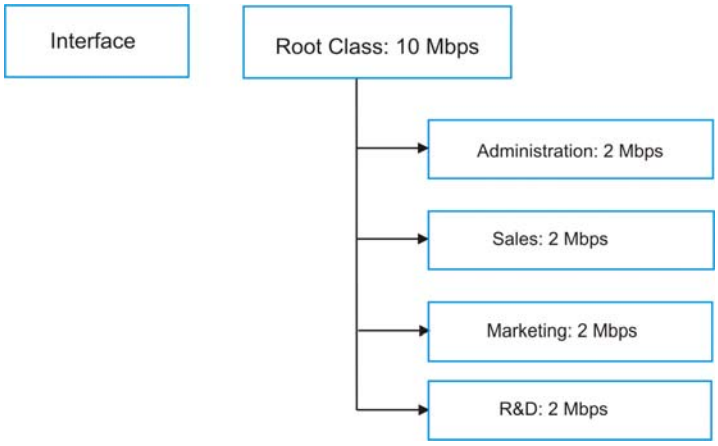


Рис. 19-4 Пример распределения пропускной способности

На следующем рисунке показано использование пропускной способности при включенной опции максимизации использования пропускной способности. Prestige распределяет нераспределенные 2 Мбит/с между классами, которым требуется дополнительная пропускная способность. Если административные подразделения используют только 1 Мбит/с из выделенных ей 2 Мбит/с, Prestige также распределяет оставшийся 1 Мбит/с между классами, которым требуется дополнительная пропускная способность. Таким образом, всего Prestige распределяет 3 Мбит/с нераспределенной и

неиспользуемой пропускной способности между классами, которым требуется дополнительная пропускная способность.

Предположим, что всем классам кроме административного требуется дополнительная пропускная способность.

- Каждый класс получает выделенную ему пропускную способность. Класс Administration использует только 1 Мбит/с из выделенных ему 2 Мбит/с.
- Sales и Marketing первыми получают дополнительную пропускную способность, т. к. они имеют самый высокий приоритет (6). Если каждому из них требуется 1,5 Мбит/с или более дополнительной пропускной способности, Prestige распределит 3 Мбит/с нераспределенной и неиспользуемой пропускной способности поровну между Sales и Marketing (по 1,5 Мбит/с дополнительно каждому, т. е. всего по 3,5 Мбит/с каждому), т. к. оба они имеют самый высокий уровень приоритета.
- R&D также нуждается в дополнительной пропускной способности, но получает только выделенные ему 2 Мбит/с, т. к. вся нераспределенная и неиспользуемая пропускная способность выделяется классам Sales и Marketing, имеющим более высокий приоритет.
- Prestige не отправляет никакого трафика, не определенного в фильтрах пропускной способности, т. к. вся нераспределенная пропускная способность отдается классам, которые в ней нуждаются.

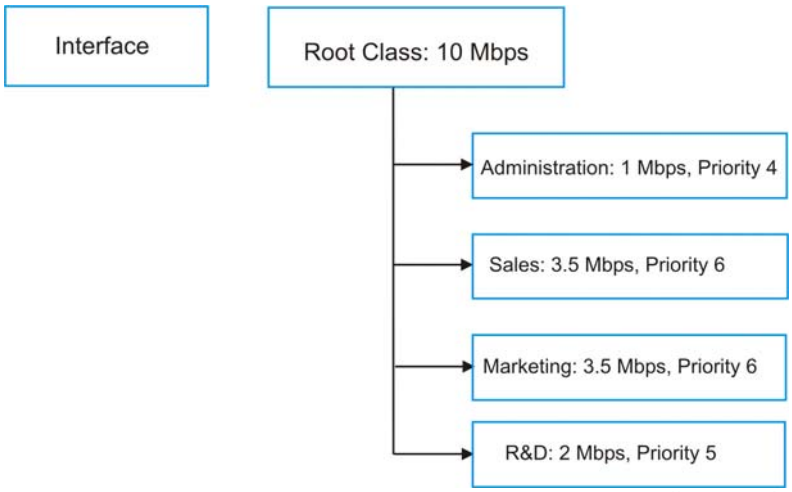


Рис. 19-5 Пример максимизации использования пропускной способности

19.7 Заимствование пропускной способности

Заимствование пропускной способности позволяет дочернему классу заимствовать неиспользуемую пропускную способность у родительского класса, а максимизации использования пропускной

способности позволяет классам пропускной способности заимствовать нераспределенную или неиспользуемую пропускную способность во всем интерфейсе.

Включение заимствования пропускной способности для дочернего класса позволит этому дочернему классу использовать неиспользуемую пропускную способность его родительского класса. Неиспользуемая пропускная способность родительского класса отдается в первую очередь дочернему классу с самым высоким приоритетом. Дочерний класс может также заимствовать пропускную способность у класса более высокого уровня (прародительского класса), если родительскому классу этого дочернего класса также разрешено заимствовать пропускную способность у своего родительского класса. Этот принцип может сохраняться для любого количества уровней, если на них разрешено заимствование пропускной способности у соответствующих родительских классов (см. *раздел 19.7.1*).

Суммарная пропускная способность, предоставленная всем дочерним классам, не может быть больше, чем пропускная способность, предоставленная их родительскому классу. Для распределения неиспользуемой пропускной способности родительского класса между дочерними классами в Prestige используется планировщик.

19.7.1 Пример заимствования пропускной способности

Ниже приводится пример управления пропускной способностью с конфигурацией классов, допускающей заимствование пропускной способности. Классы соответствуют отделам и людям в некоторых из отделов.

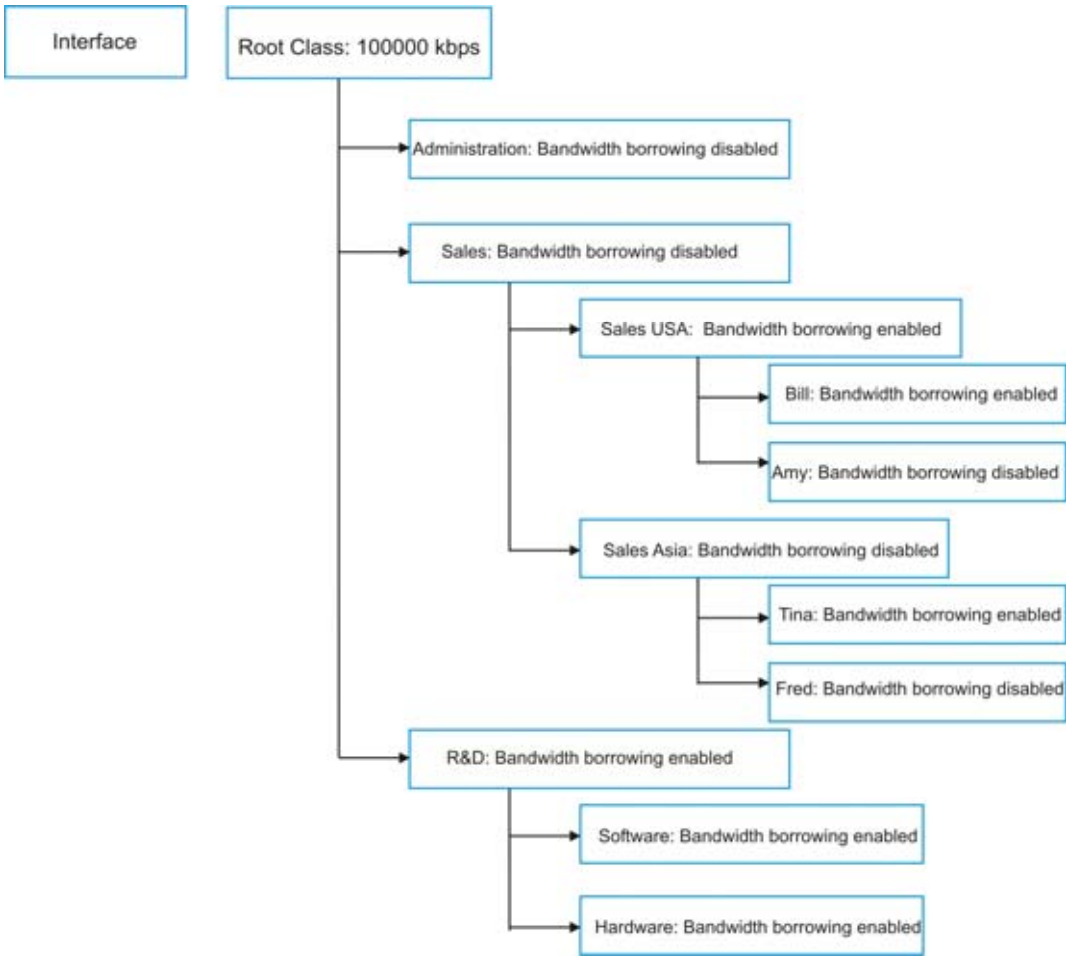


Рис. 19-6 Пример заимствования пропускной способности

- Класс Bill может заимствовать неиспользуемую пропускную способность у класса Sales USA, т. к. классу Bill разрешено заимствование пропускной способности.
- Класс Bill также может заимствовать неиспользуемую пропускную способность у класса Sales, т. к. классу Sales USA также разрешено заимствование пропускной способности.

- Класс Bill не может заимствовать неиспользуемую пропускную способность у класса Root, т. к. классу Sales не разрешено заимствование пропускной способности.
- Класс Amy не может заимствовать неиспользуемую пропускную способность у класса Sales USA, т. к. классу Amy не разрешено заимствование пропускной способности.
- Классы R&D Software и Hardware могут заимствовать неиспользуемую пропускную способность у класса R&D, т. к. обоим этим классам разрешено заимствование пропускной способности.
- Классы R&D Software и Hardware также могут заимствовать неиспользуемую пропускную способность у класса Root, т. к. классу R&D также разрешено заимствование пропускной способности.

19.7.2 Максимизация использования пропускной способности с заимствованием пропускной способности

При параллельном включении опций максимизации использования пропускной способности (на интерфейсе) и заимствование пропускной способности (на отдельных дочерних классах), Prestige работает следующим образом.

1. Prestige распределяет трафик в соответствии с бюджетом каждого класса пропускной способности.
2. Prestige предоставляет неиспользуемую пропускную способность родительского класса его дочерним классам, имеющим больший трафик, чем позволяет их бюджет, и имеющим разрешение на заимствование пропускной способности. Prestige в первую очередь предоставляет пропускную способность дочерним классам с более высоким приоритетом и предоставляет равные условия классам пропускной способности с одинаковым приоритетом.
3. Prestige распределяет оставшуюся на интерфейсе неиспользуемую или нераспределенную пропускную способность любому классу пропускной способности, которому она необходима. Prestige в первую очередь предоставляет пропускную способность классам с более высоким приоритетом и предоставляет равные условия классам пропускной способности с одинаковым приоритетом.
4. Prestige распределяет оставшуюся нераспределенную пропускную способность трафику, не соответствующему ни одному из классов пропускной способности.

19.8 Конфигурирование сводки

Щелкните **Media Bandwidth Management**, затем **Summary**, чтобы открыть окно, как показано ниже.

Включите управление пропускной способностью на интерфейсе и установите максимально допустимую для этого интерфейса пропускную способность.

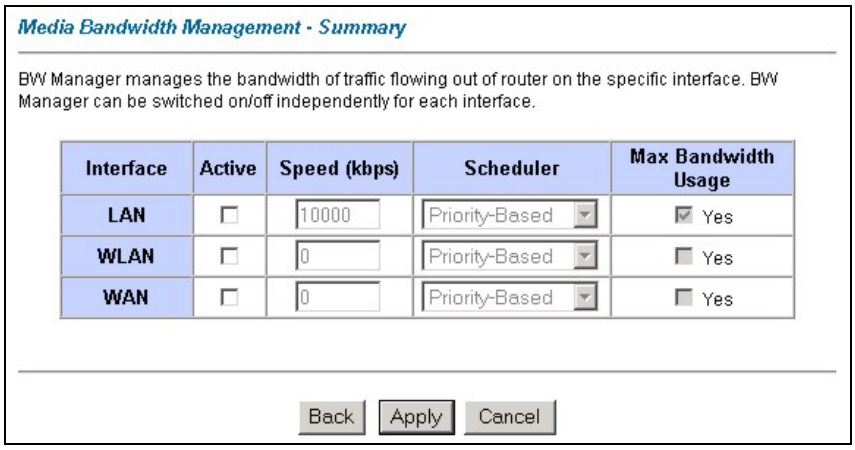


Рис. 19-7 Управление пропускной способностью: Сводка

В следующей таблице даны описания полей данного окна.

Таблица 19-2 Управление пропускной способностью: Сводка

ПОЛЕ	ОПИСАНИЕ
LAN WLAN WAN	Эти поля, открытые только для чтения, соответствуют физическим интерфейсам. Отметьте галочку интерфейса для включения управления пропускной способностью для этого интерфейса. Управление пропускной способностью применяется ко всему трафик, исходящему из маршрутизатора через интерфейс, вне зависимости от источника трафика. Перенаправление трафика или IP alias могут привести к прохождению трафика LAN-to-LAN трафика через Prestige и влияния на него механизма управления пропускной способностью.
Active (Активно)	Отметьте интерфейс, чтобы включить управление пропускной способностью на этом интерфейсе.
Speed (kbps) (Скорость (Кбит/с))	Введите для этого интерфейса пропускную способность, которую Вы хотите распределить при помощи управления пропускной способностью. Это значение будет определять пропускную способность для корневого класса этого интерфейса (см. *раздел 19.9*). Рекомендуется устанавливать эту скорость в соответствии с возможностями подключения интерфейса. Например, если соединение ADSL имеет скорость исходящего потока, равную 1000 Кбит/с, установите скорость интерфейса WAN, равную 1000 Кбит/с.

Таблица 19-2 Управление пропускной способностью: Сводка

ПОЛЕ	ОПИСАНИЕ
Scheduler (Планировщик)	Для управления потоком трафика выберите из раскрывающегося меню **Priority-Based** или **Fairness-Based**. При выборе **Priority-Based** предпочтение отдается классам пропускной способности с более высоким приоритетом. При выборе **Fairness-Based** все классы пропускной способности имеют равные возможности. См. *раздел 19.5*.
Maximize Bandwidth Usage (Максимизация использования пропускной способности)	Поставьте флажок в этом окошке для распределения Prestige всей нераспределенной и/или неиспользуемой пропускной способности интерфейса между классами пропускной способности, которым требуется дополнительная пропускная способность. Не отмечайте эту опцию, если Вы хотите зарезервировать пропускную способность для трафика, не соответствующего ни одному из классов пропускной способности (см. *раздел 19.6.1*), или ограничить скорость этого интерфейса (см. описание поля **Speed**).
Back (Назад)	Щелкните на кнопке **Back,** чтобы перейти к основному окну **Media Bandwidth Management**.
Apply (Применить)	Щелкните на **Apply** для сохранения настроек в Prestige.
Cancel (Отмена)	Щелкните на **Cancel**, чтобы начать настройку заново.

19.9 Конфигурирование настроек классов

Окно настройки классов отображает сконфигурированные классы пропускной способности по отдельным интерфейсам. Выберите интерфейс и щелкните на кнопках для проведения описанных ниже операций. Щелкните на “+”, чтобы развернуть дерево класса, и на “-“, чтобы свернуть его. У каждого интерфейса имеется постоянный корневой класс. Бюджет пропускной способности корневого класса равен скорости, установленной для интерфейса (о конфигурировании скорости интерфейса см. в *разделе 19.8*). Сконфигурируйте слои дочерних классов для корневого класса.

Чтобы добавить или удалить дочерний класс интерфейса, щелкните на **Media Bandwidth Management**., а затем на **Class Setup**. На экране появится следующее окно (с примерами классов).

В этом примере 10 Мбит/с нераспределенной пропускной способности резервируются для трафика, не определенного в фильтрах пропускной способности (см. *раздел 19.6.1*). Каждый из классов пропускной способности Administration и Sales USA имеет больший бюджет пропускной способности, чем суммарные бюджеты их дочерних классов. Дочерние классы могут заимствовать дополнительную пропускную способность, если им разрешено заимствование пропускной способности (см. *раздел 19.7*).

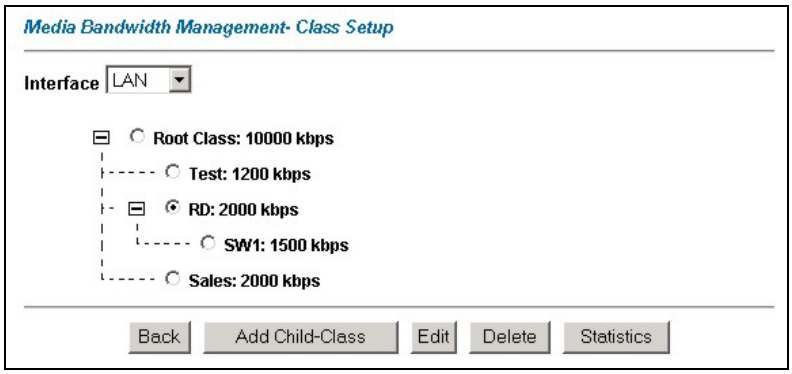


Рис. 19-8 Управление пропускной способностью: Настройка классов

В следующей таблице даны описания полей данного окна.

Таблица 19-3 Управление пропускной способностью: Настройка классов

ПОЛЕ	ОПИСАНИЕ
Interface (Интерфейс)	Выберите из раскрывающегося списка интерфейс, для которого Вы хотите определить классы.
Back (Назад)	Щелкните на **Back,** чтобы перейти к основному окну **Media Bandwidth Management**.
Add Child-Class (Добавить дочерний класс)	Щелкните на **Add Child-class**, чтобы добавить подкласс.
Edit (Редактировать)	Щелкните на **Edit** для редактирования выбранного класса. Корневой класс редактировать нельзя.
Delete (Удалить)	Щелкните на **Delete**, чтобы удалить класс и его дочерние классы. Корневой класс удалить нельзя.
Statistics (Статистика)	Щелкните на **Statistics**, чтобы отобразить статус выбранного класса.

19.9.1 Конфигурирование классов управления пропускной способностью

Конфигурирование классов управления пропускной способностью производится в окне **Class Configuration**. Перед конфигурированием классов для интерфейса Вы должны включить управление пропускной способностью для этого интерфейса в окне **Media Bandwidth Management - Summary**.

Для добавления дочернего класса щелкните на **Media Bandwidth Management**, затем на **Class Setup**. Щелкните на кнопке **Add Child-Class**, чтобы открыть следующее окно.

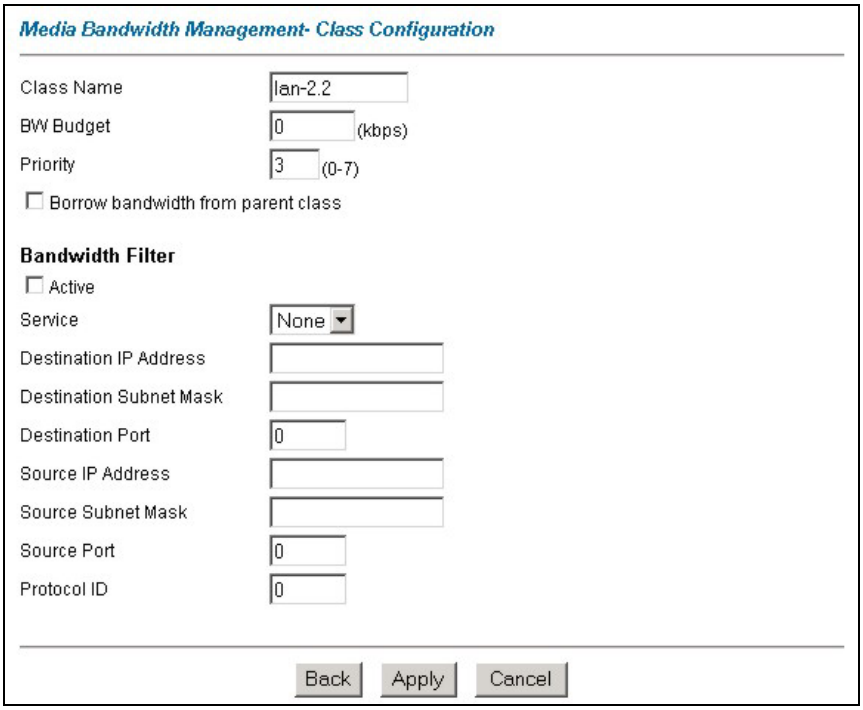


Рис. 19-9 Управление пропускной способностью: Конфигурирование классов

В следующей таблице даны описания полей данного окна.

Таблица 19-4 Управление пропускной способностью: Конфигурирование классов

ПОЛЕ	ОПИСАНИЕ
Class Name (Имя класса)	Используйте автоматически сгенерированное имя или введите идентифицирующее имя, включающее до 20 буквенно-цифровых символов, считая пробелы.
BW Budget (kbps) (Бюджет(Кбит/с))	Определите максимальную пропускную способность в Кбит/с, предоставляемую данному классу. Рекомендуется использовать для отдельных классов значения между 20 Кбит/с и 20 000 Кбит/с.
Priority (Приоритет)	Введите число от 0 до 7, определяющее приоритет данного класса. Чем больше это число, тем выше приоритет. Значение по умолчанию равно 3.

Таблица 19-4 Управление пропускной способностью: Конфигурирование классов

ПОЛЕ	ОПИСАНИЕ
Borrow bandwidth from parent class (Заимствовать пропускную способность у родительского класса)	Выберите эту опцию, чтобы разрешить дочернему классу заимствовать пропускную способность у родительского класса, если родительский класс не полностью использует свой бюджет пропускной способности. Заимствование пропускной способности регулируется приоритетами дочерних классов. Это значит, что дочерний класс с самым высоким приоритетом (7) первым получает возможность заимствования пропускной способности у родительского класса. Не выбирайте эту опцию для классов, расположенных непосредственно под корневым классом, если Вы хотите оставить пропускную способность для других типов трафика (см. *19.6.1*) или добиться соответствия скорости интерфейса возможностям следующего устройства в сети (см. описание поля **Speed** в *Таблица 19-2*).
Bandwidth Filter (Фильтр пропускной способности) Prestige использует фильтр пропускной способности для идентификации трафика, принадлежащего к некоторому классу пропускной способности.	
Active (Активно)	Поставьте флажок в этом окошке, если Вы хотите, чтобы Prestige использовал этот фильтр пропускной способности в управлении пропускной способностью.
Service (Услуга)	Вместо заполнения полей **Destination Port**, **Source Port** и **Protocol ID** Вы можете выбрать заранее определенную услугу. SIP (Session Initiation Protocol - Протокол инициализации соединения) - это протокол сигнализации, используемый в Интернет-телефонии, обмене быстрыми сообщениями и других приложениях VoIP (Voice over IP). Выберите **SIP** из раскрывающегося списка для конфигурирования этого фильтра пропускной способности для трафика, использующего SIP. В настоящий момент SIP является единственной заранее определенной услугой. При выборе **None** данный класс пропускной способности относится ко всем услугам, если одна из них не указана в полях **Destination Port**, **Source Port** и **Protocol ID**.
Destination IP Address (IP-адрес назначения)	Введите IP-адрес назначения в десятичном виде с разделительными точками Незаполненное поле IP-адреса назначения означает любой IP-адрес назначения.
Destination Subnet Mask (Маска подсети назначения)	Введите маску подсети назначения. Это поле недоступно, если не заполнено поле **Destination IP Address**. Подробнее об организации IP-подсетей см. в приложении.
Destination Port (Порт назначения)	Введите номер порта назначения. Незаполненное поле порта назначения означает любой порт назначения.
Source IP Address (IP-адрес источника)	Введите IP-адрес источника. Незаполненное поле IP-адреса источника означает любой IP-адрес источника.

Таблица 19-4 Управление пропускной способностью: Конфигурирование классов

ПОЛЕ	ОПИСАНИЕ
Destination Subnet Mask (Маска подсети источника)	Введите маску подсети источника. Это поле недоступно, если не заполнено поле **Source IP Address**. Подробнее об организации IP-подсетей см. в приложении.
Source Port (Порт источника)	Введите номер порта источника. Некоторые часто встречающиеся услуги и номера портов перечислены в следующей таблице. Незаполненное поле порта источника означает любой порт источника.
Protocol ID (Идентификатор протокола)	Введите номер идентификатора протокола (типа услуги), например: 1 - ICMP, 6 - TCP, 17 - UDP. Незаполненное поле идентификатора протокола означает любой номер протокола.
Back (Назад)	Щелкните на **Back,** чтобы перейти к основному окну **Media Bandwidth Management**.
Apply (Применить)	Щелкните на **Apply** для сохранения настроек в Prestige.
Cancel (Отмена)	Щелкните на **Cancel**, чтобы начать настройку заново.

Таблица 19-5 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 - "всемирная паутина")	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

19.9.2 Статистика управления пропускной способностью

Окно **Bandwidth Management Statistics** используется для получения информации о производительности сети. Щелкните на кнопке **Statistics** в окне **Class Setup**, чтобы открыть окно **Statistics**.

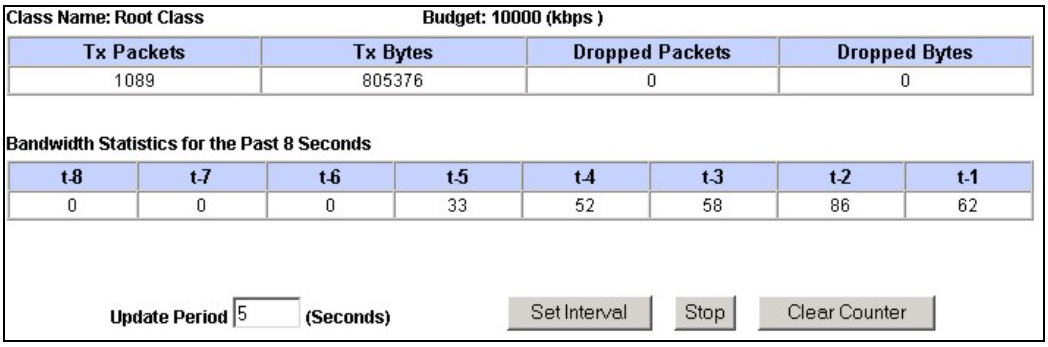


Рис. 19-10 Статистика управления пропускной способностью

В следующей таблице даны описания полей данного окна.

Таблица 19-6 Статистика управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Class Name (Имя класса)	В этом поле показано имя класса, к которому относится выводимая статистика.
Budget (kbps) (Бюджет (Кбит/с))	В этом поле показана пропускная способность, выделенная данному классу.
Tx Packets (Передано пакетов)	В этом поле показано полное количество переданных пакетов.
Tx Bytes (Передано байтов)	В этом поле показано полное количество переданных байтов.
Dropped Packets (Сброшено пакетов)	В этом поле показано полное количество сброшенных пакетов.
Dropped Bytes (Сброшено байтов)	В этом поле показано полное количество сброшенных байтов.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1 (Статистика по пропускной способности за последние 8 секунд))	
В этом поле показана статистика по пропускной способности (в битах в секунду) за последние 8 секунд. Например, t-1 означает одну последнюю секунду.	
Update Period (seconds) (Интервал обновления в секундах)	Введите интервал в секундах, определяющий частоту обновления информации.

Таблица 19-6 Статистика управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Set Interval (Установить интервал)	Щелкните на **Set Interval**, чтобы применить новый интервал обновления, введенный в расположенном выше поле **Update Period**.
Stop Update (Прекратить обновление)	Щелкните на **Stop Update**, чтобы запретить браузеру обновление статистики по управлению пропускной способностью .
Clear Counter (Очистить счетчик)	Щелкните на **Clear Counter**, чтобы удалить всю статистику по управлению пропускной способностью .

19.10 Монитор пропускной способности

Для просмотра использования и распределения пропускной способности в Prestige щелкните на **Media Bandwidth Management**, затем на **Monitor**. На экране появится изображенное ниже окно.

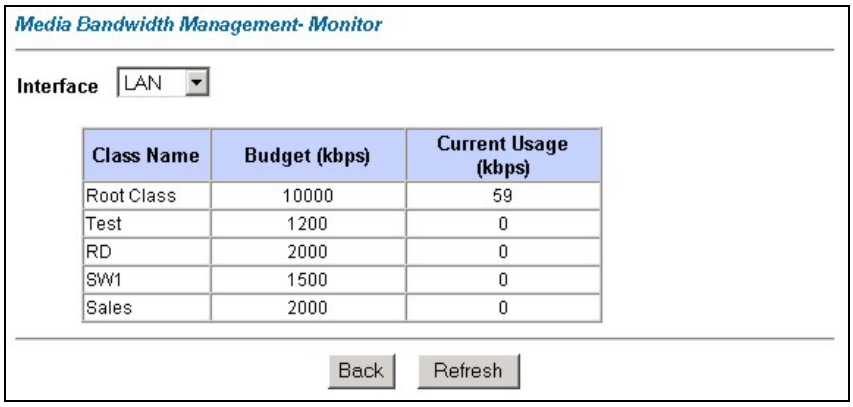


Рис. 19-11 Монитор управления пропускной способностью

В следующей таблице даны описания полей данного окна.

Таблица 19-7 Монитор управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Interface (Интерфейс)	Выберите интерфейс из раскрывающегося списка, чтобы просмотреть использование пропускной способности его классами.
Class Name (Имя класса)	В этом поле показано имя класса.
Budget (kbps) (Бюджет (Кбит/с))	В этом поле показана пропускная способность, выделенная данному классу.

Таблица 19-7 Монитор управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Current Usage (kbps) (Текущее использование (Кбит/с))	В этом поле показана пропускная способность, используемая каждым классом.
Back (Назад)	Щелкните на **Back,** чтобы перейти к основному окну **Media Bandwidth Management**.
Refresh (Обновить)	Щелкните на **Refresh**, чтобы обновить эту страницу.

Глава VII:

Обслуживание

В этой части описаны окна обслуживания.

Раздел 20
Обслуживание

ТВ этой главе содержится системная информация, в частности, о микропрограммном обеспечении ZyNOS, IP-адресах портов и статистике трафика портов.

20.1 Обзор обслуживания

Окна обслуживания помогут Вам получить информацию о системе, загрузить новое микропрограммное обеспечение, изменить конфигурацию и перезапустить Prestige.

20.2 Окно системного статуса

Щелкните на **System Status**, чтобы открыть следующее окно, используемое для мониторинга Prestige. Следует помнить, что следующие поля открываются ТОЛЬКО ДЛЯ ЧТЕНИЯ и используются только в целях диагностики.

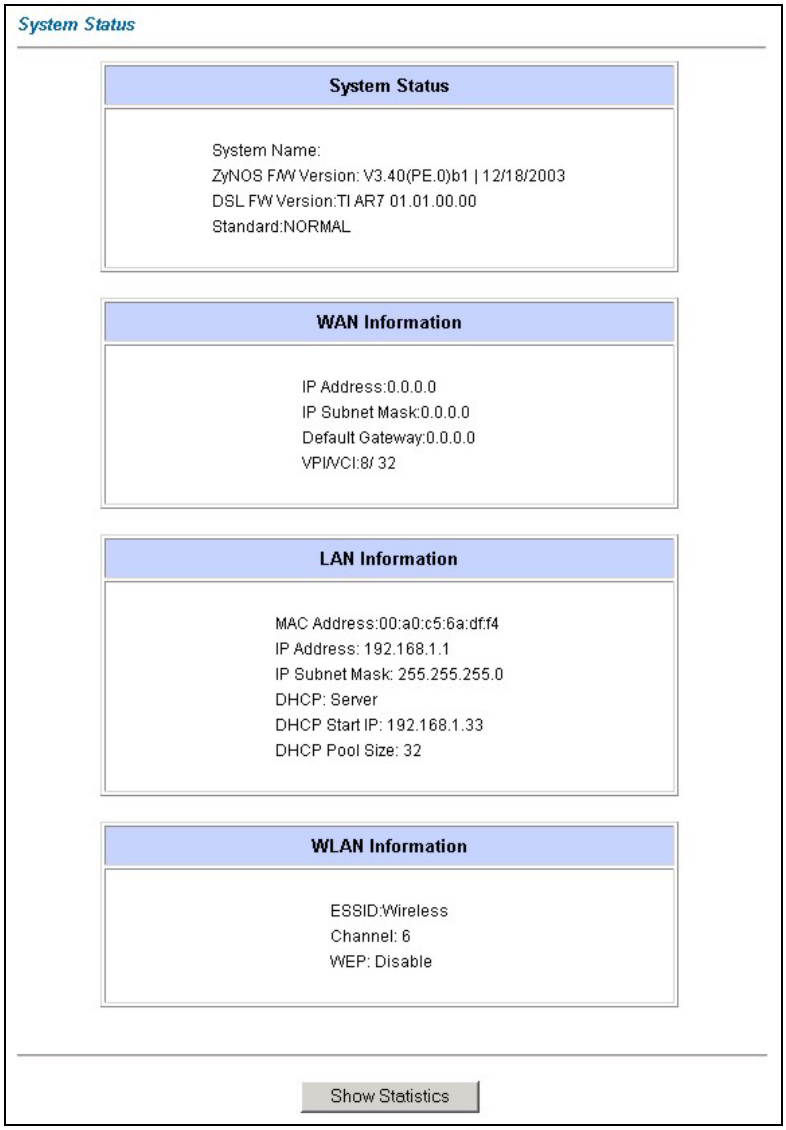


Рис. 20-1 Системный статус

В следующей таблице даны описания полей данного меню.

Таблица 20-1 Системный статус

ПОЛЕ	ОПИСАНИЕ
System Status (Системный статус)	
System Name (Системное имя)	Имя вашего Prestige. Эта информация нужна для его идентификации.
ZyNOS Firmware Version (Версия встроенного ПО ZyNOS)	Версия встроенного ПО ZyNOS и дата его создания. ZyNOS является разработанной корпорацией ZyXEL собственной сетевой операционной системой.
DSL FW Version (Версия встроенного ПО DSL)	Версия встроенного ПО DSL, используемого Prestige.
Standard (Стандарт)	Стандарт, используемый Prestige.
WAN Information (Информация о глобальной сети)	
IP Address (IP-адрес)	IP-адрес порта глобальной сети.
IP Subnet Mask (IP-маска подсети)	IP-маска подсети порта глобальной сети.
Default Gateway (Шлюз по умолчанию)	IP-адрес шлюза по умолчанию, если таковой имеется.
VPI/VCI	Идентификатор виртуального пути и идентификатор виртуального канала, определенный в первом окне мастер-программы.
LAN Information (Информация о локальной сети)	
MAC Address (MAC - адрес)	Адрес MAC (Media Access Control - Управление доступом к среде) или Ethernet, соответствующий Вашему Prestige.
IP Address (IP - адрес)	IP-адрес порта локальной сети.
IP Subnet Mask (IP-маска подсети)	IP-маска подсети порта локальной сети.
DHCP (Dynamic Host Configuration Protocol - Протокол динамического выбора конфигурации хост -машины)	DHCP-функция порта WAN - **Server**, **Relay** (не для всех моделей Prestige) или **None**.
DHCP Start IP (Начальный IP-адрес DHCP)	Первый адрес из пула непрерывных IP-адресов.
DHCP Pool Size (Размер пула DHCP)	Количество IP-адресов в пуле IP-адресов.
WLAN Information (Информация о беспроводной сети)	

Таблица 20-1 Системный статус

ПОЛЕ	ОПИСАНИЕ
ESSID (Extended Service Set Identifier- Идентификатор расширенного набора услуг)	Описательное имя, используемое для идентификации Prestige в беспроводной локальной сети.
Channel (Канал)	Текущий используемый Prestige номер канала.
WEP (Wired Equivalent Privacy- Конфиденциальность, эквивалентная проводной связи)	Отображает статус WEP шифрования данных.
Show Statistics (Показать статистику)	Щелкните на Show Statistics, чтобы просмотреть статистику работы маршрутизатора: например, количество отправленных пакетов и количество принятых пакетов для каждого порта.

20.2.1 Системная статистика

Щелкните на **Show Statistics** в окне **System Status**, чтобы открыть следующее окно. Информация, предназначенная только для чтения, включает статус портов и статистику, относящуюся к пакетам. Также приводятся "system up time" (время работы системы) и "poll interval(s)" (интервал(-ы) поллинга). Поле **Poll Interval(s)** может быть изменено.

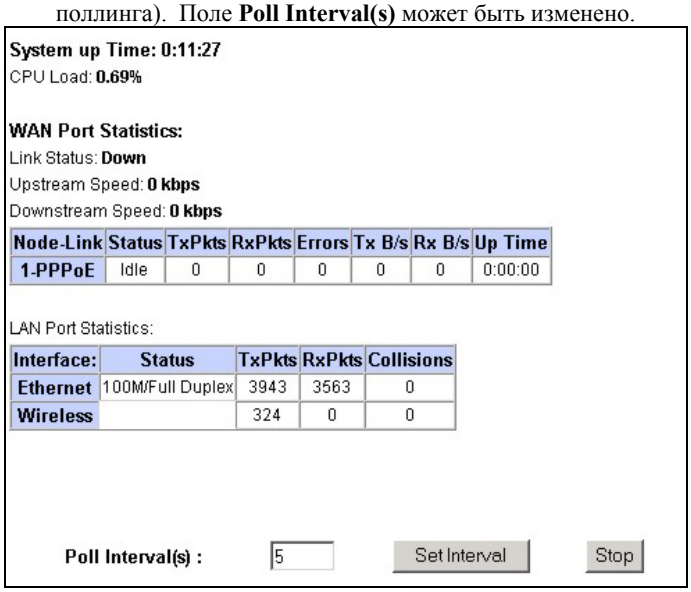


Рис. 20-2 Системный статус: Статистика

В следующей таблице даны описания полей данного меню.

Таблица 20-2 Системный статус: Статистика

ПОЛЕ	ОПИСАНИЕ
System up Time (Время работы системы)	Время, прошедшее с момента последнего включения системы.
CPU Load (Загрузка CPU)	Это поле определяет процент загрузки центрального процессора.
LAN or WAN Port Statistics (Статистика порта LAN или WAN)	Порт глобальной или локальной сети.
Link Status (Состояние канала связи)	Статус канала глобальной связи.
Transfer Rate (Скорость передачи данных)	Скорость передачи данных в Кбит/с.
Upstream Speed (Скорость исходящего потока)	Скорость исходящего потока Prestige.
Downstream Speed (Скорость входящего потока)	Скорость входящего потока Prestige.
Node-Link (Канал узла)	Индекс удаленного узла и тип связи. Возможные типы связи: PPPoA, ENET, RFC 1483 и PPPoE.
Interface (Интерфейс)	В этом поле указывается тип порта.
Status (Статус)	Для порта WAN указывается скорость порта и настройки дуплексного режима, если используется инкапсуляция Ethernet, или состояние **down** (соединение разорвано), **idle** (соединение (ppp) свободно), **dial** (начало инициации вызова) или **drop** (сброс вызова), если используется инкапсуляция PPPoE. Для порта LAN указывается скорость порта и настройки дуплексного режима.
TxPkts (Передано пакетов)	В этом поле показано количество переданных портом пакетов.
RxPkts (Принято пакетов)	В этом поле показано количество принятых портом пакетов.
Errors (Ошибки)	В этом поле показано количество пакетов с ошибками для данного порта.
Tx B/s (Скорость передачи)	В этом поле показано количество байтов, переданных за последнюю секунду.
Rx B/s (Скорость приема)	В этом поле показано количество байтов, принятых за последнюю секунду.
Up Time (Время соединения)	В этом поле показано время, прошедшее с момента последнего

Таблица 20-2 Системный статус: Статистика

ПОЛЕ	ОПИСАНИЕ
	включения порта.
Collisions (Конфликты)	Количество конфликтов при передаче через данный порт.
Poll Interval(s) (Интервал(-ы) поллинга)	Введите интервал обновления браузером системной статистики.
Set Interval (Установить интервал)	Щелкните на этой кнопке, чтобы применить новый интервал поллинга, введенный в расположенном выше поле **Poll Interval**.
Stop (Стоп)	Щелкните на этой кнопке, чтобы остановить обновление системной статистики.

20.3 Окно таблицы DHCP

DHCP (Dynamic Host Configuration Protocol, протокол динамического конфигурирования хост-машины, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получать при начальной загрузке конфигурацию TCP/IP с сервера. Prestige можно сконфигурировать как сервер DHCP или отключить его. При конфигурации в качестве сервера Prestige предоставляет клиентам конфигурацию TCP/IP. Установка **None** отключает данную функцию, и в этом случае необходимо иметь другой сервер DHCP в локальной сети, или конфигурировать компьютеры вручную.

Щелкните на **Maintenance**, затем на закладке **DHCP Table**. Эта предназначенная только для чтения информация соответствует Вашему статусу DHCP. Таблица DHCP отображает текущую информацию о клиентах DHCP (включая **IP Address**, **Host Name** и **MAC Address**) для всех сетевых клиентах, использующих сервер DHCP.

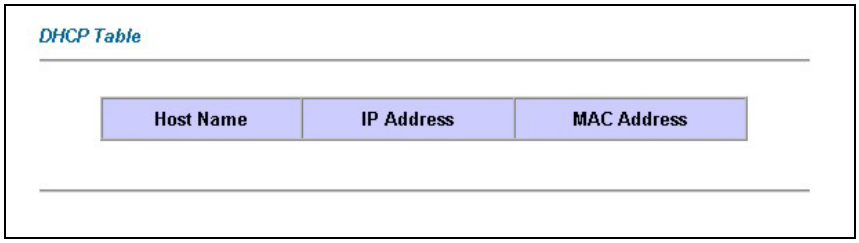


Рис. 20-3 Таблица DHCP

В следующей таблице даны описания полей данного меню.

Таблица 20-3 Таблица DHCP

ПОЛЕ	ОПИСАНИЕ
Host Name (Имя хоста)	Имя хоста.

Таблица 20-3 Таблица DHCP

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	В этом поле показан IP-адрес, относящийся к данному имени хоста.
MAC Address (MAC-адрес)	В этом поле показан адрес MAC (Media Access Control) компьютера, которому соответствует указанное имя хоста. Любое устройство Ethernet имеет уникальный MAC-адрес. MAC-адрес назначается изготовителем и состоит из шести пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02.

20.4 Окно таблицы Any IP

Щелкните на **Maintenance**, затем на закладке **Any IP**. Таблица Any IP отображает предназначенную только для чтения информация (включая IP и MAC адреса) обо всех сетевых устройств, которые используют функцию Any IP для взаимодействия с Prestige.

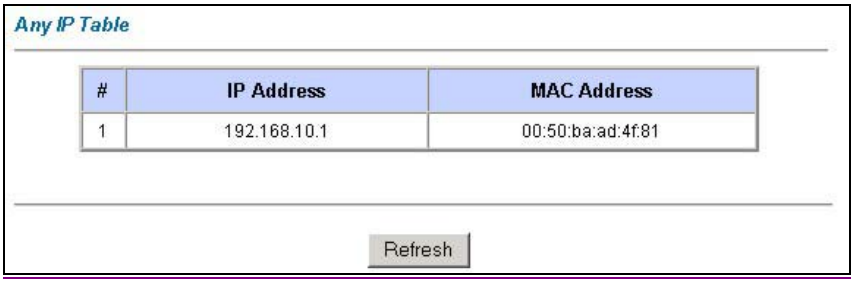


Рис. 20-4 Таблица Any IP

В следующей таблице даны описания полей данного меню.

Таблица 20-4 Таблица Any IP

ПОЛЕ	ОПИСАНИЕ
# (Номер)	Это поле отображает номер индекса.
IP Address (IP адрес)	Это поле отображает IP адрес сетевого устройства.
MAC Address (MAC-адрес)	В этом поле показан адрес MAC (Media Access Control) компьютера с указанным IP адресом.
Refresh (Обновить)	Щелкните на **Refresh**, чтобы обновить эту страницу.

20.5 Окна беспроводной сети

Эти открывающиеся только для чтения окна отображают информацию о беспроводной локальной сети Prestige.

20.5.1 Список соединений

В этом окне показаны MAC-адреса беспроводных станций, подключенных в данный момент к сети. Щелкните на **Wireless LAN**, а затем на **Association List**, чтобы открыть следующее окно.

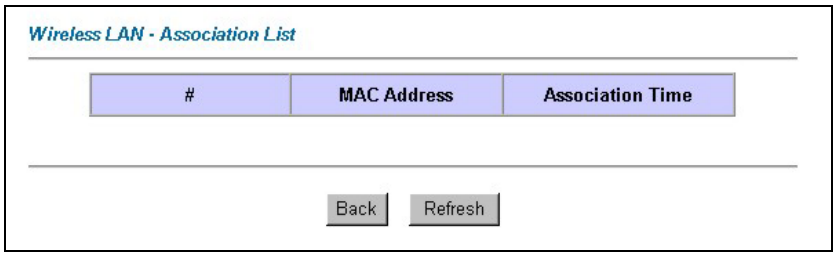


Рис. 20-5 Список соединений

В следующей таблице даны описания полей данного меню.

Таблица 20-5 Список соединений

ПОЛЕ	ОПИСАНИЕ
# (Номер)	Порядковый номер подключенного беспроводного клиента.
MAC Address (MAC-адрес)	MAC-адрес подключенного беспроводного клиента.
Association Time (Время соединения)	В этом поле показано, сколько времени длится соединение беспроводной станции и Prestige.
Back (Назад)	Щелкните на **Back**, чтобы перейти к предыдущему окну.
Refresh (Обновить)	Щелкните на **Refresh** , чтобы обновить информацию в таблице.

20.6 Окна диагностики

Эти открывающиеся только для чтения окна отображают информацию, помогающую распознать проблемы в работе Prestige.

20.6.1 Окно общей диагностики

Щелкните на **Diagnostic**, а затем на **General**, чтобы открыть следующее окно.

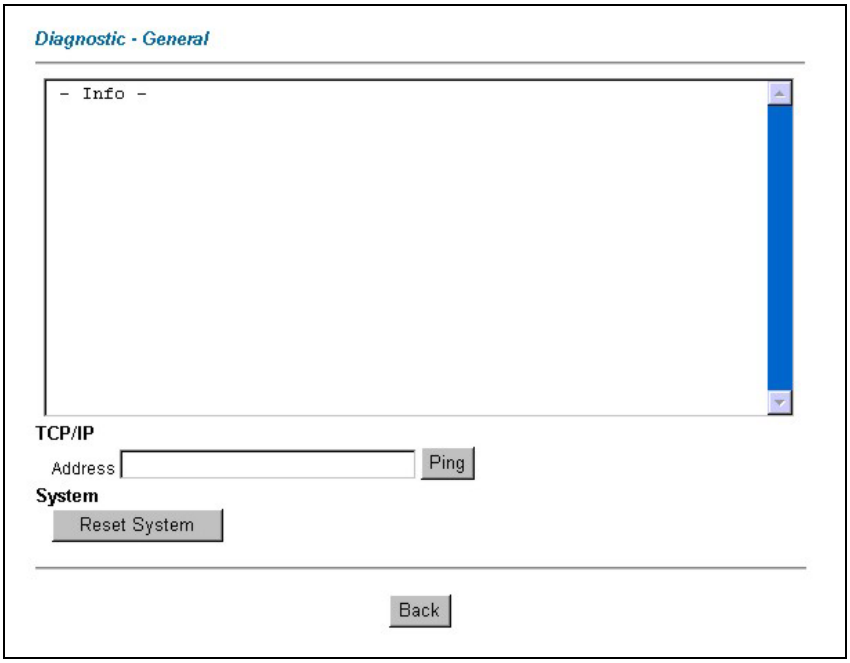


Рис. 20-6 Общая диагностика

В следующей таблице даны описания полей данного меню.

Таблица 20-6 Общая диагностика

ПОЛЕ	ОПИСАНИЕ
TCP/IP Address (Адрес TCP/IP)	Введите IP-адрес компьютера, который Вы хотите протестировать эхо-пакетами для проверки соединения.
Ping (Эхо-тестирование)	Щелкните на этой кнопке, чтобы протестировать введенный IP-адрес.
Reset System (Перезагрузить систему)	Щелкните на этой кнопке, чтобы перезагрузить Prestige. При этом появится предупреждающее диалоговое окно, запрашивающее подтверждения Вашей уверенности в желании перезагрузить систему. Для продолжения щелкните на **OK**.
Back (Назад)	Щелкните на этой кнопке, чтобы вернуться к главному окну **Diagnostic**.

20.6.2 Окно диагностики линии DSL

Щелкните на **Diagnostic**, а затем на **DSL Line**, чтобы открыть следующее окно.

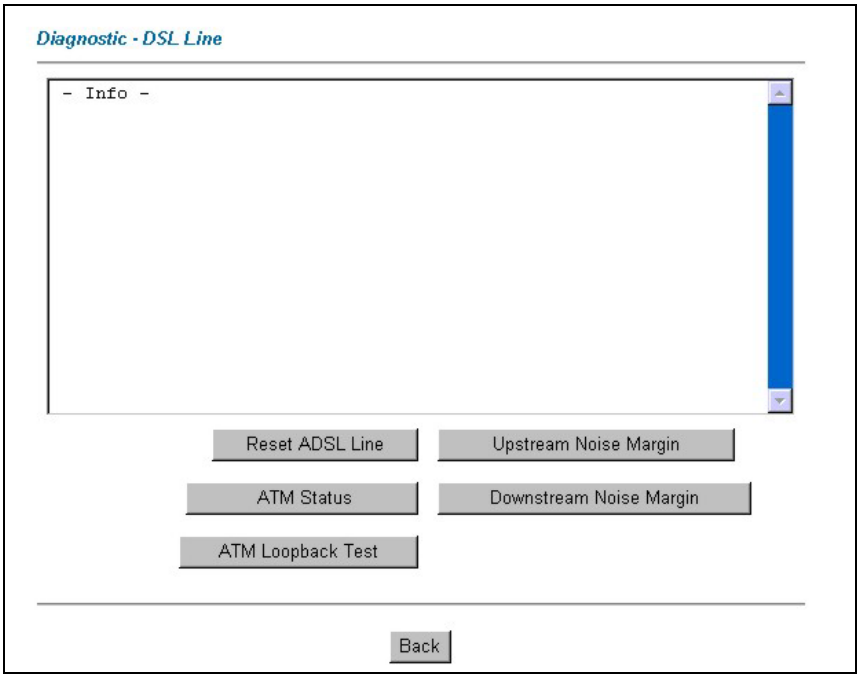


Рис. 20-7 Диагностика линии DSL

В следующей таблице даны описания полей данного меню.

Таблица 20-7 Диагностика линии DSL

ПОЛЕ	ОПИСАНИЕ
Reset ADSL Line (Перезагрузить линию ADSL)	Щелкните на этой кнопке для реинициализации линии ADSL. В большом текстовом окне, расположенном выше будут затем отображаться течение и результаты этой операции, например: "Start to reset ADSL (Начало перезагрузки ADSL) Loading ADSL modem F/W... (Загрузка встроенного ПО модема ADSL) Reset ADSL Line Successfully! (Линия ADSL успешно перезагружена!)"
ATM Status (Статус ATM)	Щелкните на этой кнопке для получения информации о статусе ATM.
ATM Loopback Test (Проверка ATM по тесту "петля")	Щелкните на этой кнопке, чтобы начать проверку ATM по тесту "петля". Перед началом теста убедитесь, что по меньшей мере один

Таблица 20-7 Диагностика линии DSL

ПОЛЕ	ОПИСАНИЕ
	PVC сконфигурирован с соответствующими VPI/VCI. Prestige посылает пакет OAM F5 на переключатель DSLAM/ATM, откуда он возвращается (по петле) на Prestige. Тест "петля" для ATM бывает полезен при поиске и устранении неисправностей, связанных с концентраторами DSLAM и сетью ATM.
Upstream Noise Margin (Предел помехоустойчивости при передаче данных)	Щелкните на этой кнопке для отображения предела помехоустойчивости при передаче данных.
Downstream Noise Margin (Предел помехоустойчивости при приеме данных)	Щелкните на этой кнопке для отображения предела помехоустойчивости при приеме данных.
Back (Назад)	Щелкните на этой кнопке, чтобы вернуться к главному окну **Diagnostic**.

20.7 Окно микропрограммного обеспечения

Микропрограммное обеспечение можно найти на сайте www.zyxel.com в файле, названном (как правило) по наименованию модели с расширением "*.bin" - например, "Prestige.bin". Загрузка производится при помощи протокола HTTP (Hypertext Transfer Protocol) и может занимать до двух минут. После успешной загрузки система перезагружается. См. информацию об обновлении микропрограммного обеспечения при помощи команд FTP/TFTP в главе *Микропрограммное обеспечение и обслуживание файлов конфигурации* в частях, описывающих системную консоль.

Следует использовать только микропрограммное обеспечение, точно предназначенное для Вашей модели устройства. См. этикетку на нижней стороне устройства.

Для перехода к следующему окну щелкните на **Firmware**. При загрузке микропрограммного обеспечения для Вашего Prestige выполняйте указания, появляющиеся в этом окне.

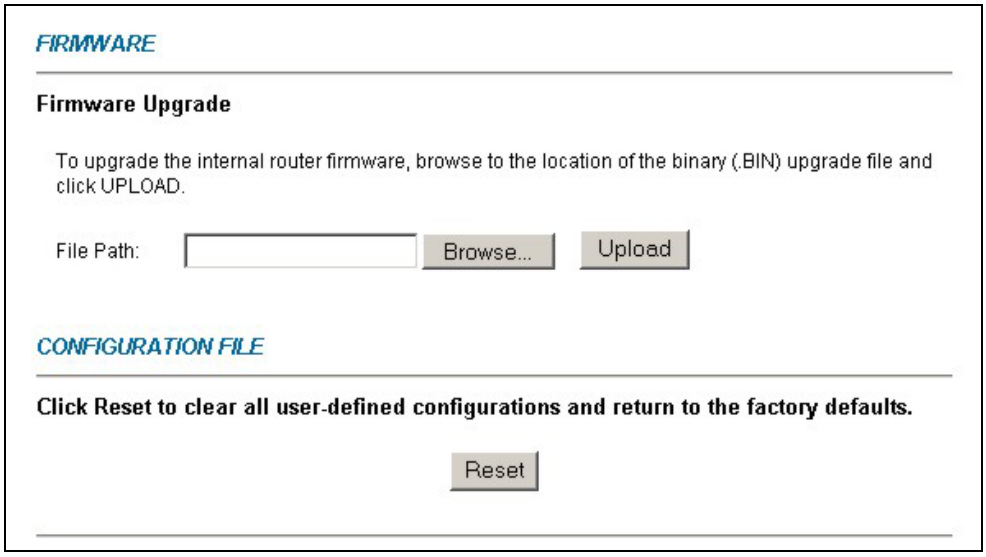


Рис. 20-8 Обновление микропрограммного обеспечения

В следующей таблице даны описания полей данного меню.

Таблица 20-8 Обновление микропрограммного обеспечения

ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите в этом поле местонахождение файла, который Вы хотите загрузить, или щелкните на **Browse...**, чтобы найти его.
Browse... (Просмотр...)	Щелкните на **Browse...**, чтобы найти файл .bin, который Вы хотите загрузить. Помните, что перед загрузкой Вы должны распаковать упакованные файлы (.zip).
Upload (Загрузить)	Щелкните на **Upload**, чтобы начать процесс загрузки. Этот процесс может занимать до двух минут.
Reset (Сброс)	Щелкните на этой кнопке, чтобы удалить все пользовательские установки и снова установить на Prestige заводские настройки по умолчанию.

Не выключайте Prestige в процессе загрузки микропрограммного обеспечения!

После появления окна **Firmware Upload in Process** (Идет загрузка микропрограммного обеспечения) подождите две минуты, прежде чем снова входить в Prestige.

В это время Prestige автоматически перезапустится, что вызовет кратковременное отсоединение сети. В некоторых операционных системах, на Рабочем Столе может появиться следующая иконка.

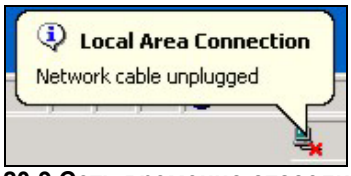


Рис. 20-9 Сеть временно отсоединена

Через две минуты снова войдите в систему и убедитесь в обновлении версии микропрограммного обеспечения при помощи окна **System Status**.

Если загрузка не была успешной, на экране появится следующее окно. Щелкните на кнопке **Back**, чтобы вернуться к предыдущему окну **Firmware**.

Рис. 20-10 Сообщение об ошибке

Глава VIII:

Основное конфигурирование SMT

В этой части дается обзор конфигурирования системной консоли для настройки общих параметров, резервного доступа к WAN, настройки LAN, настройки беспроводной LAN, доступа в Интернет, настройки удаленного узла, статического маршрута, NAT и включения межсетевого экрана.

Для получения вводной информации о характеристиках, конфигурируемых с помощью Web-конфигуратора и SMT, см. разделы по Web-конфигуратору данного руководства.

Раздел 21
Ознакомление с SMT

В этой главе описывается как получить доступ и управлять системной консолью и представлен обзор меню SMT.

21.1 Введение в SMT

SMT (System Management Terminal/Системная консоль) Prestige представляет собой управляемый интерфейс, к которому можно получить доступ из терминального эмулятора при подключении через Telnet. В этой главе описывается как получить доступ к меню SMT через Telnet, как управлять SMT и как сконфигурировать меню SMT.

21.1.1 Алгоритм конфигурирования SMT через Telnet

Следующая процедура подробно описывает как установить связь с Prestige путем сетевого теледоступа.

Step 1. В Windows щелкните **Start (Пуск)** (обычно в левом нижнем углу), **Run (Выполнить)**, а затем ведите “telnet 192.168.1.1” (IP-адрес по умолчанию) и щелкните по **OK**.

Step 2. Введите “1234” в поле **Password (Пароль)**.

Step 3. После ввода пароля отобразится Главное меню.

Следует отметить, что если после регистрации в течение пяти минут (время простоя по умолчанию) ничего не будет введено, Prestige автоматически выведет Вас из системы. В этом случае Вам придется снова подключиться к Prestige.

21.1.2 Ввод пароля

При нажатии клавиши [ENTER] появляется экран регистрации и предлагает ввести пароль, как показано ниже.

Для первой регистрации ввести пароль по умолчанию “1234”. При вводе пароля символы ввода заменяются на экране на символ звездочка “*”.

Следует отметить, что если после регистрации в течение 5 минут ничего не будет введено, Prestige автоматически выведет Вас из системы.

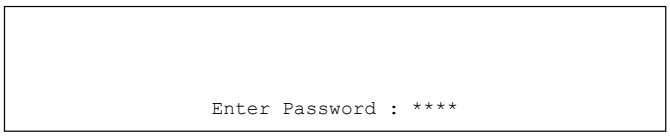


Рис. 21-1 Экран регистрации

21.1.3 Обзор меню SMT Prestige

В качестве примера в этом руководстве используются меню SMT Prestige 660HW-61. В разных моделях Prestige меню SMT немного различаются.

На следующем рисунке дан обзор экранных форм меню SMT Prestige.

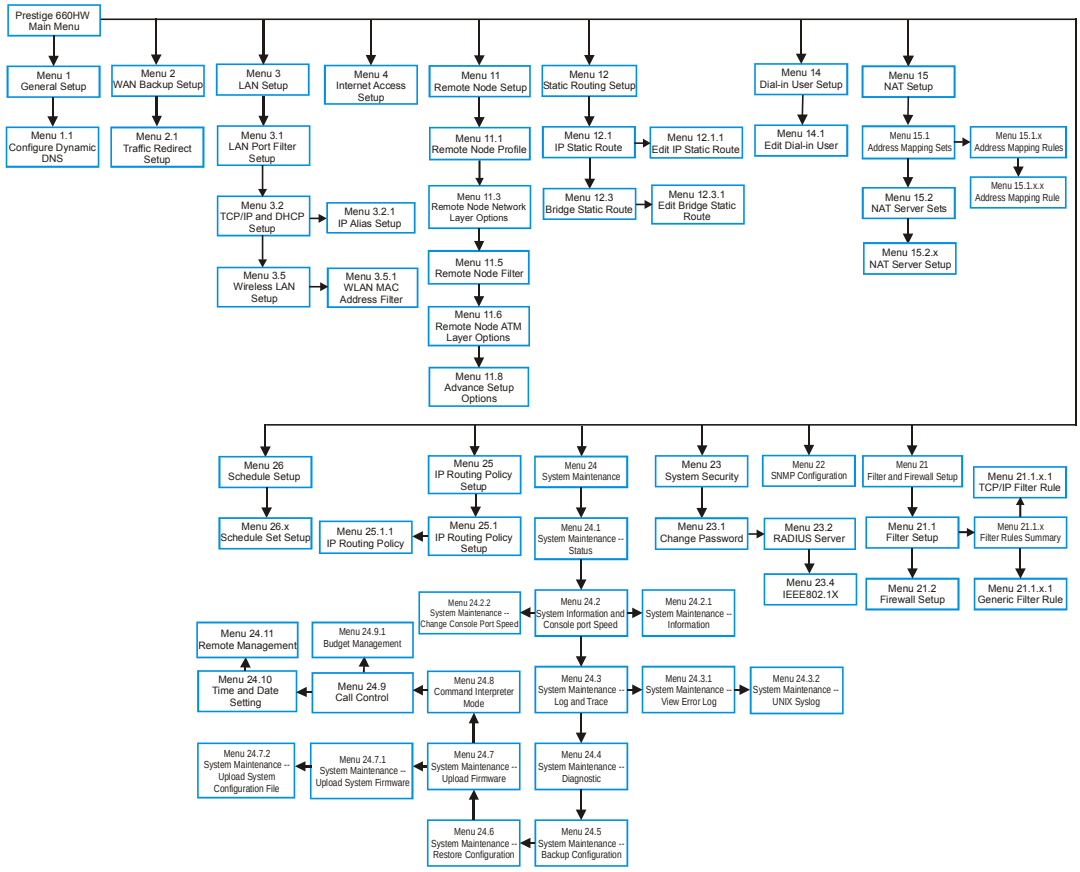


Рис. 21-2 Обзор меню SMT Prestige 660HW-61

21.2 Работа с интерфейсом SMT

SMT (System Management Terminal/Системная консоль) представляет собой интерфейс, предназначенный для конфигурирования Prestige.

Прежде чем приступать к конфигурированию, следует ознакомиться с базовыми операциями, приведенными в следующей таблице.

Табл. 21-1 Команды Главного меню

ОПЕРАЦИЯ	НАЖАТЬ/<ЧИТАТЬ>	ОПИСАНИЕ
Переход к другому меню	[ENTER]	Для перехода к подменю ввести его номер и нажать клавишу [ENTER].
Возврат к предыдущему меню	[ESC]	Для возврата к предыдущему меню нажать клавишу [ESC].
Переход к “скрытому” меню	Нажать клавишу пробела [SPACE BAR] для изменения **No** на **Yes**, а затем нажать клавишу [ENTER].	Поля начинающиеся с “Edit”, ведут к скрытым меню и по умолчанию имеют значение **No**. Нажать клавишу пробела [SPACE BAR] для изменения **No** на **Yes**, а затем нажать клавишу [ENTER] для перехода к “скрытому“ меню.
Перемещение курсора	Клавиша [ENTER] или клавиши со стрелками “вверх/вниз“ [UP]/[DOWN].	Находясь в меню, для перехода к следующему полю нажать клавишу [ENTER]. Для перемещения по полям можно использовать клавиши со стрелками “вверх/вниз“ [UP]/[DOWN].
Ввод данных	Заполнить поле или нажать клавишу пробела для выбора, а затем нажать [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 для сохранения новой конфигурации. Все поля с **ChangeMe** не следует оставлять пустыми для сохранения новой конфигурации.
Поля N/A	<N/A>	Некоторые поля SMT содержат символ <N/A>. Этот символ означает, что данная функция не доступна (Not Applicable).
Сохранение конфигурации	[ENTER]	При появлении сообщения “Press ENTER to confirm or ESC to cancel” нажать клавишу [ENTER] для сохранения конфигурации. После сохранения данных, как правило, происходит возврат к предыдущему меню.

Табл. 21-1 Команды Главного меню

Выход из SMT	Ввести 99, а затем нажать клавишу [ENTER].	Для завершения работы с SMT при появлении сообщения Главного меню ввести 99 и нажать клавишу [ENTER].

После ввода пароля SMT выводит на экран Главное меню, показанное ниже.

```
                Copyright (c) 1994 - 2003 ZyXEL Communications
Corp.

                            Prestige 660HW-61 Main Menu


     Getting Started                      Advanced Management
       1. General Setup                     21. Filter and
Firewall Setup
       2. WAN Backup Setup                  22. SNMP Configuration
       3. LAN Setup                         23. System Security
```

Рис. 21-3 Главное меню SMT

21.2.1 Сводка функций интерфейса SMT

Табл. 21-2 Сводка по Главному меню

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
1	General Setup (Настройка общих параметров)	Данное меню используется для настройки общих параметров.

Табл. 21-2 Сводка по Главному меню

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
2	WAN Backup Setup (Настройка резервного доступа к WAN)	Данное меню используется для настройки переадресации трафика и резервного удаленного доступа.
3	LAN Setup (Настройка LAN)	Данное меню используется для настройки беспроводной LAN и подключения к LAN.
4	Internet Access Setup (Настройка доступа в Интернет)	Простая и быстрая настройка подключения к Интернету.
11	Remote Node Setup (Настройка удаленного узла)	Используйте данное меню для настройки 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)	Данное меню используется для настройки учетных записей локального пользователя в Prestige.
15	NAT Setup (Настройка NAT)	Данное меню используется для установления внутренних серверов при включенном NAT.
21	Filter and Firewall Setup (Настройка фильтра и межсетевого экрана)	Данное меню используется для конфигурирования фильтров, включения/отключения межсетевого экрана и обзора журнальной регистрации межсетевого экрана.
22	SNMP Configuration (Конфигурирование SNMP)	Данное меню используется для настройки параметров, относящихся к SNMP.
23	System Security (Защитные функции системы)	Данное меню используется для настройки защиты беспроводных соединений и для изменения пароля.
24	System Maintenance (Сопровождение системы)	Системный статус, диагностика, загрузка программного обеспечения и т.д.
25	IP Routing Policy Setup (Настройка стратегии маршрутизации IP)	Данное меню используется для конфигурирования стратегий маршрутизации IP.
26	Schedule Setup (Составление расписания)	Данное меню используется для планирования исходящих вызовов.

Табл. 21-2 Сводка по Главному меню

#	НАЗВАНИЕ МЕНЮ	ОПИСАНИЕ
99	Exit (Выход)	Выход из SMT и возврат к чистому экрану.

21.3 Изменение системного пароля

Для изменения пароля Prestige, заданного по умолчанию, следует выполнить описанные ниже действия.

Step 1. Ввести 23 в Главном меню для перехода в **Меню 23 - System Security (Защитные функции системы)**.

Step 2. Ввести 1 для перехода в **Меню 23.1 - System Security (Защитные функции системы) - Change Password (Изменение пароля),** как показано ниже.

Step 3. Ввести существующий системный пароль в поле **Old Password**, напр., “1234” и нажать клавишу [ENTER].

```
                Menu 23.1 - System Security - Change
Password


                  Old Password= ?
```

Рис. 21-4 Меню 23.1 - Изменение пароля

Step 4. Ввести новый системный пароль в поле **New Password** (до 30 символов) и нажать клавишу [ENTER].

Step 5. Подтвердить ввод нового системного пароля, для чего повторно ввести его в поле **Retype to confirm** и нажать клавишу [ENTER].

Следует отметить, что при вводе пароля вводимые символы заменяются на экране на звездочку “*”.

Раздел 22
Меню 1 Настройка общих параметров

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

22.1 Настройка общих параметров

Меню 1 — General Setup (**Настройка общих параметров)** содержит административную и общесистемную информацию (представленную далее). Поле **System Name (Системное имя)** используется только в целях идентификации. Однако, ввиду того, что некоторые Интернет-провайдеры проверяют это имя, необходимо ввести "Имя компьютера" машины.

- В Windows 95/98 щелкните **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)**, **Network (Сеть)**. Щелкните по закладке **Identification (Идентификация)**, отметьте запись для поля **Computer name (Имя компьютера)** и введите ее как **System Name (Системное имя)** Prestige.
- В Windows 2000 щелкните **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)** и дважды щелкните на **System (Система)**. Щелкните по закладке **Network Identification (Идентификация сети),** а затем щелкните по кнопке **Properties (Свойства)**. Отметьте запись для поля **Computer name (Имя компьютера)** и введите ее как **System Name (Системное имя)** Prestige.
- В Windows XP щелкните **Start**, **My Computer**, **View system information (Обзор системной информации)**, а затем щелкните по закладке **Computer Name (Имя компьютера)**. Отметьте запись в поле **Full computer name (Полное имя компьютера)** и введите ее как **System Name (Системное имя)** Prestige.

Запись **Domain Name (Имя домена)** распространяется на клиентов DHCP в LAN. Если оставляете это поле не заполненным, используется имя домена, полученное DHCP от Интернет-провайдера. Хотя необходимо ввести имя хоста (System Name) для каждого индивидуального компьютера, имя домена может быть назначено Prestige при помощи DHCP.

22.2 Алгоритм конфигурирования Меню 1

Step 1. Ввести 1 в Главном меню для перехода в **Меню 1 — General Setup** (**Настройка общих параметров)** (как показано ниже).

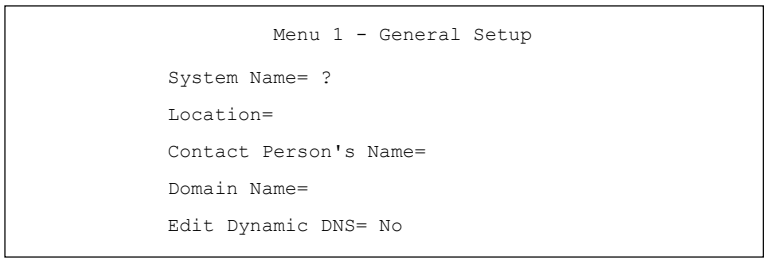


Рис. 22-1 Меню 1 - Настройка общих параметров

Step 2. Заполните обязательные поля. Для дополнительной информации об этих полях см. таблицу, представленную ниже.

Табл. 22-1 Меню 1 - Настройка общих параметров

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
System Name (Системное имя)	Выберите идентифицирующее имя в целях идентификации. Имя может включать до 30 алфавитно-цифровых символов. Пробелы внутри имени не допускаются, но допускаются тире “-” и знак подчеркивания "_" .	
Location (optional) (Местонахождение) (не обязательно)	Введите географическое местонахождение Prestige (до 31символа).	MyHouse
Contact Person's Name (optional) (Имя ответственного лица) (не обязательно)	Введите имя лица, ответственного за Prestige (до 30 символов).	JohnDoe
Domain Name (Служба имен доменов)	Введите имя домена (если оно известно). Если это поле остается не заполненным, Интернет-провайдер может назначить имя домена через DHCP. Перейдите в Меню 24.8 и введите "sys domainname" для отображения текущего имени домена, используемого шлюзом. Если необходимо очистить данное поле, просто нажмите клавишу пробела [SPACE BAR]. Введенное имя домена представляет приоритет перед именем домена, назначенным Интернет-провайдером.	zyxel.com.tw

Табл. 22-1 Меню 1 - Настройка общих параметров

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Edit Dynamic DNS (Редактирование динамического DNS)	Нажмите клавишу пробела [SPACE BAR] для переключения между **Yes** и **No** (по умолчанию). Выберите **Yes** для конфигурирования **Меню 1.1 — Configure Dynamic DNS (Конфигурирование динамического DNS)** (рассматривается ниже).	**No**
Route IP (Маршрут IP)	Установите в данном поле **Yes**, чтобы включить маршрутизацию IP или **No**, чтобы ее отключить. Для доступа в Интернет необходимо включить маршрутизацию IP.	**Yes**
Bridge (Мост)	Включить/выключить продвижение данных по мосту для неподдерживаемых протоколов (напр., SNA) или для тех, которые не включены в предыдущем поле **Route IP**. Выберите **Yes** для включения межсетевого моста; выберите **No** для отключения межсетевого моста.	**No**

22.2.1 Алгоритм конфигурирования динамического DNS

Если имеется частный IP-адрес WAN, тогда Вы не можете использовать динамический DNS.

Step 1. Для конфигурирования динамического DNS перейдите в **Меню 1 — General Setup (Настройка общих параметров**) и выберите **Yes** в поле **Edit Dynamic DNS (Редактирование динамического DNS)**. Нажмите клавишу [ENTER] для отображения **Меню 1.1— Configure Dynamic DNS (Конфигурирование динамического DNS)**, как показано ниже.

```
                    Menu 1.1 - Configure Dynamic DNS

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

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

Рис. 22-2 Меню 1.1 - Конфигурирование динамического DNS

Следуйте указаниям по конфигурированию параметров динамического DNS в приведенной ниже таблице.

Табл. 22-2 Меню 1.1 - Конфигурирование динамического DNS

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Service Provider (Провайдер услуг)	В этом поле отображается имя провайдера услуг динамического DNS.	WWW.DynDNS.ORG (default)
Active (Активно)	Нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите [ENTER] для активации динамического DNS.	**Yes**
Host (Хост)	Введите имя домена, назначенное для Prestige провайдером динамического DNS.	me.dyndns.org
EMAIL	Введите адрес e-mail.	mail@mailserver
USER (ПОЛЬЗОВАТЕЛЬ)	Введите имя пользователя.	
Password (Пароль)	Введите назначенный пароль.	
Enable Wildcard (Включение группового символа)	Prestige поддерживает групповой символ DYNDNS. Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для переключения между **Yes** и **No** Данное поле не доступно, если в качестве провайдера услуг выбран клиент DDNS.	**No**
При 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.		

Раздел 23
Меню 2 Настройка резервного доступа к WAN

В этой главе описывается конфигурирование переадресации трафика и резервного удаленного доступа при помощи Меню 2 и 2.1.

23.1 Введение в настройку резервного доступа к WAN

В этой главе описывается конфигурирование Prestige для переадресации трафика и резервного удаленного доступа к сети.

23.2 Конфигурирование резервного удаленного доступа в Меню 2

В Главном меню ввести 2 для вызова Меню 2.

```
                    Menu 2 - Wan Backup Setup


          Check Mechanism = DSL Link
          Check WAN IP Address1 = 0.0.0.0
          Check WAN IP Address2 = 0.0.0.0
          Check WAN IP Address3 = 0.0.0.0
            KeepAlive Fail Tolerance = 0
```

Рис. 23-1 Меню 2 - Настройка резервного доступа к WAN

В следующей таблице представлено описание полей данного меню.

Табл. 23-1 Меню 2 - Настройка резервного доступа к WAN

ПОЛЕ	ОПИСАНИЕ

Табл. 23-1 Меню 2 - Настройка резервного доступа к WAN

ПОЛЕ	ОПИСАНИЕ
Check Mechanism (Механизм проверки)	Нажмите клавишу пробела [SPACE BAR], а затем нажмите [ENTER] для выбора метода, с помощью которого Prestige проверяет соединение DSL. Выберите **DSL Link** для проверки Prestige физического уровня соединения DSL. Выберите **ICMP** для того, чтобы Prestige периодически посылал эхо-пакеты на IP-адреса, заданные в полях **Check WAN IP Address**.
Check WAN IP Address1-3 (Проверка IP-адресов 1-3 WAN)	Заполните это поле для проверки доступности WAN для Prestige. Введите IP-адрес надежного соседнего компьютера (напр., адрес сервера DNS Интернет-провайдера). При использовании дублирующего соединения WAN, Prestige периодически посылает эхо-пакеты на заданные здесь адреса и использует другое дублирующее соединение WAN (если сконфигурировано), если не получает ответа.
KeepAlive Fail Tolerance	Введите время в секундах (рекомендуется 2), в течение которого Prestige может посылать эхо-пакеты на IP-адреса, заданные в полях **Check WAN IP Address,** без получения ответа до коммутации на дублирующее соединение WAN (или другое дублирующее соединение WAN).
Recovery Interval(sec) (Интервал восстановления) (с)	Если Prestige использует соединение с более низким приоритетом (обычно дублирующее соединение WAN), он периодически проверяет может ли он использовать соединение с более высоким приоритетом. Введите время в секундах (рекомендуется 30), когда Prestige может прибывать в ожидании между проверками. Допускается более длительный промежуток времени, если IP-адрес назначения справляется с обширным трафиком.
ICMP Timeout (Время простоя ICMP)	Введите время в секундах, необходимое для ожидания сеансом связи ICMP ответа ICMP.
Traffic Redirect (Переадресация трафика)	Нажмите клавишу пробела [SPACE BAR] для переключения между **Yes** и **No**. Для конфигурирования **Меню 2.1 Traffic Redirect Setup (Настройка переадресации трафика)** выберите **Yes** и нажмите клавишу [ENTER]. Если нет необходимости в конфигурировании этой функции выберите **No** (по умолчанию).
При 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.	

23.2.1 Настройка переадресации трафика

Сконфигурируйте параметры, определяющие, когда Prestige будет пересылать трафик WAN на резервный шлюз при помощи **Меню 2.1 — Traffic Redirect Setup (Настройка переадресации трафика)**.

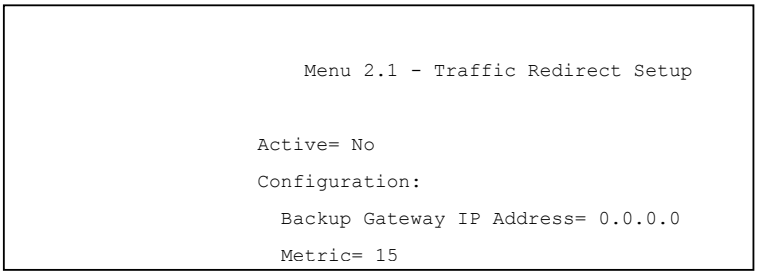


Рис. 23-2 Меню 2.1 - Настройка переадресации трафика

В следующей таблице представлено описание полей данного меню.

Табл. 23-2 Меню 2.1 - Настройка переадресации трафика

ПОЛЕ	ОПИСАНИЕ
Active (Активно)	Нажмите клавишу пробела [SPACE BAR] и выберите **Yes** (включить) или **No** (отключить) настройку переадресации трафика. По умолчанию - **No**.
Configuration: (Конфигурация:)	
Backup Gateway IP Address (IP-адрес резервного шлюза)	Введите IP-адрес резервного шлюза в десятичном виде с разделительными точками. Prestige автоматически пересылает трафик на данный IP-адрес, если соединение Prestige с Интернетом прерывается.

Табл. 23-2 Меню 2.1 - Настройка переадресации трафика

ПОЛЕ	ОПИСАНИЕ
Metric (Метрика)	В этом поле устанавливается приоритет маршрута среди маршрутов, используемых Prestige. Метрика определяет "стоимость передачи". Маршрутизатор определяет лучший маршрут для передачи, выбирая траекторию с наименьшей "стоимостью". Маршрутизация RIP использует счетчик переходов по сети в качестве своего рода единицы стоимости, с минимальным значением равным "1" для прямого соединения. Число должно находиться в диапазоне от "1" до "15"; номер больше, чем "15" означает, что связь отсутствует. Чем меньше номер, тем меньше "стоимость".
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.	

Раздел 24
Меню 3 Настройка LAN

В этой главе рассматривается конфигурирование настроек беспроводной локальной вычислительной сети (LAN).

24.1 Настройка LAN

В этом разделе описывается конфигурирование Ethernet с помощью **Меню 3 — LAN Setup (Настройка LAN)**. Ввести 3 в Главном меню для перехода в Меню 3.

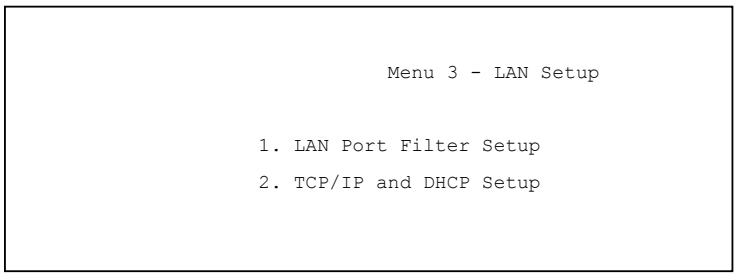


Рис. 24-1 Меню 3 - Настройка LAN

24.1.1 Общая настройка Ethernet

Данное меню используется для задания набора 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=
```

Рис. 24-2 Меню 3.1 - Настройка фильтра для порта LAN

Если нужно определить фильтры, сначала следует ознакомится с главой *Конфигурирование набора фильтров,* а затем вернуться в данное 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 Ethernet TCP/IP см. главу *Организация доступа в Интернет*.
- Для настройки Ethernet для межсетевого моста см. главу *Настройка межсетевого моста*.

24.3 Настройка TCP/IP и DHCP для Ethernet

С помощью Меню 3.2 сконфигурируйте Prestige под TCP/IP.

Чтобы отредактировать Меню 3.2, следует ввести 3 в Главном меню для перехода в **Меню 3 — LAN Setup** (**Настройка LAN)**. В Меню 3 выбрать 2 и нажать клавишу [ENTER] для отображения **Меню 3.2 — TCP/IP and DHCP Ethernet Setup** (**Настройка TCP/IP и DHCP для Ethernet)**, как показано ниже:

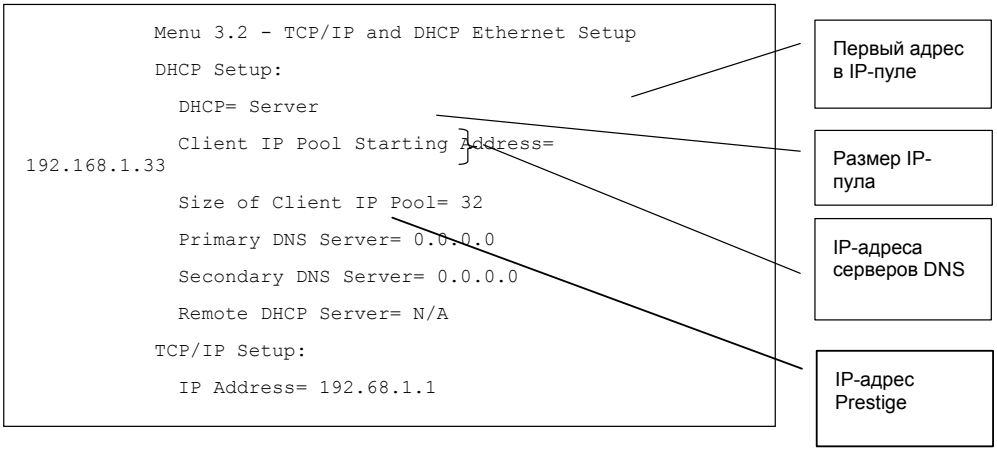


Рис. 24-3 Меню 3.2 - Настройка TCP/IP и DHCP для Ethernet

Следуйте указаниям по конфигурированию DHCP в приведенной ниже таблице.

Табл. 24-1 Настройка DHCP для Ethernet

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
DHCP Setup (Настройка DHCP)		
DHCP (Dynamic Host Configuration Protocol/Протокол динамического выбора конфигурации хост-машины)	Если в поле установлено **Server**, Prestige может назначать IP-адреса, шлюз IP по умолчанию и серверы DNS для Windows 95, Windows NT и других систем, поддерживающих клиента DHCP. Если установлено **None**, функция сервера DHCP отключена. Если установлено **Relay**, то Prestige выступает в качестве фиктивного сервера DHCP и передает запросы и ответы DHCP между удаленным сервером и клиентами. В данном случае следует ввести IP-адрес фактического удаленного сервера DHCP в поле Remote DHCP Server. Если используется DHCP, необходимо задать следующие параметры:	**Server** (по умолчанию)

Табл. 24-1 Настройка DHCP для Ethernet

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
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 число непрерывных IP-адресов пула.	32
Primary DNS Server (Основной сервер DNS) Secondary DNS Server (Дополнительный сервер DNS)	Введите IP-адреса серверов DNS. Серверы DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.	
Remote DHCP Server (Удаленный сервер DHCP)	Если в указанном поле **DHCP** выбрано **Relay**, следует ввести IP-адрес фактического удаленного сервера DHCP.	

При конфигурировании параметров TCP/IP для порта Ethernet следуйте указаниям в приведенной ниже таблице.

Табл. 24-2 Настройка TCP/IP для Ethernet

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
TCP/IP Setup (Настройка TCP/IP)		
IP Address (IP-адрес)	Введите IP-адрес (LAN) Prestige в десятичном виде с разделительными точками	192.168.1.1
IP Subnet Mask (Маска подсети IP)	Prestige вычисляет маску подсети автоматически на основе назначенного IP-адреса. Пока не реализована организация подсетей, следует использовать маску подсети, вычисленную Prestige.	255.255.255.0
RIP Direction (Направление RIP)	Нажмите клавишу пробела [SPACE BAR] для выбора направления RIP. Опциями являются: **Both**, **In Only**, **Out Only** или **None**.	**Both** (по умолчанию)

Табл. 24-2 Настройка TCP/IP для Ethernet

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Version (Версия)	Нажмите клавишу пробела [SPACE BAR] для выбора формата RIP. Опциями являются: **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. Prestige поддерживает как версию 1 (**IGMP-v1**), так и версию 2 (**IGMP-v2**). Нажмите клавишу пробела [SPACE BAR] для включения многоадресной рассылки по IP или выберите **None** для ее отключения.	**None** (по умолчанию)
IP Policies (Стратегии IP)	Создайте стратегии с помощью Меню 25 SMT (см. главу *Маршрутизация на базе стратегии IP*) и примените их к интерфейсу LAN Prestige. Можно применять до четырех наборов стратегий IP (из двенадцати), введя их номера через запятую.	2,4,7,9
Edit IP Alias (Редактирование псевдонима IP)	Prestige поддерживает три логических интерфейса LAN через один физический интерфейс Ethernet, при этом сам Prestige выступает в качестве шлюза для каждой сети LAN. Нажмите клавишу пробела [SPACE BAR] для изменения **No** на **Yes**, а затем нажмите клавишу [ENTER] для вывода на экран Меню 3.2.1.	**No** (по умолчанию)

Раздел 25
Настройка беспроводной LAN

В этой главе описывается конфигурирование настроек беспроводной LAN в Меню 3.5. SMT

25.1 Описание беспроводной LAN

Для вводной информации о беспроводной LAN обратитесь к главе *Экранные меню LAN*.

25.2 Настройка беспроводной LAN

Для настройки Prestige в качестве беспроводной точки доступа используйте Меню 3.5. Чтобы отредактировать Меню 3.5, следует ввести 3 в Главном меню для перехода в **Меню 3 – LAN Setup (Настройка LAN)**. В Меню 3 выбрать 5 и нажать клавишу [ENTER] для перехода в **Меню 3.5 – Wireless LAN Setup (Настройка беспроводной LAN)**, как показано ниже.

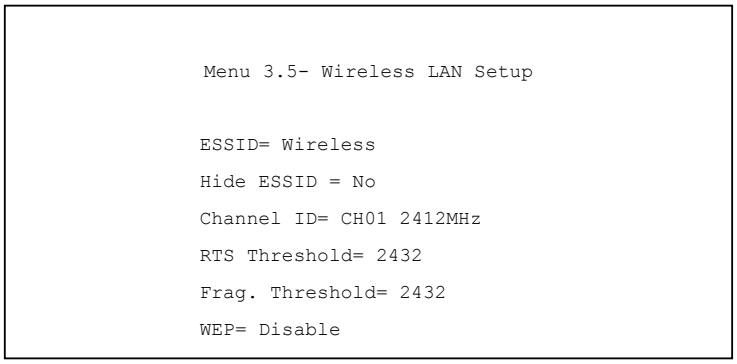


Рис. 25-1 Меню 3.5 - Настройка беспроводной LAN

В следующей таблице представлено описание полей данного меню.

Табл. 25-1 Меню 3.5 - Настройка беспроводной LAN

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
ESSID	The ESSID (Extended Service Set IDentifier/Идентификатор расширенного набора служб) определяет точку доступа, с которой связаны беспроводные станции. Беспроводные станции, связанные с точкой доступа должны иметь один и тот же ESSID. Введите идентифицирующее имя до 32 семибитных печатаемых символов в стандарте ASCII.	**Wireless**
Hide ESSID (Скрытый ESSID)	Нажмите клавишу пробела [SPACE BAR] и выберите **Yes** для скрытия ESSID в исходящем кадре "маяка" для того, чтобы станция не могла обнаружить ESSID при помощи пассивного сканирования.	**No**
Channel ID (Идентификатор канала)	Нажмите клавишу пробела [SPACE BAR] для выбора канала. Это позволяет установить рабочую частоту/канал, в зависимости от Вашей конкретной области.	**CH01 2412MHz**
RTS Threshold (Порог RTS)	Порог RTS (Request To Send/Запрос на передачу) (количество байт) предназначен для включения квитирования RTS/CTS. Данные с размером кадра больше, чем данное значение, обеспечат квитирование RTS/CTS. Настройка этой характеристики больше, чем максимальный размер MSDU (MAC service data unit), приведет к отключению квитирования RTS/CTS. Настройка этой характеристики близкой к нулю приведет к включению квитирования RTS/CTS. Введите значение от 0 до 2432.	**2432**
Frag. Threshold (Порог фрагментации)	Порог (количество байт) для границы фрагментации предназначен для отправляемых сообщений. Это максимальный размер фрагмента данных, который можно послать. Введите значение от 256 до 2432.	**2432**
WEP	WEP (Wired Equivalent Privacy/Конфиденциальность, равная Конфиденциальности в проводных сетях) обеспечивает шифрование данных, препятствующее доступу беспроводных станций к передаваемым через беспроводную сеть данным. Выберите **Disable** для того, чтобы беспроводные станции поддерживали связь с точками доступа без шифрования данных. Выберите **64-bit WEP** или **128-bit WEP** для ввода шифрования данных. WEP вызывает снижение производительности соединения.	**Disable**

Табл. 25-1 Меню 3.5 - Настройка беспроводной LAN

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Default Key (Ключ по умолчанию)	Введите номер ключа в качестве активного ключа.	
Key 1 to Key 4 (Ключи)	Если выбираете **64-bit WEP** в поле **WEP Encryption**, тогда введите 5 символов или 10 шестнадцатеричных символов ("0-9", "A-F"), предшествующих 0x для каждого ключа (1-4). Если выбираете **128-bit WEP** в поле **WEP Encryption**, тогда введите 13 символов или 26 шестнадцатеричных символов ("0-9", "A-F"), предшествующих 0x для каждого ключа (1-4). Существует четыре ключа шифрования данных для защиты данных от подслушивания неправомочными беспроводными пользователями. Значения для ключей должны быть установлены одинаковые как для точек доступа, так и для радиостанций.	
Edit MAC Address Filter (Редактирование фильтра MAC-адреса)	Для редактирования таблицы фильтрации MAC-адреса, нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите клавишу [ENTER] для вывода Меню 3.5.1.	**No**
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.		

25.2.1 Фильтр MAC-адреса беспроводной LAN

Следующий уровень безопасности представляет собой фильтр MAC-адреса. Для соединения беспроводной станции с Prestige, введите MAC-адрес сетевой беспроводной карты в таблицу MAC-адресов.

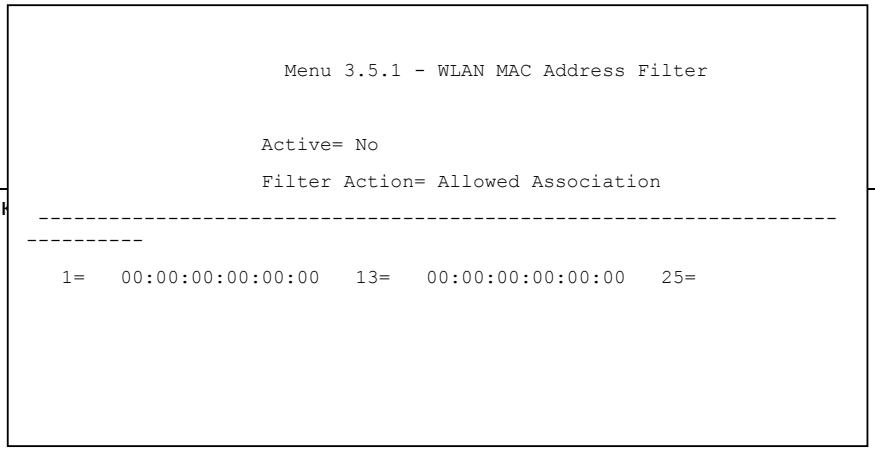


Рис. 25-2 Меню 3.5.1 - Фильтрация MAC-адреса WLAN

В следующей таблице представлено описание полей данного меню.

Табл. 25-2 Меню 3.5.1 - Фильтрация MAC-адреса WLAN

ПОЛЕ	ОПИСАНИЕ
Active (Активно)	Для включения фильтрации MAC-адреса, нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите [ENTER].
Filter Action (Действие фильтра)	Определите действие фильтра для списка MAC-адресов в таблице фильтр MAC-адресов. Для отказа в доступе к Prestige, нажмите клавишу пробела [SPACE BAR] для выбора **Deny Association** и нажмите клавишу [ENTER]. MAC-адресам, не указанным в списке, будет разрешен доступ к маршрутизатору. Действие по умолчанию, **Allowed Association**, разрешает соединение с Prestige. MAC-адресам, не указанным в списке будет отказано в доступе к маршрутизатору.
MAC Address Filter (Фильтр MAC-адреса)	
Address 1….	Введите MAC-адреса (в формате XX:XX:XX:XX:XX:XX) беспроводных станций, которым разрешено или отказано в доступе к Prestige.
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.	

Раздел 26
Доступ в Интернет

В этой главе описывается конфигурирование LAN и WAN в Prestige для доступа в Интернет.

26.1 Обзор доступа в Интернет

Для получения более подробной информации о полях экранных меню SMT, рассматриваемых в этой главе, см. главы по экранам LAN и WAN Web-конфигуратора.

26.2 Стратегии IP

Обычно, маршрутизация основывается *только* на адресе назначения, а маршрутизатор выбирает кратчайший 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. Создайте стратегии с помощью Меню 25 SMT (см. главу *Маршрутизация на базе стратегии IP*) и примените их к интерфейсам LAN и/или WAN Prestige, используя Меню 3.2 (LAN) и 11.3 (WAN).

26.3 Псевдоним IP

Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей с помощью одного интерфейса Ethernet. Prestige поддерживает три логических интерфейса LAN через один физический интерфейс Ethernet, при этом сам Prestige выступает в качестве шлюза для каждой сети LAN.

Если используется псевдоним IP, можно также сконфигурировать правила межсетевого экрана для контроля доступа к логическим сетям LAN (подсетям).

Убедитесь, что подсети логических сетей не перекрываются.

Следующий рисунок демонстрирует разбиение LAN на несколько подсетей A, B и C.

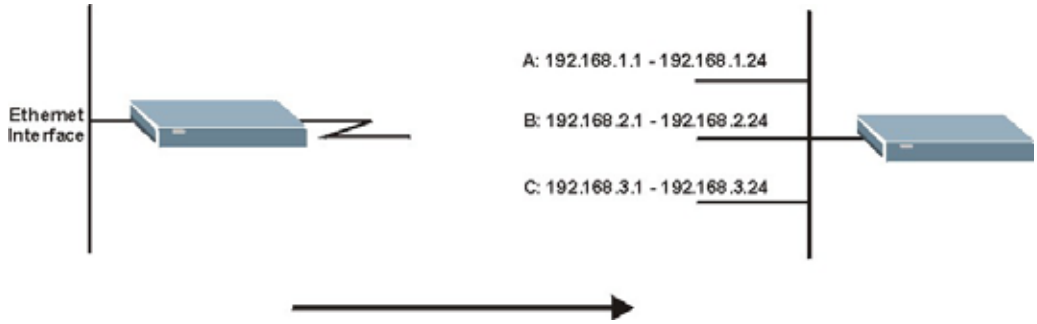


Рис. 26-1 Физическая сеть **Рис. 26-2 Разделение на логические сети**

Сконфигурируйте псевдоним IP на Prestige с помощью Меню 3.2.1.

26.4 Настройка псевдонима IP

Для конфигурирования первой сети используйте Меню 3.2. Переместите курсор к полю **Edit IP Alias** и переключите клавишей пробела [SPACEBAR] на **Yes**, а затем нажмите клавишу [ENTER] , чтобы сконфигурировать вторую и третью сеть.

```
Menu 3.2 - TCP/IP and DHCP Setup
DHCP Setup:
 DHCP= Server
 Client IP Pool Starting Addres= 192.168.1.33
 Size of Client IP Pool= 32
 Primary DNS Server= 0.0.0.0
 Secondary DNS Server= 0.0.0.0
 Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
```

Рис. 26-3 Меню 3.2 - Настройка TCP/IP и DHCP

При нажатии клавиши [ENTER] открывается **Меню 3.2.1 — IP Alias Setup** (**Настройка псевдонима IP)**, как показано 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
                 Outgoing protocol filters= N/A
               IP Alias 2= No
```

Рис. 26-4 Меню 3.2.1 - Настройка псевдонима IP

Следуйте указаниям по конфигурированию параметров псевдонима IP в приведенной ниже таблице.

Табл. 26-1 Меню 3.2.1 - Настройка псевдонима IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
IP Alias (Псевдоним IP)	Выберите **Yes** для конфигурирования сети LAN в Prestige.	**Yes**
IP Address (IP-адрес)	Введите IP-адрес Prestige в десятичном виде с разделительными точками	192.168.2.1
IP Subnet Mask (Маска подсети IP)	Prestige вычисляет маску подсети автоматически на основании назначенного IP-адреса. Пока не реализована организация подсетей, следует использовать маску подсети, вычисленную Prestige	255.255.255.0
RIP Direction (Направление RIP)	Нажмите клавишу пробела [SPACE BAR] для выбора направления RIP. Опциями являются: **None**, **Both**, **In Only** или **Out Only**.	**None**
Version (Версия)	Нажмите клавишу пробела [SPACE BAR] для выбора формата RIP. Опциями являются: **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 Prestige.	

Табл. 26-1 Меню 3.2.1 - Настройка псевдонима IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Outgoing Protocol Filters (Выходные фильтры протоколов)	Введите набор(ы) фильтров, которые должны применяться к исходящему трафику между этим узлом и Prestige.	
При 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 маршрута IP

Первым шагом является включение функции маршрутизации IP в **Меню 1 — General Setup (Настройка общих параметров)**.

Для редактирования Меню 1 введите 1 в Главном меню и нажмите клавишу [ENTER]. Установите **Yes** в поле **Route IP** нажатием клавиши пробел [SPACE BAR].

```
                        Menu 1 - General Setup
                    System Name= ?
                    Location= location
                    Contact Person's
Name=
                    Domain Name=
                    Edit Dynamic DNS=
No
```

Рис. 26-5 Меню 1 - Настройка общих параметров

26.6 Конфигурирование доступа в Интернет

Меню 4 предоставляет возможность в одной экранной форме установить все параметры доступа в Интернет. Фактически, Меню 4 представляет собой упрощенную настройку для одного из удаленных узлов, доступную через Меню 11. Прежде, чем выполнить конфигурирование Prestige для доступа в Интернет, необходимо получить учетную информацию для сети Интернет.

Используйте таблицу *Учетная информация для сети Интернет* в *Кратком руководстве* для занесения учетной информации. Следует отметить, что в случае использования инкапсуляции PPPoA или PPPoE необходима только информация по регистрационному имени и паролю, предоставляемая Интернет-провайдером. Если используется инкапсуляция ENET ENCAP, необходимо знать только IP-адрес шлюза инкапсуляции Ethernet.

В Главном меню введите 4 для вывода **Меню 4 - Internet Access Setup** (**Настройка доступа в Интернет)**, как показано ниже.

```
  Menu 4 - Internet Access Setup
ISP's Name= MyIsp
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 8
VCI #= 32
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
```

Рис. 26-6 Меню 4 - Настройка доступа в Интернет

В следующей таблице содержатся указания по конфигурированию Prestige для доступа в Интернет.

Табл. 26-2 Меню - 4 Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР

Табл. 26-2 Меню - 4 Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
ISP’s Name (Имя Интернет-провайдера)	Введите имя Интернет-провайдера. Эта информация нужна только для идентификации.	MyIsp
Encapsulation(Инкапсуляция)	Нажмите клавишу пробела [SPACE BAR] для выбора метода инкапсуляции, используемого Интернет-провайдером. Опциями являются: **PPPoE**, **PPPoA**, **RFC 1483** или **ENET ENCAP**.	ENET ENCAP
Multiplexing (Мультиплексирование)	Нажмите клавишу пробела [SPACE BAR] для выбора метода мультиплексирования, используемого Интернет-провайдером. Опциями являются: **на базе VC** или **на базе LLC**.	На базе LLC
VPI # (Номер VPI)	Введите идентификатор виртуального пути (VPI), предоставленный телефонной компанией.	8
VCI # (Номер VCI)	Введите идентификатор виртуального канала (VCI), предоставленный телефонной компанией.	32
ATM QoS Type (Тип QoS ATM)	Нажмите клавишу пробела [SPACE BAR] и выберите **CBR** (Continuous Bit Rate/Постоянная скорость передачи в битах) для определения фиксированной (всегда включена) пропускной способности. Выберите **UBR** (Unspecified Bit Rate - Не определена скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите **VBR** (Variable Bit Rate/Регулируемая скорость передачи в битах) для пульсирующего трафика и пропускной способности, совместимой с другими вариантами использования.	UBR
Peak Cell Rate (PCR) (Пиковая скорость ячеек)	Это — максимальная скорость, с которой отправитель может передавать ячейки. Введите PCR.	0
Sustain Cell Rate (SCR)= 0 (Поддерживаемая скорость ячеек) (ячеек/с) По умолчанию= 0 ячеек/с	Поддерживаемая скорость ячеек - это средняя скорость ячеек при пульсирующем трафике по принципу “включено-выключено“, а также один из параметров пульсирующего трафика. Введите SCR; всегда должно быть меньше PCR.	0

Табл. 26-2 Меню - 4 Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Maximum Burst Size (MBS)= 0 (Максимальный размер пакета)	Обозначает максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите MBS. MBS должно быть меньше 65535.	0
My Login (Регистрационное имя)	Сконфигурируйте поля **My Login** и **My Password** только для инкапсуляции PPPoA и PPPoE. Введите регистрационное имя, которое назначает Интернет-провайдер. Если используется инкапсуляция PPPoE, тогда данное поле должно быть в виде user@domain, где домен определяет название услуги PPPoE.	N/A
My Password (Пароль)	Введите пароль, соответствующий регистрационному имени, представленному выше.	N/A
ENET ENCAP Gateway (Шлюз ENET ENCAP)	Введите IP-адрес шлюза, предоставленный Интернет-провайдером, если используется инкапсуляция **ENET ENCAP**.	N/A
Idle Timeout (Время простоя)	Данное значение определяет сколько секунд проходит до того, как Prestige автоматически разъединяет сеанс связи PPPoE.	0
IP Address Assignment (Назначение IP-адреса)	Нажмите клавишу пробела [SPACE BAR] для выбора адреса назначения **Static** или **Dynamic**.	Dynamic
IP Address (IP-адрес)	Если доступно, введите IP-адрес, предоставленный Интернет-провайдером.	N/A
Network Address Translation (Трансляция сетевых адресов)	Нажмите клавишу пробела [SPACE BAR] для выбора **None**, **SUA Only** или **Full Feature**. Для подробной информации о SUA (Учетная запись одиночного пользователя) см. *главу NAT*.	SUA Only
Address Mapping Set (Набор преобразования адресов)	Введите число наборов преобразования (1-8) для использования с NAT. Для подробной информации см. главу *NAT*.	N/A

Табл. 26-2 Меню - 4 Настройка доступа в Интернет

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.		

Если все настройки верны, Prestige 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.

Раздел 27
Конфигурирование удаленного узла

В данной главе рассматривается конфигурирование удаленного узла.

27.1 Обзор настройки удаленного узла

В этой главе рассматриваются параметры удаленного узла, не зависящие от протокола. Удаленный узел необходим для отправки вызовов на удаленный шлюз. Удаленный узел представляет как удаленный шлюз, так и сеть WAN за ним. При настройке доступа в Интернет в Меню 4 конфигурируются параметры одного из удаленных узлов.

Вначале выберите удаленный узел в **Меню 11- Remote Node Setup (Настройка удаленного узла)**. Затем в Меню 11.1 можно отредактировать настройки этого узла, а также сконфигурировать особые настройки в трех подменю: редактирование параметров IP и моста в Меню 11.3; редактирование параметров ATM в Меню 11.6; и редактирование набора фильтров в Меню 11.5.

27.2 Настройка удаленного узла

В этой главе рассматриваются параметры удаленного узла, не зависящие от протокола.

27.2.1 Настройки пользователя для удаленного узла

Для конфигурирования удаленного узла нужно выполнить следующие действия:

Step 1. Ввести 11 в Главном меню для перехода в **Меню 11 - Remote Node Setup (Настройка удаленного узла).**

Step 2. Когда Меню 11 появится на экране, как показано на следующем рисунке, введите номер удаленного узла, который нужно сконфигурировать.

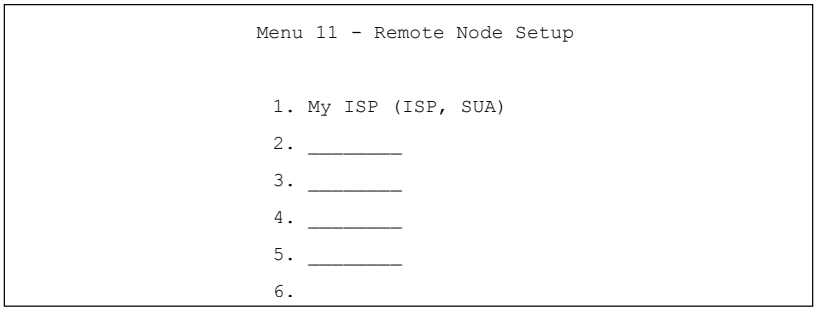


Рис. 27-1 Меню 11 - Настройка удаленного узла

27.2.2 Сценарии инкапсуляции и мультиплексирования

Для обеспечения доступа в Интернет должны использоваться методы инкапсуляции и мультиплексирования, предписанные Вашим Интернет-провайдером. Проконсультируйтесь с Вашей телефонной компанией относительно использования методов инкапсуляции и мультиплексирования для соединения локальных сетей, напр. филиалов и головного офиса компании. Об используемых методах инкапсуляции и мультиплексирования должно быть заключено предварительное взаимное соглашение, так как механизма автоматического определения метода не существует. Выбор методов инкапсуляции и мультиплексирования также зависит от количества имеющихся виртуальных каналов и количества необходимых сетевых протоколов. Дополнительная служебная информация, требуемая для инкапсуляции ENET ENCAP, делает эти методы нерентабельными для соединения локальных сетей. Далее приведено несколько примеров комбинаций, более подходящих для реализации этой задачи.

Сценарий 1. Один виртуальный канал, множество протоколов

Инкапсуляция PPPoA (RFC-2364) с мультиплексированием **на базе VC** является наиболее оптимальной комбинацией, так как не требуется дополнительный протокол для идентификации заголовков. 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 байт). Однако, если в дальнейшем возникнет необходимость в поддержке множества протоколов, более удобной может оказаться инкапсуляция **PPPoA**, а не **RFC-1483**, так как не придется переконфигурировать все 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**.

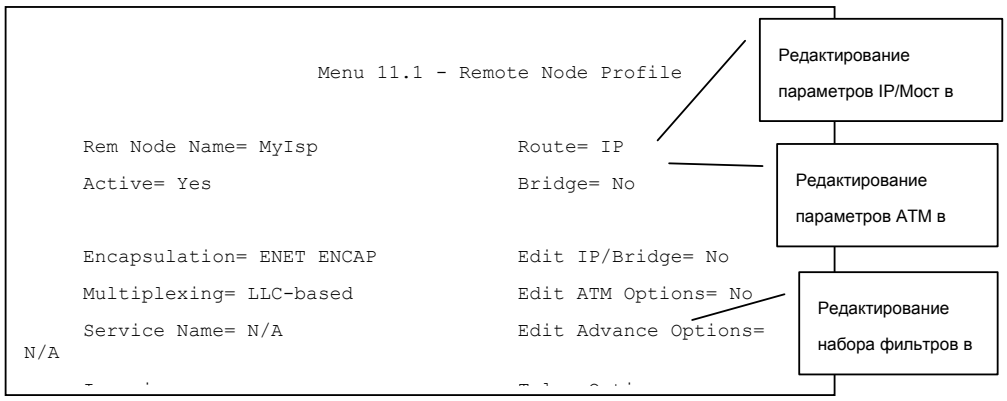


Рис. 27-2 Меню 11.1 - Настройки пользователя для удаленного узла

В **Меню 11.1 – Remote Node Profile(Настройки пользователя для удаленного узла)** заполните поля, 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 до восьми символов для удаленного узла.	MyIsp
Active (Активен)	Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для переключения между **Yes** и **No**. Неактивные узлы обозначаются знаком минус “–“, стоящим перед именем узла в Меню 11 SMT.	**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 адаптации 5 ATM). Если выбрано RFC-1483 (многопротокольная инкапсуляция через уровень адаптации 5 ATM) **ENET ENCAP**, то поля **Rem Login**, **Rem Password**, **My Login**, **My Password** и **Authen** недоступны (**N/A**).	**ENET ENCAP**
Multiplexing (Мультиплексирование)	Нажмите клавишу пробела [SPACE BAR], затем клавишу [ENTER] для выбора метода мультиплексирования, используемого Интернет-провайдером: **VC-based** или **LLC-based**.	**LLC-based**
Service Name (Название услуги)	Введите имя услуги PPPoE, если используется инкапсуляция **PPPoE**.	N/A
Incoming: (Входящий)		
Rem Login (Регистрационное имя удаленного узла)	Введите регистрационное имя, которое данный удаленный узел будет использовать при вызове Prestige. Регистрационное имя вместе с **Rem Password** будет использоваться для аутентификации данного узла.	
Rem Password (Пароль удаленного узла)	Введите пароль, который данный удаленный узел будет использовать при вызове Prestige.	
Outgoing: (Исходящий)		
My Login (Регистрационное имя)	Введите регистрационное имя, назначенное Интернет-провайдером, которое Prestige будет использовать при вызове данного удаленного узла.	
My Password (Пароль)	Введите пароль, назначенный Интернет-провайдером, который Prestige будет использовать при вызове данного удаленного узла.	
Authen (Аутентификация)	Данное поле устанавливает протокол аутентификации, используемый для исходящих вызовов. Опциями для этого поля являются: **CHAP**/**PAP** – Prestige 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)	Данное поле определяет протокол, согласно которому будет производиться маршрутизация. Опциями являются: **IP** и **None.**	**IP**
Bridge (Мост)	Если передача по мосту включена, Prestige будет пересылать любой пакет, который он не распознает, на данный удаленный узел; в противном случае, все пакеты сбрасываются. Выберите **Yes** для включения или **No** для отключения.	**No**
Edit IP/Bridge (Редактирование IP/моста)	Нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите клавишу [ENTER] для перехода в **Меню 11.3 – Remote Node Network Layer Options (Параметры сетевого уровня для удаленного узла)**.	**No**
Edit ATM Options (Редактирование параметров ATM)	Нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите клавишу [ENTER] для перехода в **Меню 11.6 – Remote Node ATM Layer Options (Параметры уровня ATM для удаленного узла)**.	**No**
Edit Advance Options (Редактирование дополнительных параметров)	Данное поле доступно только в случае выбора **PPPoE** в поле **Encapsulation**. Нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите клавишу [ENTER] для перехода в **Меню 11.8 – Advance Setup Options (Редактирование дополнительных параметров)**.	**No**
Telco Option (Опции телефонного соединения)		
Allocated Budget (min) (Выделенный бюджет) (мин)	В этом поле устанавливается предельное значение времени исходящих вызовов для данного удаленного узла. Установкой по умолчанию для этого поля является - 0, что означает, что бюджет не контролируется.	

Табл. 27-1 Меню 11.1 - Настройки пользователя для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Period (hr) (Период) (ч)	В этом поле указывается промежуток времени, через который бюджет сбрасывается. Напр., если разрешается совершение вызова на данный удаленный узел в течение максимум 10 минут за каждый час, тогда **Allocated Budget -** (10 минут), а **Period (hr)** - 1 (час).	
Schedule Sets (Наборы расписаний)	Данное поле доступно только в том случае, если используется инкапсуляция **PPPoE** или **PPPoA**. Можно выбрать до четырех наборов расписаний. Для получения более подробной информации см. главу *Составление расписания вызовов*.	
Nailed up Connection (Полупостоянное соединение)	Данное поле доступно только в том случае, если используется инкапсуляция **PPPoE** или **PPPoA**. Данное поле заполняется в том случае, если необходимо установить полупостоянное соединение с данным удаленным узлом. Более подробная информация представлена ранее в этом разделе.	
Session Options (Параметры сеанса связи)		
Edit Filter Sets (Редактирование наборов фильтров)	Нажмите клавишу пробел [SPACE BAR] 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 простоя) (с)	Введите время в секундах (0-9999), которое может проходить с момента, когда Prestige находится в ожидании (нет трафика на удаленный узел), до того как Prestige автоматически отключается от удаленного узла. 0 - означает, что сеанс связи не будет блокироваться по времени.	
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.		

27.2.3 Протокол аутентификации исходящих вызовов

По вполне понятным причинам рекомендуется использовать максимально надежный протокол аутентификации. Однако, некоторые реализации оборудования используют в качестве настроек пользователя специфические протоколы аутентификации. Если для такого устройства будет задан

протокол аутентификации, отличающийся от установленного в настройках пользователя, вызов будет автоматически разъединен. Если удаленный узел разъединяет вызов после успешной аутентификации, следует убедиться, что используется правильный протокол аутентификации для данного устройства.

27.3 Параметры сетевого уровня для удаленного узла

Для настройки параметров TCP/IP следует выполнить ряд действий по редактированию в **Меню 11.3 – Remote Node Network Layer Options (Параметры сетевого уровня для 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**, нажмите клавишу пробела [SPACE BAR] для выбора **Yes,** а затем нажмите клавишу [ENTER] для перехода в **Меню 11.3** – **Remote Node**

```
          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= Full Feature
```

Network Layer Options (Параметры сетевого уровня для удаленного узла).

Рис. 27-3 Меню 11.3 - Параметры сетевого уровня для удаленного узла

В следующей таблице рассматриваются поля в **Меню 11.3 – Параметры сетевого уровня для удаленного узла**.

Табл. 27-2 Меню 11.3 - Параметры сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
IP Address Assignment (Назначение IP-адреса)	Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для выбора **Dynamic**, если удаленный узел использует динамически назначенный IP-адрес или **Static**, если он использует статический (фиксированный) IP-адрес. Это можно будет сконфигурировать только в узле Интернет-провайдера (узел, конфигурируемый в Меню 4), для всех других узлов устанавливается **Static**.	**Dynamic**
Rem IP Addr (IP-адрес удаленного шлюза)	IP-адрес, введенный в предыдущем меню.	
Rem Subnet Mask (Маска подсети для удаленного узла)	Введите маску подсети, назначенную 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 такой случай, введите IP-адрес, назначенный порту WAN Prestige. ПРИМЕЧАНИЕ: Это адрес местного Prestige, а не удаленного маршрутизатора.	
NAT	Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для выбора **Full Feature**, если для Prestige имеется общедоступный IP-адрес WAN. Выберите **SUA Only**, если для Prestige имеется только один общедоступный IP-адрес WAN. SMT использует набор преобразования адресов 255 (Меню 15.1 - см. *раздел 30.3.1*). Выберите **None** для отключения NAT.	**SUA Only**
Address Mapping Set (Набор преобразования адресов)	Если выбрано **Full Feature** в поле **NAT**, следует сконфигурировать набор преобразования адресов в Меню 15.1. Выберите один из наборов (2-10) сервера NAT в Меню 15.2 (для дополнительной информации см. главу *NAT*) и введите этот номер здесь. Если выбрано **SUA Only** в поле NAT, SMT использует набор 1 сервера NAT в Меню 15.2 (для дополнительной информации см. *NAT*).	2

Табл. 27-2 Меню 11.3 - Параметры сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Metric (Метрика)	Метрика определяет “стоимость” передачи и используется для целей маршрутизации. Маршрутизация IP использует счетчик переходов по сети в качестве своего рода единицы “стоимости“, с минимальным значением равным 1, соответствующим 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 хорошо подходят значения 2 или 3.	2
Private (Частный)	Этот параметр определяет, будет ли Prestige 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)	Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для выбора направления RIP. Опциями являются: **Both**, **In Only**, **Out Only** или **None**.	**None**
Version (Версия)	Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для выбора версии RIP. Опциями являются: **RIP-1**, **RIP-2B** или **RIP-2M**.	**RIP-1**
Multicast (Многоадресная рассылка)	**IGMP-v1** устанавливает версию 1 для IGMP, **IGMP-v2** устанавливает версию 2 для IGMP и **None** отключает IGMP.	**None**
IP Policies (Стратегии IP)	Можно применить до четырех наборов стратегий IP (из двенадцати), введя их номера через запятую. Вначале сконфигурируйте наборы фильтров в Меню 25 (см. главу *Маршрутизация на базе стратегии IP*), а затем примените их здесь.	3, 4, 5, 6
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.		

27.3.1 Пример IP-адресации поля My WAN Addr

На следующем рисунке на примере IP-адресации разъясняется смысл поля **My WAN Addr** в Меню 11.3. Для краткого обзора, что представляет собой IP-адрес WAN, обратитесь к предыдущему

рисунку *IP-адреса LAN и WAN* в главе Web-конфигуратора по настройке LAN. **My WAN Addr** обозначает местный IP WAN для Prestige (172.16.0.1 на следующем рисунке), а **Rem IP Addr** обозначает удаленный IP WAN (172.16.0.2 на следующем рисунке).

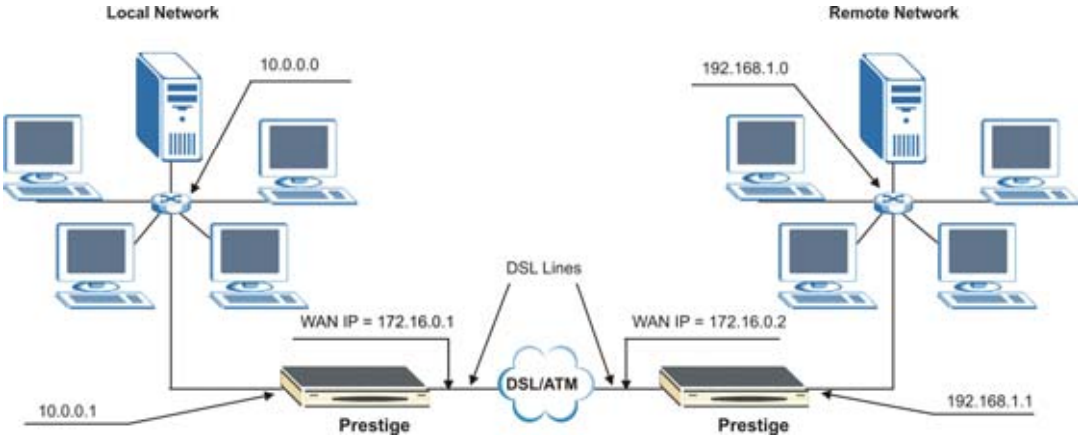


Рис. 27-4 Пример IP-адресации для соединения локальных сетей на базе TCP/IP

27.4 Фильтр удаленного узла

В Меню 11.1 переместите курсор в поле **Edit Filter Sets** и нажмите клавишу пробела [SPACE BAR] для выбора **Yes**. Нажмите клавишу [ENTER] для вывода **Меню 11.5 – Remote Node Filter (Фильтр удаленного узла)**.

В **Меню 11.5 – Remote Node Filter (Фильтр удаленного узла)** задайте набор(ы) фильтров для применения к входящему и исходящему трафику между данным удаленным узлом и Prestige, а также для блокировки инициирования вызовов определенными пакетами. В каждом поле фильтра можно задать до четырех наборов фильтров, введя их номера через запятую, напр., 1, 5, 9, 12.

В данном поле допускается использование пробелов. Prestige поставляется с готовым набором фильтров, NetBIOS_WAN, который блокирует пакеты NetBIOS. 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:
```

Рис. 27-5 Меню 11.5 - Фильтр удаленного узла (инкапсуляция RFC 1483 или ENET)

```
Menu 11.5 - Remote Node Filter

        Input Filter Sets:
          protocol filters= 11, 12
            device filters=
        Output Filter Sets:
          protocol filters=
```

Рис. 27-6 Меню 11.5 - Фильтр удаленного узла (инкапсуляция PPPoA или PPPoE)

27.5 Редактирование параметров уровня ATM

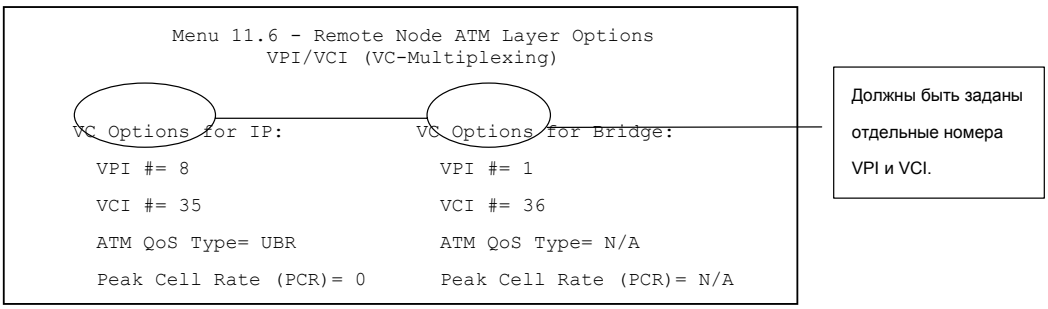
Для редактирования **Меню 11.6 – Remote Node ATM Layer Options (Параметры уровня ATM для удаленного узла)** следует выполнить описанные ниже действия.

В Меню 11.1 переместите курсор в поле **Edit ATM Options** и нажмите клавишу [SPACE BAR] для выбора **Yes**. Нажмите клавишу [ENTER] для перехода в **Меню 11.6 – Remote Node ATM Layer Options** (**Параметры уровня ATM для удаленного узла)** .

Существует два варианта Меню 11.6 для Prestige в зависимости от выбранного в Меню 11.1 метода мультиплексирования - **на базе VC** или **на базе LLC** и инкапсуляции **PPP**.

27.5.1 Мультиплексирование на базе VC (не инкапсуляция PPP)

При мультиплексировании **на базе VC**, по предварительному соглашению, за протоколом закрепляется конкретный виртуальный канал, напр., VC1 передает IP. Для каждого протокола



должны быть заданы отдельные номера VPI и VCI.

Рис. 27-7 Меню 11.6 для мультиплексирования на базе VC

27.5.2 Мультиплексирование на базе LLC или инкапсуляция PPP

При мультиплексировании **на базе LLC** или использовании инкапсуляции **PPP** один виртуальный канал передает несколько протоколов с идентифицирующей информацией, которая содержится в заголовке каждого пакета.

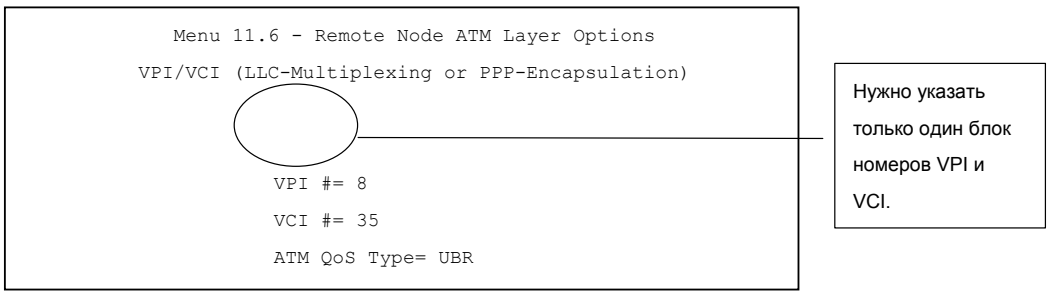


Рис. 27-8 Меню 11.6 для мультиплексирования на базе LLC или инкапсуляции PPP

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

27.5.3 Параметры дополнительной настройки

В Меню 11.1 выберите **PPPoE** в поле **Encapsulation**.

```
                    Menu 11.1 - Remote Node Profile


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


  Encapsulation= PPPoE              Edit IP/Bridge= No
  Multiplexing= LLC-based              Edit ATM Options= No
  Service Name=                        Edit Advance Options=
Yes
  Incoming:                            Telco Option:
    Rem Login=                           Allocated
```

Рис. 27-9 Меню 11.1 - Настройки пользователя для удаленного узла

Переместите курсор в поле **Edit Advance Options**, нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите клавишу [ENTER] для перехода в **Меню 11.8 – Advance Setup Options (Параметры дополнительной настройки)**.

```
              Menu 11.8 - Advance Setup Options


          PPPoE pass-through= No
```

Рис. 27-10 Меню 11.8 - Параметры дополнительной настройки

В следующей таблице представлено описание полей данного меню.

Табл. 27-3 Меню 11.8 Параметры дополнительной настройки

ПОЛЕ	ОПИСАНИЕ
PPPoE pass-through (Транзитная пересылка PPPoE)	Нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите клавишу [ENTER] для включения транзитной пересылки PPPoE. В дополнение к встроенному в Prestige клиенту PPPoE, можно включить пересылку PPPoE, допускающую до десяти хостов в LAN, использующих программное обеспечение PPPoE-клиентов на своих компьютерах для подключения к Интернет-провайдеру при помощи Prestige. Каждый хост может иметь отдельную учетную запись и общедоступный IP-адрес WAN. Транзитная пересылка PPPoE является вариантом использования NAT, где NAT не назначен. Нажмите клавишу пробела [SPACE BAR] для выбора **No**, а затем нажмите клавишу [ENTER] для отключения пересылки PPPoE, если нет необходимости допускать хосты в LAN, использующие клиентское программное обеспечение PPPoE на своих компьютерах, для подключения к Интернет-провайдеру.
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.	

Раздел 28
Настройка статического маршрута

В этой главе рассматривается настройка статического маршрута IP.

28.1 Обзор статического маршрута IP

Статические маршруты сообщают Prestige информацию о маршрутизации, которую он не может получить автоматически другими средствами. Такая ситуация может возникнуть, если обмен RIP запрещен в локальной сети или если удаленная сеть не подключена непосредственно к удаленному узлу.

Каждый удаленный узел определяет только ту сеть, к шлюзу которой он непосредственно подключен, при этом Prestige не владеет никакой информацией о других сетях. Например, на приведенном ниже рисунке Prestige получает информацию о сети N2 через маршрутизатор 1 удаленного узла. Тем не менее, Prestige не может маршрутизировать пакеты в сеть N3, так как он не знает о существовании маршрута через маршрутизатор 1 удаленного узла (через маршрутизатор 2). Статические маршруты и предназначены для того, чтобы предоставлять Prestige информацию о сетях за пределами удаленных узлов.

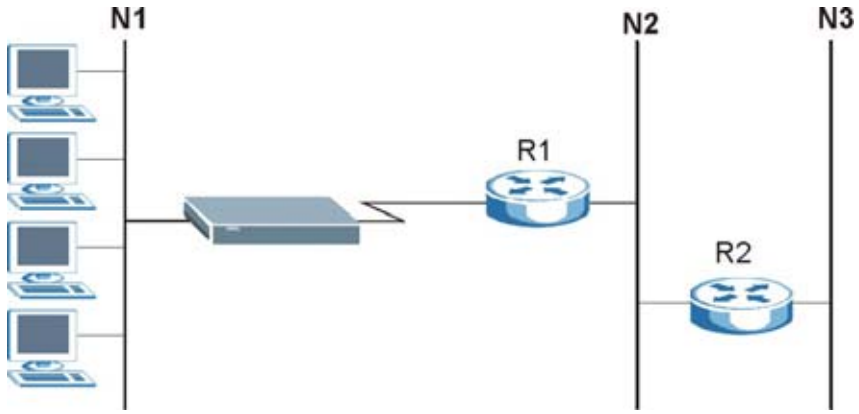


Рис. 28-1 Пример топологии статической маршрутизации

28.2 Конфигурирование

Step 1. Для конфигурирования статического маршрута IP следует использовать **Меню 12 – Static Route Setup (Настройка статического маршрута),** как показано ниже.

```
Menu 12 - Static Route Setup


        1. IP Static Route
        3. Bridge Static Route
```

Рис. 28-2 Меню 12 - Настройка статического маршрута

Step 2. В Меню 12 выберите 1 для перехода в **Меню 12.1 — IP Static Route Setup (Настройка статического маршрута IP)**, показанное ниже.

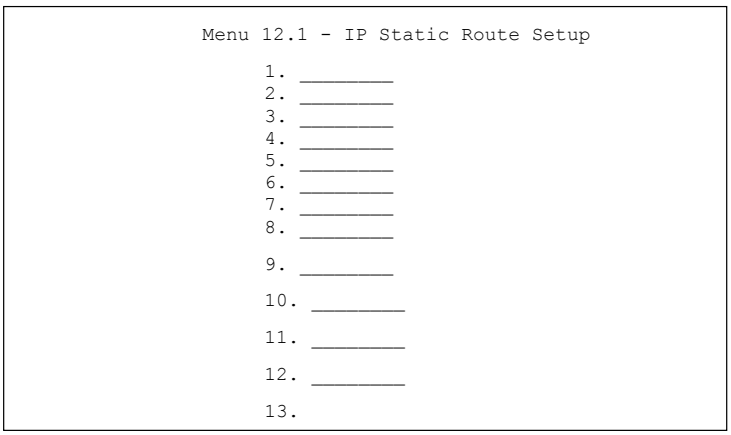


Рис. 28-3 Меню 12.1 - Настройка статического маршрута IP

Step 3. После этого введите индекс одного из маршрутов, которые нужно сконфигурировать.

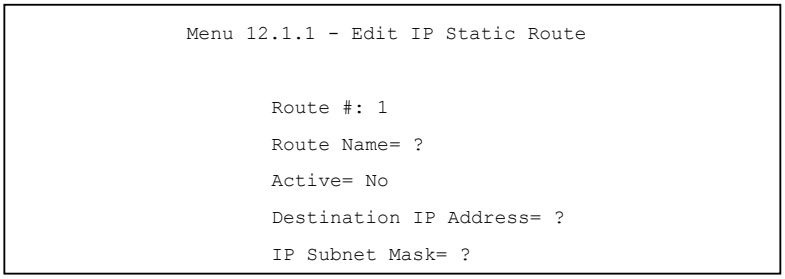


Рис. 28-4 Меню12.1.1 - Редактирование статического маршрута IP

В следующей таблице описываются поля **Меню 12.1.1 – Edit IP Static Route (Редактирование статического маршрута IP)**.

Табл. 28-1 Меню 12.1.1 - Редактирование статического маршрута IP

ПОЛЕ	ОПИСАНИЕ
Route # (Номер маршрута)	Индекс статического маршрута, выбранный в Меню 12.1.
Route Name (Имя маршрута)	Введите идентифицирующее имя для данного маршрута. Эта информация нужна только для идентификации.
Active (Активно)	Данное поле предназначено для включения/отключения данного статического маршрута.
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. Это нужно, чтобы сетевой номер был такой же, как и идентификационный номер (ID) хост-машины.
IP Subnet Mask (Маска подсети IP)	Введите маску подсети для данного назначения. См. порядок назначения *масок подсети IP* в этом руководстве.
Gateway IP Address (IP-адрес шлюза)	Введите IP-адрес шлюза. Шлюзом является ближайшее к Prestige устройство, которое будет пересылать пакет по назначению. В локальной сети шлюзом должен быть маршрутизатор, находящийся в том же сегменте, что и Prestige. В глобальной сети адресом шлюза должен быть IP-адрес одного из удаленных узлов.

Табл. 28-1 Меню 12.1.1 - Редактирование статического маршрута IP

ПОЛЕ	ОПИСАНИЕ
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 хорошо подходят значения 2 или 3.
Private (Частный)	Этот параметр определяет, будет ли Prestige включать данный маршрут к удаленному узлу в циркулярную рассылку RIP. Если установлено **Yes**, данный маршрут считается частным и не включается в циркулярную рассылку пакетов RIP. Если установлено **No**, данный маршрут к удаленному узлу является доступным для других хост-машин через циркулярную рассылку RIP.
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.	

Раздел 29
Настройка межсетевого моста

В данной главе описывается конфигурирование параметров Prestige для межсетевого моста.

29.1 Общие сведения о межсетевом мосте

При передаче по мосту переадресация производится на основе MAC (Media Access Control/Управление доступом к среде), или аппаратного адреса, в то время как маршрутизация осуществляет это на основе адреса сетевого уровня (IP). Передача по мосту позволяет Prestige передавать пакеты для протоколов сетевого уровня, которые не маршрутизируются, напр., SNA, из одной сети в другую. 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 процессора и памяти.

По причинам, связанным с рентабельностью, *не* следует включать передачу по мосту, пока не возникнет необходимость в сетевой поддержке других протоколов, кроме IP. Для IP следует включить маршрутизацию; не следует передавать по мосту то, что Prestige может маршрутизировать.

29.2 Настройка моста Ethernet

В основном, все не локальные пакеты передаются по мосту в WAN. Prestige не поддерживает IPX.

29.2.1 Настройка передачи по мосту для удаленного узла

Для конфигурирования независимых от протокола параметров в **Меню 11.1 – Remote Node Profile (Настройки удаленного узла)** следует выполнить процедуру, описанную в другом разделе. Для специфических параметров передачи по мосту следует **сконфигурировать Меню 11.3 – Remote Node Network Layer Options (Параметры сетевого уровня для удаленного узла)**.

Для настройки параметров **Меню 11.3 – Remote Node Network Layer Options (Параметры сетевого уровня для удаленного узла**), нужно выполнить следующие действия:

Step 1. В Меню 11.1 убедитесь, что в поле **Bridge** установлено **Yes**.

```
                        Menu 11.1 - Remote Node Profile

    Rem Node Name= ?                        Route= IP
    Active= Yes                             Bridge= Yes

    Encapsulation= ENET ENCAP               Edit IP/Bridge= No
    Multiplexing= VC-based                  Edit ATM Options= No
    Service Name= N/A                       Edit Advance Options= N/A
    Incoming:                               Telco Option:
      Rem Login= N/A                          Allocated Budget(min)=
N/A
```

Рис. 29-1 Меню 11.1 - Настройки удаленного узла

Step 2. Переместите курсор в поле **Edit IP/Bridge**, затем нажмите клавишу пробела [SPACE BAR] для переключения на **Yes** и клавишу [ENTER] для редактирования **Меню 11.3 – Remote Node Network Layer Options (Параметры 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
```

Рис. 29-2 Меню 11.3 - Параметры сетевого уровня для удаленного узла

Табл. 29-1 Параметры сетевого уровня для удаленного узла : Поля межсетевого моста

ПОЛЕ	ОПИСАНИЕ
Bridge (Мост) (Меню 11.1)	Убедитесь, что в данном поле установлено **Yes**.
Edit IP/Bridge (Редактирование IP/моста) (Меню 11.1)	Нажмите клавишу пробела [SPACE BAR] для переключения на **Yes**, а затем клавишу [ENTER] для перехода в Меню 11.3.
Ethernet Addr Timeout (min.) (Тайм-аут адресации в Ethernet) (мин) (Меню 11.3)	Введите время (количество минут), в течение которого Prestige должен сохранять информацию адреса Ethernet в своих внутренних таблицах, когда линия отключена. Если данная информация сохраняется, тогда Prestige не придется перекомпилировать таблицы при повторном установлении линии.
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.	

29.2.2 Настройка статического маршрута для моста

Аналогично статическим маршрутам сетевого уровня, статические маршруты для моста сообщают Prestige, как достичь узла до того, как будет установлено соединение. Статические маршруты для моста конфигурируются в Меню 12.3.1 (перейдите в Меню 12, выберите 3, затем выберите редактирование статического маршрута), как показано ниже.

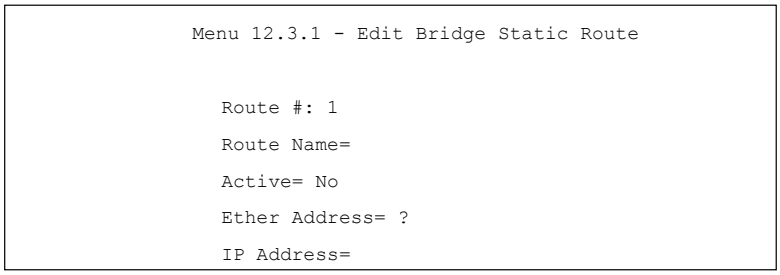


Рис. 29-3 Меню 12.3.1 - Редактирование статического маршрута для моста

Следующая таблица описывает меню **Edit Bridge Static Route**.

Табл. 29-2 Меню 12.3.1 - Редактирование статического маршрута для моста

ПОЛЕ	ОПИСАНИЕ
Route # (Номер маршрута)	Индекс маршрута, выбранный в **Меню 12.3 – Bridge Static Route Setup**.
Route Name (Имя маршрута)	Введите имя статического маршрута для моста (для целей идентификации).
Active (Активен)	Показывает, активен (**Yes**) или нет (**No**) статический маршрут.
Ether Address (Адрес Ethernet)	Введите MAC-адрес машины назначения, на который по мосту должны передаваться пакеты.
IP Address (IP-адрес)	Если возможно, введите IP-адрес машины назначения, на который по мосту должны передаваться пакеты.
Gateway Node (Шлюзовой узел)	Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для выбора номера удаленного узла (от 1 до 8), который является шлюзом для статического маршрута.
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.	

Раздел 30
Трансляция сетевых адресов (NAT)

В этой главе описывается конфигурирование NAT в Prestige.

30.1 Применение NAT

Необходимо создать правило межсетевого экрана в дополнение к созданию SUA/NAT для того, чтобы трафик из WAN пересылался через Prestige.

30.1.1 SUA (Single User Account/Учетная запись одиночного пользователя) в сравнении с NAT

SUA (Single User Account/Учетная запись одиночного пользователя) представляет собой реализацию ZyNOS подсети NAT, которая поддерживает два типа отображения, **Many-to-One** и **Server**. Для получения подробного описания набора NAT для SUA см. *раздел 30.3.1*. Prestige также поддерживает **Full Feature** NAT для преобразования многочисленных глобальных IP-адресов в многочисленные частные IP-адреса LAN клиентов или серверов при помощи типов отображения.

3. **Выберите** SUA Only**, если для Prestige имеется только один общедоступный IP-адрес WAN.**

4. **Выберите** Full Feature**, если для Prestige имеется множество общедоступных IP-адресов WAN.**

30.2 Применение NAT

Примените NAT с помощью меню 4 или 11.3, как показано далее. На следующем рисунке показывается как применить NAT для доступа в Интернет в Меню 4. В Главном меню введите 4 для перехода в **Меню 4 - Internet Access Setup (Настройка доступа в Интернет)**.

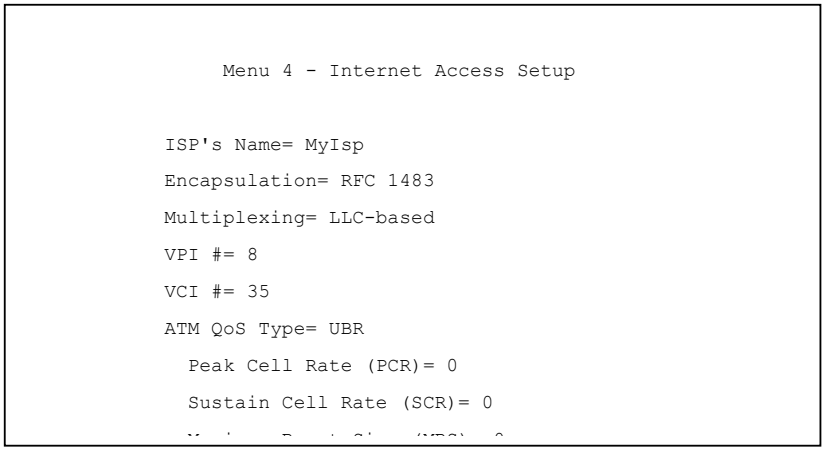


Рис. 30-1 Меню 4 - Использование NAT для доступа в Интернет

Следующий рисунок демонстрирует использование NAT для удаленного узла в Меню 11.1.

Step 1. В Главном меню введите 11.

Step 2. Когда Меню 11 появится на экране, как показано на следующем рисунке, введите номер удаленного узла, который нужно сконфигурировать.

Step 3. Переместите курсор в поле **Edit IP/Bridge**, нажмите клавишу пробела [SPACE BAR] для выбора **Yes**, а затем нажмите клавишу [ENTER] для перехода в Меню **11.3 - Remote Node Network Layer Options (Параметры сетевого уровня для удаленного узла).**

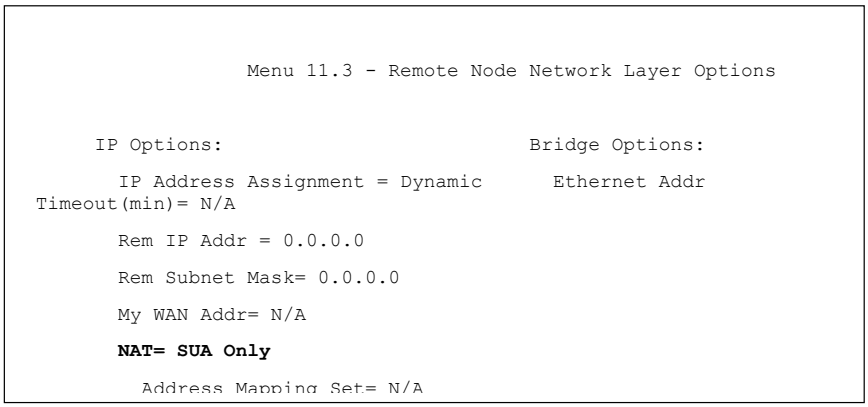


Рис. 30-2 Меню 11.3 - Использование NAT для удаленного узла

В следующей таблице представлено описание параметров NAT.

Табл. 30-1 Использование NAT в Меню 4 и 11.3

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
NAT (Трансляция сетевых адресов)	Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для выбора **Full Feature**, если для Prestige имеется множество общедоступных IP-адресов WAN. SMT использует набор преобразования адресов, который нужно сконфигурировать и ввести в поле **Address Mapping Set** (Меню 15.1 - см. раздел *30.3.1*).	**Full Feature**
	Выберите **None** для отключения NAT.	**None**
	При выборе **SUA Only**, SMT использует набор преобразования адресов 255 (Меню 15.1 - см. see раздел *30.3.1*). Выберите **SUA Only**, если для Prestige имеется только один общедоступный IP-адрес WAN.	**SUA Only**

30.3 Настройка NAT

Для создания таблицы отображения, используемой для назначения глобальных адресов компьютерам в LAN, используйте меню и подменю набора преобразования адресов. **Набор 255** - применяется для SUA. При выборе **Full Feature** в Меню 4 или 11.3, SMT будет использовать **Набор 1**. При выборе **SUA Only**, SMT будет использовать заранее сконфигурированный **Набор 255** (только для чтения).

Набор серверов - это группа серверов LAN, преобразованных во внешние порты. Для использования этого набора, необходимо создать правило сервера в наборе преобразования адресов NAT. Для получения подробной информации по этим меню, обратитесь к разделу о переадресации порта в главе по экранным меню Web-конфигуратора NAT. Для конфигурирования NAT, в Главном меню введите 15 для отображения следующего экрана.

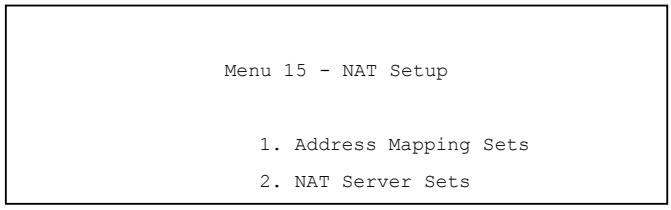


Рис. 30-3 Меню 15 - Настройка NAT

30.3.1 Наборы преобразования адресов

Ввести 1 для перехода в **Меню 15.1 — Address Mapping Sets (Наборы преобразования адресов)**.

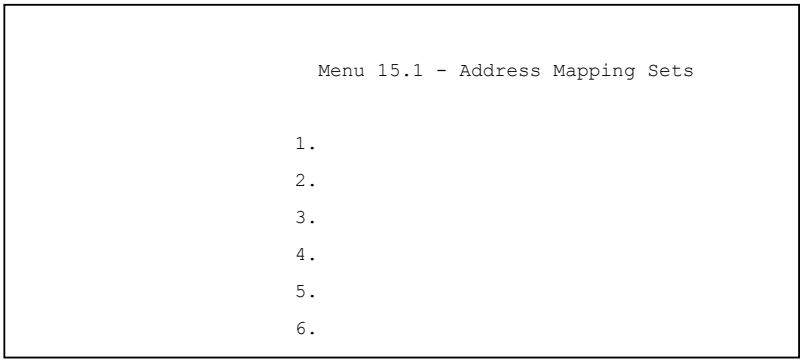


Рис. 30-4 Меню 15.1 - Наборы преобразования адресов

Набор преобразования адресов для SUA

Введите 255 для перехода к следующему экрану (см. также *раздел 30.1.1)*. Поля данного Меню не могут быть изменены.

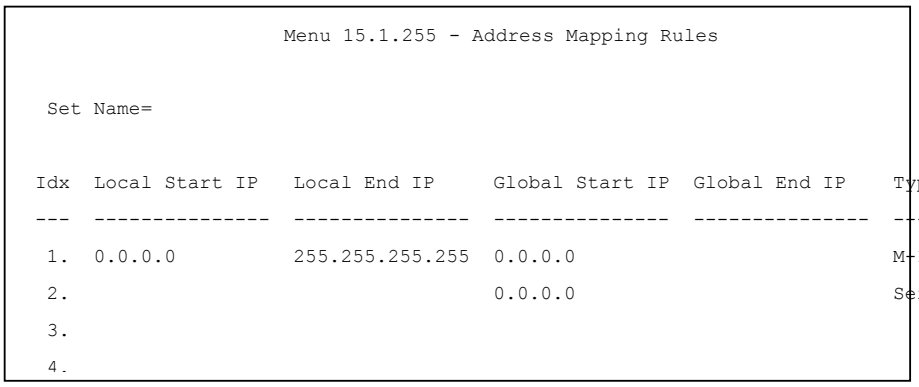


Рис. 30-5 Меню 15.1.255 - Правила преобразования адресов для SUA

В следующей таблице представлено описание полей данного меню.

Меню 15.1.255 используется только для чтения.

Табл. 30-2 Правила преобразования адресов для SUA

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Set Name (Название набора)	Название набора, выбранного в Меню 15.1, или введите название нового набора, который нужно создать.	Учетная запись одиночного пользователя (SUA)
Idx	Индекс или номер правила.	1
Local Start IP (Начальный локальный IP)	**Local Start IP** - начальный локальный IP-адрес (ILA).	0.0.0.0
Local End IP (Конечный локальный IP)	**Local End IP** - конечный локальный IP-адрес (ILA). Если правило соответствует всем локальным IP, тогда начальный IP - 0.0.0.0, а конечный IP - 255.255.255.255.	255.255.255.255
Global Start IP (Начальный глобальный IP)	Начальный глобальный IP-адрес (IGA). Если имеется динамический IP-адрес, введите 0.0.0.0 как **Global Start IP**.	0.0.0.0

Табл. 30-2 Правила преобразования адресов для SUA

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Global End IP (Конечный глобальный IP)	Конечный глобальный IP-адрес (IGA).	
Type (Тип)	Типы отображения. **Server** позволяет установить множество серверов различных типов позади NAT для данной машины. Примеры представлены далее.	Server
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.		

Наборы преобразования адресов, определяемые пользователем

Теперь обратим внимание на опцию 1 в Меню 15.1. Введите 1 для отображения этого меню. Посмотрим на различия от предыдущего меню. Дополнительные поля **Action** и **Select Rule**, означают, что можно сконфигурировать правила в этом экране. Символ [?] в поле **Set Name** означает, что это обязательное поле и необходимо ввести название для этого набора.

```
                    Menu 15.1.1 - Address Mapping Rules


   Set Name= NAT_SET


  Idx  Local Start IP   Local End IP     Global Start IP  Global End IP
Type
  ---  ---------------  ---------------  ---------------  ---------------  -
-----
   1.
   2
   3.
   4.
```

Рис. 30-6 Меню 15.1.1 - Первый набор

Если поле Set Name **не заполнено, весь набор будет удален.**

Type, Local и Global Start/End IPs конфигурируются в Меню 15.1.1.1 (рассматривается ниже), а значения отображаются здесь.

Упорядочение правил

Упорядочение правил является важным моментом, так как Prestige применяет правила в порядке их расположения. Если правило соответствует текущему пакету, Prestige предпринимает соответствующее действие, а остальные правила игнорируются. Если есть несколько пустых правил до сконфигурированного нового правила, сконфигурированное правило будет поднято на это число пустых правил. Напр., если уже сконфигурированы правила с 1 по 6 в текущем наборе и конфигурируется правило номер 9. В сводном экране наборов, новое правило будет 7, а не 9.

Поэтому, если удалить правило 4, правила с 5 по 7 поднимутся на 1 строку, таким образом старое правило 5 станет правилом 4, старое правило 6 станет правилом 5, а старое правило 7 станет правилом 6.

Табл. 30-3 Меню 15.1.1 - Первый набор

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Set Name (Название набора)	Введите название для данного набора правил. Это обязательное поле. Если это поле не заполнено, весь набор будет удален.	NAT_SET
Action (Действие)	По умолчанию - **Edit**. **Edit,** означает, что нужно редактировать выбранное правило (см. следующее поле). **Insert Before**, обозначает, что необходимо вставить правило до выбранного правила. Правила после выбранного правила будут понижены на одно правило. **Delete,** означает удаление выбранного правила, а затем все правила после выбранного правила будут повышены на одно правило. **None** отключает пункт **Select Rule**.	**Edit**
Select Rule (Выбор правила)	При выборе **Edit**, **Insert Before** или **Delete** в предыдущем поле, курсор перемещается к этому полю для выбора правила, которое применяется в рассматриваемом действии.	1

Необходимо нажать клавишу [ENTER] **в нижней части экрана для сохранения всего набора. Если Вы производите какие-либо изменения в наборе, включая удаление правила, необходимо нажать эту клавишу снова. Никакие изменения в наборе не вступят в силу, если не выполнить это действие.**

Выберите **Edit** в поле **Action**, а затем выберите правило, появится следующее меню, **Меню 15.1.1.1 - Address Mapping Rule (Правило преобразования адресов),** в котором можно отредактировать отдельное правило и сконфигурировать **Type**, **Local** и **Global Start/End IPs**.

Конечный IP-адрес должен быть численно больше, чем соответствующий начальный IP-адрес.

```
                Menu 15.1.1.1 Address Mapping Rule

            Type= One-to-One

            Local IP:
              Start=
              End  = N/A

            Global IP:
              Start
```

Рис. 30-7 Меню 15.1.1.1 - Редактирование/конфигурирование отдельного правила в наборе

В следующей таблице представлено описание полей данного меню.

Табл. 30-4 Меню 15.1.1.1 - Редактирование/конфигурирование отдельного правила в наборе

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Type (Тип)	Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для выбора из пяти типов. Типы отображения рассматриваются в главе по *экранным меню NAT Web-конфигуратора*. **Server** позволяет установить множество серверов различных типов позади NAT для данной машины. Для примера см. *раздел 30.5.3*.	**One-to-One**
Local IP (Локальный IP-адрес)	Для сервера не доступны (**N/A)** только поля локального IP-адреса; поля глобального IP-адреса для **Server** ДОЛЖНЫ быть установлены.	
Start (Начальный)	Начальный локальный IP-адрес (ILA).	0.0.0.0

Табл. 30-4 Меню 15.1.1.1 - Редактирование/конфигурирование отдельного правила в наборе

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
End (Конечный)	Конечный локальный IP-адрес (ILA). Если правило соответствует всем локальным IP-адресам, тогда начальный IP соответствует - 0.0.0.0, а конечный IP - 255.255.255.255. Это поле не доступно (**N/A)** для типов One-to-One (Один-к-одному) и Server (Сервер).	N/A
Global IP (Глобальный IP-адрес)		
Start (Начальный)	Начальный внутренний глобальный IP-адрес (IGA). Если имеется динамический IP-адрес, введите 0.0.0.0 в качестве **Global IP Start**. Следует учитывать, что **Global IP Start** может быть установлен как - 0.0.0.0 только в том случае, если типами являются **Many-to-One** или **Server**.	0.0.0.0
End (Конечный)	Конечный внутренний глобальный IP-адрес (IGA). Это поле не доступно (**N/A)** для типов **One-to-One (Один-к-одному)**, **Many-to-One (Много-к-одному)** и **Server (Сервер)**.	N/A
Server Mapping Set (Набор преобразования серверов)	Поле доступно только, когда **Type** установлено на **Server**. Введите число от 1 до 10 для выбора набора серверов в Меню 15.2.	
При завершении работы в Меню при появлении сообщения “Press ENTER to confirm or ESC to cancel” нажмите клавишу [ENTER] для сохранения конфигурации или нажмите клавишу [ESC] для отмены и возврата к предыдущей экранной форме.		

30.4 Конфигурирование сервера за NAT

Для конфигурирования сервера за NAT нужно выполнить следующие действия:

Step 7. Введите 15 в Главном меню для перехода в Меню **15 - NAT Setup (Настройка NAT) .**

Step 8. Введите 2 для отображения Меню **15.2 - NAT Server Sets (Наборы серверов NAT)**, как показано 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 - Настройка сервера NAT

Step 9. Введите 1 в Главном меню для перехода в **Меню 15.2.1- NAT Server Setup (Настройка сервера NAT)**, как показано ниже.

```
                        Menu 15.2 - NAT Server Setup


              Rule   Start Port No.   End Port No.   IP Address
             ------------------------------------------------
-
                1.    Default          Default        0.0.0.0
                2.      21               21
192.168.1.33
                3.      0                0            0.0.0.0
                4.      0                0            0.0.0.0
```

Рис. 30-9 Меню 15.2.1 - Настройка сервера NAT

Step 10. Введите номер порта в неиспользуемое поле **Start Port No**. Для пересылки только одного порта снова введите номер порта в поле **End Port No**. Для установления диапазона портов введите последний порт, подлежащий пересылке в поле **End Port No**.

Step 11. Введите внутренний IP-адрес сервера в поле **IP Address**. На следующем рисунке представлен компьютер, выступающий в качестве сервера FTP, Telnet и SMTP (порты 21, 23 и 25) при 192.168.1.33.

Step 12. Нажмите клавишу [ENTER] при появлении сообщения “Press ENTER to confirm …” для сохранения конфигурации после определения всех серверов, или в любой момент нажмите клавишу [ESC] для отмены.

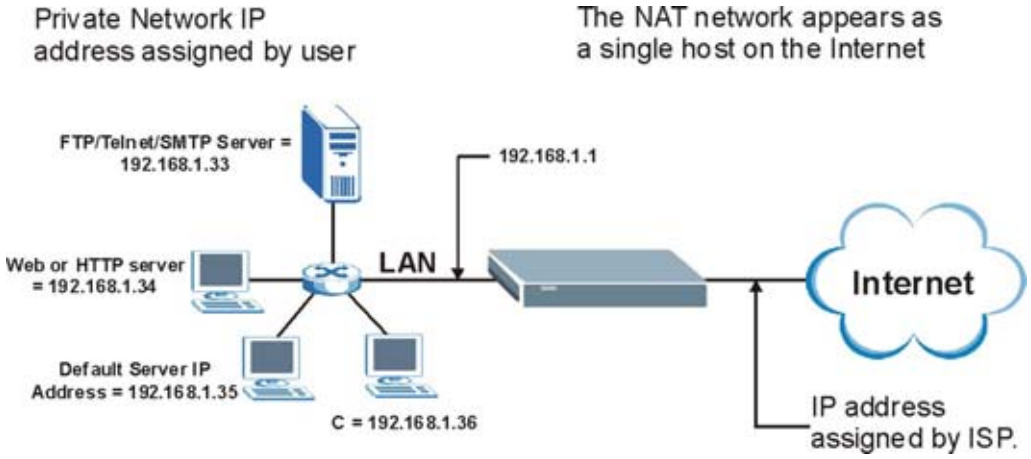


Рис. 30-10 Пример множества серверов за NAT

30.5 Примеры основного использования NAT

Далее представлено несколько примеров конфигурирования NAT.

30.5.1 Пример 1: Только для доступа в Интернет

В следующем примере, описывающем доступ в Интернет, необходимо только одно правило, где все внутренние локальные адреса (ILA) преобразовываются в один динамический внутренний глобальный адрес (IGA), назначенный Интернет-провайдером.

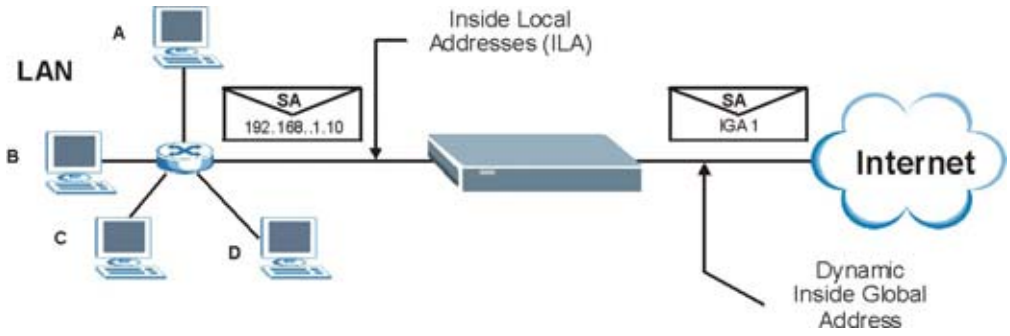


Рис. 30-11 Пример 1 NAT

```
                Menu 4 - Internet Access Setup


        ISP's Name= MyIsp
        Encapsulation= RFC 1483
        Multiplexing= LLC-based
        VPI #= 8
        VCI #= 35
        ATM QoS Type= UBR
          Peak Cell Rate (PCR)= 0
          Sustain Cell Rate (SCR)= 0
```

Рис. 30-12 Меню 4 - Пример доступа в Интернет и NAT

В Меню 4 выберите параметр **SUA Only** в поле **Network Address Translation**. Это отображение Many-to-One, рассматриваемое в *разделе 30.5*. Параметр **SUA Only**, используемый только для чтения

из поля **Network Address Translation** в Меню 4 и 11.3 специально заранее сконфигурирован для того, чтобы разобрать этот случай.

30.5.2 Пример 2: Доступ в Интернет с внутренним сервером

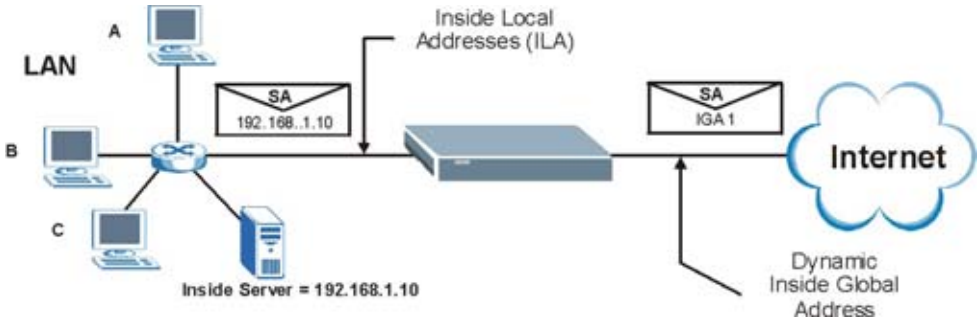


Рис. 30-13 Пример 2 NAT

В этом случае, методика аналогична вышеописанной (используйте удобный, заранее сконфигурированный набор **SUA Only**), перейдите в Меню 15.2 для установки внутреннего сервера за 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
```

Рис. 30-14 Меню 15.2.1 - Установка внутреннего сервера

30.5.3 Пример 3: Множество общедоступных IP-адресов с внутренними серверами

В данном примере имеется 3 внутренних глобальных адреса (IGA), назначенных Интернет-провайдером. Существует много отделов, но два имеют собственные серверы FTP. Все отделы имеют один и тот же маршрутизатор. В примере один IGA резервируется для каждого отдела с сервером FTP и все отделы используют оставшиеся IGA. Преобразуйте серверы FTP в первые два IGA, а остальной трафик LAN в оставшийся IGA. Преобразуйте третий IGA во внутренний Web-сервер и почтовый сервер. Необходимо сконфигурировать четыре правила: два - в двух направлениях и два - в одном направлении, следующим образом.

Rule 1. Преобразуйте первый IGA в первый внутренний сервер FTP для трафика FTP в обоих направлениях отображение (**1 : 1**, представляющее как локальные, так и глобальные IP-адреса).

Rule 2. Преобразуйте второй IGA во второй внутренний сервер FTP для трафика FTP в обоих направлениях отображение (**1 : 1**, представляющее как локальные, так и глобальные IP-адреса).

Rule 3. Преобразуйте остальной исходящий трафик LAN в IGA3 отображение (**Many : 1**).

Rule 4. Преобразуйте также третий IGA в Web-сервер и почтовый сервер в LAN. Тип **Server** позволяет установить множество серверов различных типов, вдобавок к другим компьютерам за NAT в LAN.

Ситуация, указанная в примере приблизительно выглядит следующим образом:

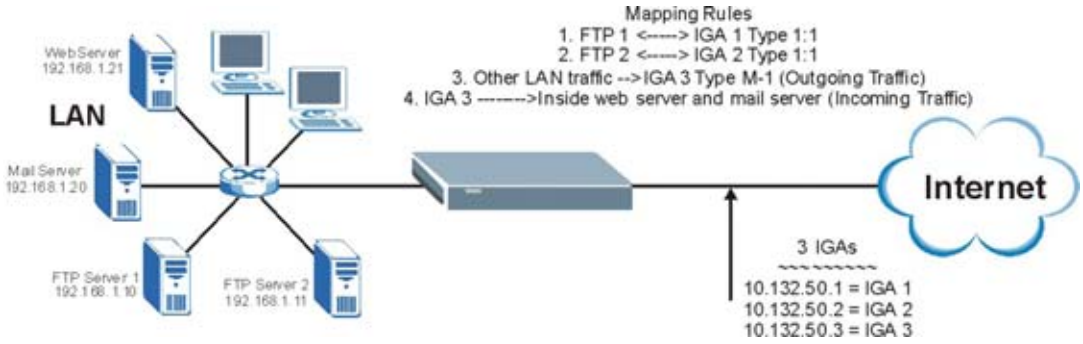


Рис. 30-15 Пример 3 NAT

Step 1. В этом случае необходимо сконфигурировать набор преобразования адресов 1 в **Меню 15.1 - Address Mapping Sets (Наборы преобразования адресов).** Поэтому нужно выбрать

опцию **Full Feature** в поле **Network Address Translation** (в Меню 4 или Меню 11.3) на *Рис. 30-16*.

Step 2. Затем ввести 15 в Главном меню.

Step 3. Ввести 1 для конфигурирования наборов преобразования адресов.

Step 4. Ввести 1 для того, чтобы начать конфигурирование этого нового набора. Ввести Set Name (Название набора), выбрать **Edit Action**, а затем ввести 1 в поле **Select Rule**. Нажать клавишу [ENTER] для подтверждения.

Step 5. Выбрать **Type** в качестве **One-to-One** (прямое отображение для пакетов пересылаемых обоими способами), и ввести локальный **Start IP** как 192.168.1.10 (IP-адрес сервера 1 FTP), глобальный **Start IP** как 10.132.50.1 (первый IGA). (См. *Рис. 30-17).*

Step 6. Повторите предыдущие шаги для правил 2 - 4, как описано выше.

Step 7. При завершении, Меню 15.1.1 должно выглядеть как показано на *Рис. 30-18*.

```
         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
```

Рис. 30-16 Пример 3: Меню 11.3

На следующих рисунках представлено конфигурирование первого правила

```
                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
```

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
```

Рис. 30-18 Пример 3: Конечное Меню 15.1.1

Теперь сконфигурируйте преобразования IGA3 в Web-сервер и почтовый сервер в LAN.

Step 8. Введите 15 в Главном меню.

Step 9. Введите 2 в **Меню 15 - NAT Setup (Настройка NAT)**.

Step 10. Введите 1 в **Меню 15.2 - NAT Server Sets (Наборы серверов NAT)** для перехода в следующее меню. Сконфигурируйте его как показано на рисунке.

```
                        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
```

Пример 3: Меню 15.2.1

30.5.4 Пример 4: Недружественные NAT прикладные программы

Некоторые приложения не поддерживают преобразование NAT, использующее TCP или преобразование адреса порта UDP. В этом случае, лучше всего использовать отображение **Many-to-Many No Overload** , так как номера порта не меняются для типов отображения NAT **Many-to-Many No Overload** (и **One-to-One**). Это иллюстрирует следующий рисунок.

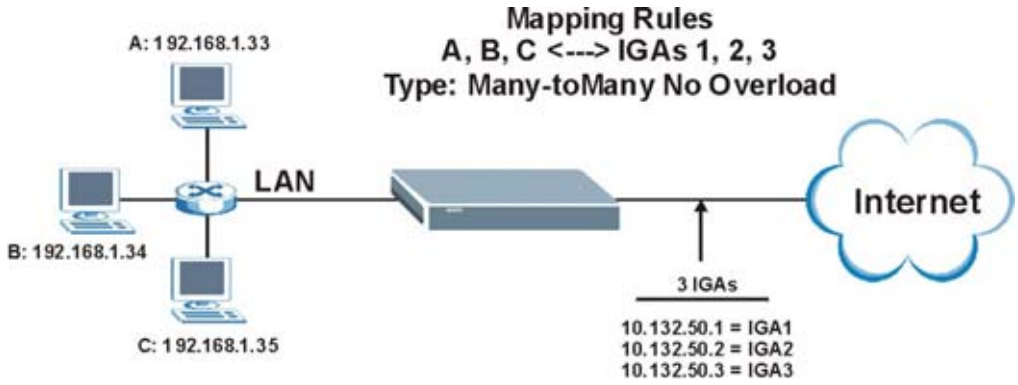


Рис. 30-19 Пример 4 NAT

Некоторые приложения, такие как игровые программы, являются недружественными для NAT, так как они встраивают адресную информацию в поток данных. Эти приложения не будут работать через NAT, даже, если используются типы отображения One-to-One **и** Many-to-Many No Overload**.**

Следуйте шагам, описанным в примере 3, для конфигурирования этих двух меню.

```
                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
```

Рис. 30-20 Пример 4: Меню 15.1.1.1 - Правило преобразования адресов

После того, как сконфигурировано правило, необходимо проверить настройки 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.
  -
```

Рис. 30-21 Пример 4: Меню 15.1.1 - Правила преобразования адресов

Раздел 31
Включение межсетевого экрана

В этой главе описывается как начать работать с межсетевым экраном серии Prestige.

31.1 Дистанционное управление и межсетевой экран

Когда Меню 24.11 SMT конфигурируется для управления (см. главу *Дистанционное управление*) и межсетевой экран включается:

- Межсетевой экран блокирует дистанционное управление из WAN, если не сконфигурировано правило межсетевого экрана, разрешающее управление.
- Межсетевой экран допускает дистанционное управление из LAN.

31.2 Методы доступа

Web-конфигуратор, несомненно, является наиболее полным средством конфигурирования межсетевого экрана, которое может предложить Prestige. По этой причине, рекомендуется, чтобы при конфигурировании межсетевого экрана использовался Web-конфигуратор. См. следующие главы для дополнительных инструкций. Экранные формы меню SMT позволяют активировать межсетевой экран и просмотреть журнальные регистрации межсетевого экрана.

31.3 Включение межсетевого экрана

В Главном меню введите 21 для перехода в **Меню 21 - Filter Set and Firewall Configuration (Набор фильтров и конфигурирование межсетевого экрана)** для отображения экрана, представленного ниже**.**

Введите 2 в этом меню для вызова следующего экрана. Нажмите клавишу пробела [SPACE BAR], а затем клавишу [ENTER] для выбора **Yes** в поле **Active,** чтобы активировать межсетевой экран. Межсетевой экран может применяться для защиты от атак типа *Отказ от обслуживания* (DoS). Дополнительные правила могут быть сконфигурированы при помощи Web-конфигуратора.

```
                    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
```

Рис. 31-1 Меню 21.2 - Настройка межсетевого экрана

Для конфигурирования правил межсетевого экрана используйте Web-конфигуратор или интерпретатор команд.

Глава IX:

Системная консоль (SMT) - Дополнительные возможности управления

В данном разделе описывается порядок установки параметров фильтрации, SNMP, защитных функций системы, системной информации и диагностики, сопровождение микропрограммного обеспечения и файла конфигурации, сопровождение системы, дистанционное управление, маршрутизация на базе стратегии IP (IPPR), составление расписания вызовов и внутренний генератор таблицы системных параметров, предназначенные для одновременного конфигурирования нескольких устройств Prestiges.

Общая ознакомительная информация о функциональных возможностях, параметры конфигурации которых можно установить при помощи web-конфигуратора и системной консоли, изложена в разделах настоящего руководства пользователя, посвященных web-конфигуратору.

Раздел 32
Конфигурирование фильтров

В данной главе описываются порядок создания и установки фильтров.

32.1 Что такое фильтрация

Фильтры в устройстве Prestige используются для того, чтобы разрешать или запрещать пересылку пакета данных и/или инициацию телефонного вызова. Существуют два типа фильтров: фильтры данных и фильтры телефонных вызовов. Фильтры подразделяются на фильтры устройств и фильтры протоколов, о которых речь пойдет позже.

Фильтр данных выводит данные на экран для того, чтобы принять решение о разрешении или запрещении передачи этого пакета. Фильтры данных подразделяются на фильтры входящих данных и фильтры исходящих данных, в зависимости от направления движения пакета данных по отношению к порту. Фильтры данных могут устанавливаться как на стороне глобальной вычислительной сети (WAN), так и на стороне Ethernet. Фильтры вызовов используются для принятия решения о разрешении или запрещении пакету данных инициировать вызов.

Пакеты исходящих данных должны сначала пройти через фильтры данных, и только потом — через фильтры вызовов. Фильтры вызовов подразделяются на две группы: встроенные фильтры вызовов и определяемые пользователем. Устройство Prestige оснащено встроенными фильтрами вызовов, предназначенными для того, чтобы не допускать инициацию вызовов административными пакетами, например, RIP пакетами. Эти фильтры всегда находятся во включенном состоянии и недоступны для пользователя. Prestige сначала задействует встроенные фильтры, а затем, если таковые используются, определяемые пользователем фильтры вызовов так, как показано ниже.

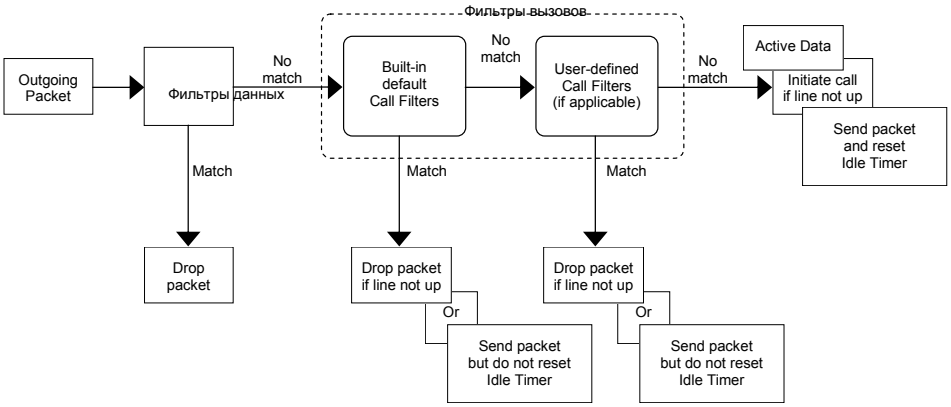


Рис. 32-1 Процесс фильтрации исходящих пакетов

В меню 21 имеются два набора правил фильтров, установленных на заводе-изготовителе, предназначенных для того, чтобы не допускать инициацию вызовов трафиком NetBIOS. На рисунках ниже представлен краткий обзор этих правил фильтров.

На рисунке ниже изображена логическая схема реализации правила фильтра.

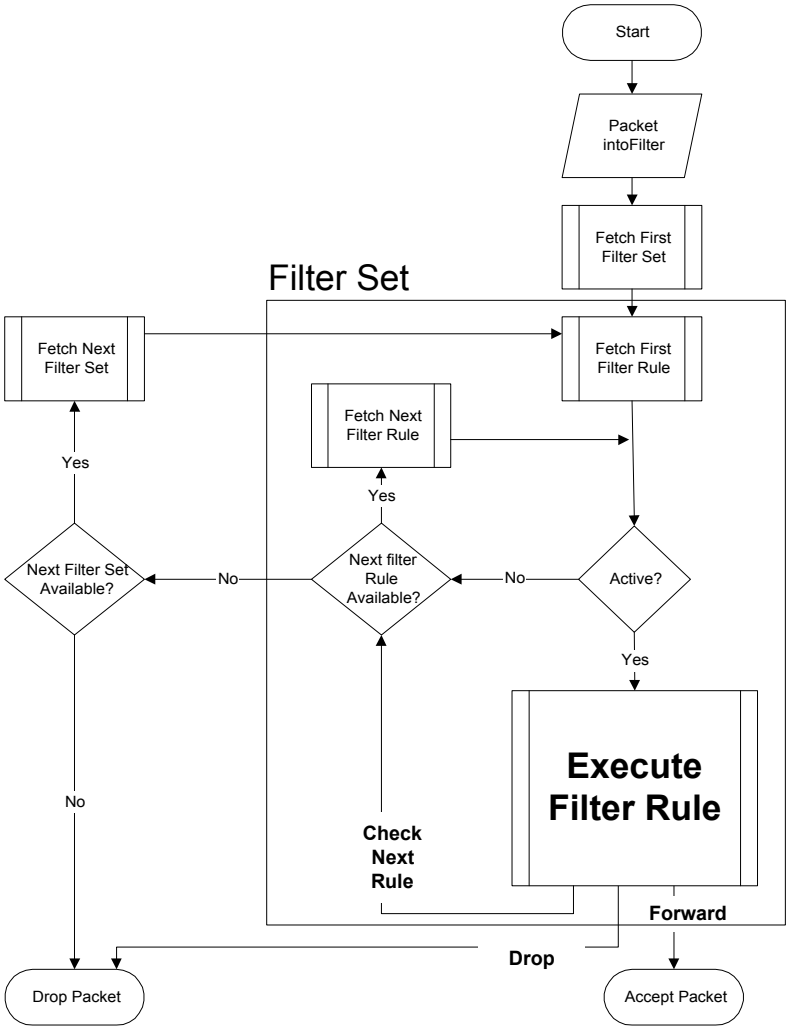


Рис. 32-2 Процесс реализации правила фильтра

На каждом порту можно устанавливать до четырех наборов фильтров, предназначенных для блокирования пакетов различных типов. Каждый набор фильтров может содержать 6 правил, поэтому что на каждый отдельный порт можно установить до 24 активных правил.

Для входящих пакетов Prestige использует только фильтры данных. Обработка пакетов осуществляется в зависимости от того, найдено соответствие или нет. В следующем разделе описывается порядок конфигурирования наборов фильтров.

Структура фильтров устройства Prestige

Набор фильтров состоит из одного или нескольких правил фильтров. Обычно, схожие по значению правила объединяются в группы, например: все правила для NetBIOS объединяются в отдельную группу, которой присваивается идентифицирующее имя. В системе могут быть сконфигурированы не более 72 правил фильтров: 12 наборов фильтров по 6 правил в каждом.

32.2 Конфигурирование набора фильтров для Prestige

Для того, чтобы сконфигурировать набор фильтров, выполните нижеперечисленные действия.

Step 1. Откройте **Меню 21 – Filter and Firewall Setup (Настройка фильтра и межсетевого экрана).** Для этого, в главном меню наберите цифру 21.

Step 2. Откройте окно **Menu 21.1 – Filter Set Configuration (Настройка набора фильтров)**, см. ниже. Для этого в открывшемся окне наберите цифру 1.

```
                  Меню 21.1 – Filter Set Configuration

   Filter                                Filter
   Set #        Comments                 Set #        Comments
   ------  -----------------             ------  --------------
---
     1      _______________                7
_______________
     2      NetBIOS_WAN                    8
_______________
     3      NetBIOS_LAN                    9
```

Рис. 32-3 Меню 21.1. Настройка набора фильтров

Step 3. Наберите номер набора фильтров для настройки (номер от 1 до 12) и нажмите клавишу [ENTER].

Step 4. В поле **Edit Comments** (**Редактирование комментариев)** наберите идентифицирующее имя или комментарий и нажмите клавишу [ENTER].

Step 5. Нажмите кнопку [ENTER] в сообщении “Press ENTER to confirm…(Нажмите Enter для подтверждения)”. При этом откроется **Меню 21.1.1 – Filter Rules Summary (Сводка правил фильтров)** (если Вы в меню 21.1 выбрали набор фильтров 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
```

Рис. 32-4 Сводка правил фильтров NetBIOS_WAN

```
                        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
```

Рис. 32-5 Сводка правил 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
```

Рис. 32-6 Сводка правил фильтров IGMP (Протокола управления группами сети Интернет)

32.3 Меню сводки правил фильтров

В таблице ниже приводятся краткие описания сокращений, используемых в меню 21.1.1 и 21.1.2.

Табл. 32-1 Сокращения, используемые в меню сводки правил фильтров

ПОЛЕ	ОПИСАНИЕ
#	Номер правила фильтра: от 1 до 6.
A	Активно: Значение “Y” означает, что правило активно. Значение “N” означает, что правило не активно.
Type (Тип)	Тип правила фильтра: Значение "GEN" обозначает общее правило, "IP" — правило для TCP/IP.
Filter Rules (Правила фильтра)	В этом поле отображаются следующие параметры.
M	More (Больше). "Y" означает, что имеется продолжение списка правил, подлежащих проверке, которые образуют цепочку правил, связанных с данным правилом. Действие не может быть предпринято до тех пор, пока не завершится проверка всей цепочки правил. "N" означает, что больше нет правил для проверки. Вы можете указать действие, которое следует предпринять, например: переслать пакет, сбросить пакет или проверить следующее правило. Что касается последнего действия, то оно относится к следующему правилу, не зависимому от того, которое было проверено ранее.

Табл. 32-1 Сокращения, используемые в меню сводки правил фильтров

ПОЛЕ	ОПИСАНИЕ
m	Действие при соответствии. "F" означает, что пакет должен быть переслан немедленно, а проверку оставшихся правил следует пропустить. "D" означает, что пакет должен быть сброшен. "N" означает, что следующее правило необходимо проверить.
n	Действие при несоответствии. "F" означает, что пакет должен быть переслан немедленно, а проверку оставшихся правил следует пропустить. "D" означает, что пакет должен быть сброшен. “N" означает, что следующее правило необходимо проверить.

Ниже приводится список сокращений правил фильтров, зависимых от протокола:

Табл. 32-2 Используемые сокращения правил

ТИП ФИЛЬТРА	ОПИСАНИЕ
IP	
Pr	Протокол
SA	Адрес источника
SP	Номер порта источника
DA	Адрес назначения
DP	Номер порта назначения
GEN	
Off	Смещение
Len	Длина

32.4 Конфигурирование правила фильтра

Для конфигурирования правила фильтра, в **Меню 21.1.x – Filter Rules Summary (Сводка правил фильтров)** введите номер правила фильтра и нажмите клавишу [ENTER].

Существуют два типа правил фильтров: **TCP/IP** и **Generic (Общий)**. Параметры каждого правила зависят от типа правил, к которому оно относится. В поле **Filter Type (Тип фильтра)** при помощи

клавиши пробела выберите тип создаваемого правила и нажмите клавишу [ENTER]. При этом откроется соответствующее меню.

Для того. чтобы процесс фильтрации протекал быстрее, все правила в наборе фильтров должны быть одного класса, например: фильтры протоколов или общие фильтры. Класс набора фильтров определяется первым правилом, которое Вы создаете. При установке наборов фильтров на порт, отделяйте поля меню для наборов фильтров протоколов от наборов фильтров устройств. Если Вы включите набор фильтров протокола в поле фильтров устройств или наоборот, то Prestige выдаст предупреждение об ошибке и не позволит сохранить такие параметры.

32.4.1 Правило фильтра TCP/IP

В данном разделе описывается порядок конфигурирования правила фильтра TCP/IP. Правила TCP/IP позволяют установить правило в полях протокола IP и в протоколах более высокого уровня, например в заголовках UDP и TCP.

Для конфигурирования правил TCP/IP, в поле **Filter Type (Тип фильтра)** выберите правило фильтра TCP/IP и нажмите клавишу [ENTER]. При этом откроется **Меню 21.1.x.1 – TCP/IP Filter Rule (Правило фильтра TCP/IP)**, см. 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=
```

Рис. 32-7 Меню 21.1.x.1 Правило фильтра TCP/IP

В таблице ниже даны описания параметров конфигурации правила фильтра TCP/IP.

Табл. 32-3 Меню 21.1.x.1 Правило фильтра TCP/IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Filter # (Номер фильтра)	В этом поле отображается набор фильтров и координаты правила фильтра. Например: 2, 3 обозначает — второй набор фильтров и третье правило фильтра данного набора.	1,1
Filter Type (Тип фильтра)	При помощи клавиши [ПРОБЕЛ] выберите правило и нажмите клавишу [ENTER]. Для каждого типа правил отображаются параметры, отличающиеся от параметров других типов. Опциями являются: **TCP/IP Filter Rule** (**Правило фильтра TCP/IP)** и **Generic Filter Rule** (**Правило общего фильтра)**.	**TCP/IP Filter Rule** (**Правило фильтра TCP/IP)**
Active (Активно)	Для того, чтобы активировать правило фильтра, выберите опцию **Yes (Да),** а для того, чтобы отключить — **No (Нет)**.	**No (Нет)** (по умолчанию)
IP Protocol (Протокол IP)	В этом поле отображается протокол верхнего уровня, например: TCP, обозначенный цифрой 6, UDP — цифрой 17, а ICMP — цифрой 1. Цифровое значение должно быть в диапазоне от 0 до 255. Значение 0 означает ЛЮБОЙ протокол.	от 0 до 255
IP Source Route (Маршрут источника IP)	Маршрут источника IP является не обязательным заголовком, предписывающим маршрут, по которому пакет IP передается от источника к адресату. Если выбирается опция **Yes (Да)**, то это правило применяется к любому пакету, имеющему маршрут источника IP. Однако большинство IP пакетов не имеют маршрута источника.	**No (Нет)** (по умолчанию)
Destination (Пункт назначения):		

Табл. 32-3 Меню 21.1.x.1 Правило фильтра TCP/IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
IP Addr (IP-адрес)	Введите в этом поле IP-адрес пункта назначения пакета, на который распространяется действие фильтра. Если в это поле вводится значение 0.0.0.0., то оно игнорируется.	IP Address (IP-адрес)
IP Mask (IP-маска)	Введите в это поле IP-маску для поля: Destination IP Addr (IP-адрес пункта назначения).	IP-маска
port#	Введите в этом поле порт назначения пакетов, на которые распространяется действие фильтров. Значения устанавливаются в диапазоне от 0 до 65535. При вводе значения 0, поле игнорируется.	от 0 до 65535
Port # Comp (Сравнивание номеров портов)	Выберите способ сравнения портов назначения, указанных в пакетах и в поле **Destination (Пункт назначения)**:**Port #** (**Номер порта).** Опциями являются: **None (Никакой)**, **Less (Меньше)**, **Greater (Больше)**, **Equal (Равно)** или **Not Equal (Не равно)**.	**None (Никакой)**
Source (Источник):		
IP Addr (IP-адрес)	Введите в этом поле IP-адрес источника пакета, на который распространяется действие фильтра. Поле со значением 0.0.0.0 игнорируется.	IP Address (IP-адрес)
IP Mask (IP-маска)	Введите в это поле IP-маску для поля **Source IP Addr:** (**IP-адрес источника)**.	IP-маска
port#	Введите в этом поле порт источника пакета, на который распространяется действие фильтра. Значения в этом поле устанавливаются в диапазоне от 0 до 65535. Поле со значением 0 игнорируется.	от 0 до 65535
Port # Comp (Сравнивание номеров портов)	Выберите способ сравнения портов источников, указанных в пакетах и в поле **Source** (**Источник):Port # (Номер порта)**. Опциями являются: **None (Никакой)**, **Less (Меньше)**, **Greater (Больше)**, **Equal (Равно)** или **Not Equal (Не равно).**	**Никакой**
TCP Estab	Это поле используется только в случае, когда значение поля IP Protocol (Протокол IP) равно 6, TCP. Если выбрана опция **Yes (Да)**, то это правило распространяется на пакеты, которые предназначены для установки TCP соединения(ий) (SYN=1 и ACK=0). В остальных случаях это правило игнорируется.	**No (Нет)** (по умолчанию)

Табл. 32-3 Меню 21.1.x.1 Правило фильтра TCP/IP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
More (Больше).	Если в поле установлено значение **Yes (Да)**, то пакет, соответствующий данным правилам, передается другому правилу фильтра прежде, чем выполняется какое-либо действие, либо пакет удаляется в соответствии с полями действия. Если в поле **More (Больше)** установлено значение **Yes (да)**, то в полях **Action Matched (Действие при соответствии)** и **Action Not Matched (Действие при несоответствии)** должно быть установлено значение N/A (не доступно).	**No (Нет)** (по умолчанию)
Log (Журнальная регистрация)	Выберите функцию журнальной регистрации из предложенных: **None (Никакая)** – Регистрации пакетов в журнале не происходит. **Action Matched (Действие при соответствии)** – В журнале регистрируются только те пакеты, которые соответствуют параметрам правила. **Action Not Matched (Действие при несоответствии)** – В журнале регистрируются только те пакеты, которые не соответствуют параметрам правила. **Both (Все)** – В журнале регистрируются все пакеты.	**None** (**Никакой)**
Action Matched (Действие при соответствии)	Выберите действие, выполняемое при соответствии пакета правилу. Опциями являются: **Check Next Rule (Проверить следующее правило)**, **Forward (Переслать)** или **Drop (Сбросить)**.	**Check Next Rule** (**Проверить следующее правило)** (по умолчанию)
Action Not Matched (Действие при несоответствии)	Выберите действие, выполняемое при несоответствии пакета правилу. Опциями являются: **Check Next Rule (Проверить следующее правило)**, **Forward (Переслать)** или **Drop (Сбросить)**.	**Check Next Rule** (**Проверить следующее правило)** (по умолчанию)
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.		

На рисунке ниже представлена логическая схема работы фильтра IP.

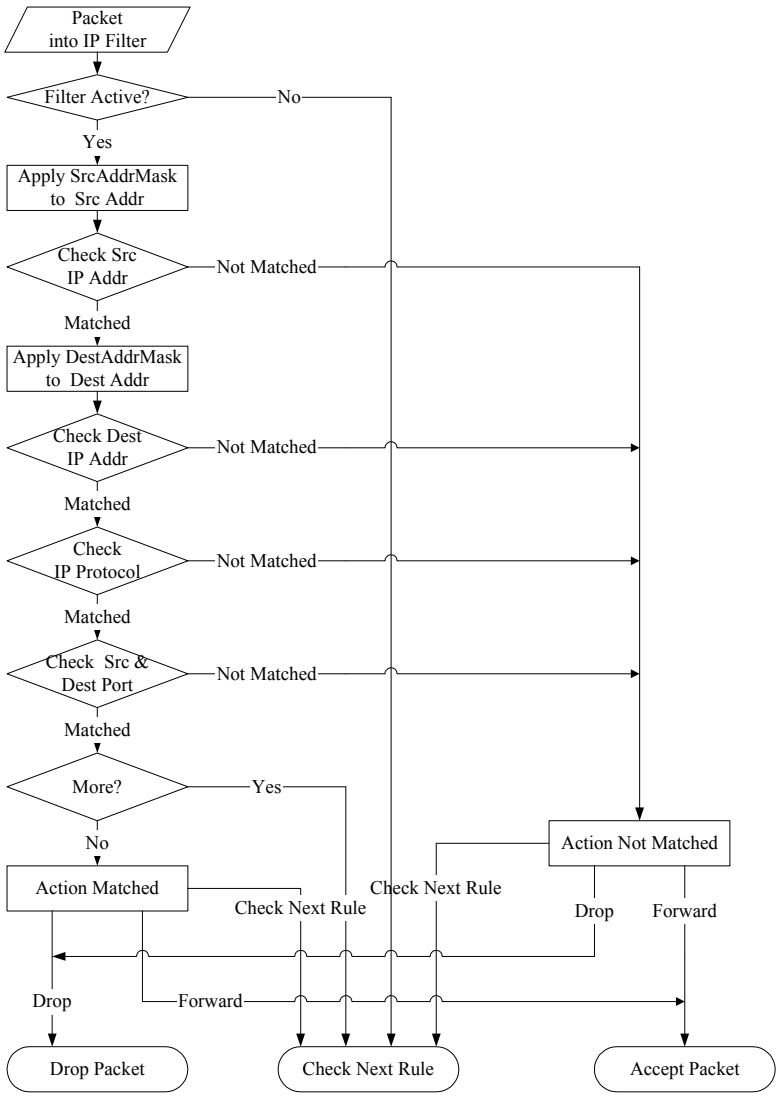


Рисунок 32-8 Функционирование фильтра IP

32.4.2 Правило общего фильтра

В данном разделе описывается, как сконфигурировать правило общего фильтра. Общие правила предназначены для того, чтобы дать возможность пользователю фильтровать пакеты, не относящиеся к IP. Обычно для фильтрования пакетов IP значительно проще использовать непосредственно правила IP.

При общих правилах, Prestige обрабатывает пакет не как паке IP, а как битовый поток. Вы указываете часть пакета, которую надлежит проверить по полям **Смещение** (**Offset)** (от 0) и **Длина** (**Length)**, и то и другое в байтах. Prestige использует Маску (поразрядное выполнение операции "И") для блока данных до того, как проводит сравнение полученного результата со Значением и определяет соответствие. Значения полей **Mask (Маска)** и **Value** (**Значение)** указываются в шестнадцатеричной форме. Следует иметь в виду, что для обозначения байта используются две шестнадцатеричные цифры. Поэтому, если длина равна 4, то значение в каждом поле будет состоять из 8 цифр, например, FFFFFFFF.

Для того, чтобы сконфигурировать общее правило, в меню 21 выберите пустой набор фильтров, например, 5. Затем в поле **Filter Type (Тип фильтра)** выберите **Правило общего фильтра** и нажмите клавишу [ENTER]. При этом откроется **Меню 21.1.5.1 – Правило общего фильтра (Generic Filter Rule)**, см. рисунок ниже.

```
Меню 21.1.5.1 - Generic Filter Rule


Filter #: 5,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
```

Рис. 32-9 Меню 21.1.5.1 Правило общего фильтра

В таблице ниже приводятся описания полей меню Правила общего фильтра.

Табл. 32-4 Меню 21.1.5.1 Правило общего фильтра

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Filter #(Номер фильтра)	В этом поле отображается набор фильтров и координаты правила фильтра. Например: 2, 3 обозначает — второй набор фильтров и третье правило фильтра данного набора.	5,1
Filter Type (Тип фильтра)	При помощи клавиши [ПРОБЕЛ] выберите тип правила и нажмите клавишу [ENTER]. Под каждым типом правил отображаются параметры, отличающиеся от параметров других типов. Опциями являются: **Generic Filter Rule** (**Правило общего фильтра)** и **TCP/IP Filter Rule** (**Правило фильтра TCP/IP**).	**Правило общего фильтра**
Active (Активно)	Для того, чтобы включить правило фильтра, выберите опцию **Yes (Да),** а для того, чтобы выключить — опцию **No (Нет)**.	**No (Нет)** (по умолчанию)
Offset (Смещение)	Наберите с клавиатуры начальный байт блока данных в пакете, который требуется сравнить. Значения в этом поле устанавливаются в диапазоне от 0 до 255.	0 (по умолчанию)
Length (Длина)	Наберите с клавиатуры счетчик байтов блока данных в пакете, который требуется сравнить. Значения в этом поле устанавливаются в диапазоне от 0 до 8.	0 (по умолчанию)
Mask (Маска)	Введите с клавиатуры маску (в шестнадцатеричной форме), используемую для блока данных до выполнения операции сравнения.	
Value (Значение)	Введите с клавиатуры значение (в шестнадцатеричной форме), используемое для сравнения с блоком данных.	
More (Больше).	Если в поле установлено значение **Yes (Да)**, то пакет, соответствующий параметрам фильтра, передается другому правилу фильтра прежде, чем выполняется действие, либо пакет удаляется, согласно значениям полей действия**.** Если в поле **More (Больше)** установлено значение **Yes (да)**, то в полях **Action Matched (Действие при соответствии)** и **Action Not Matched** (Действие при несоответствии) должно быть установлено значение N/A (не доступно)**.**	**No (Нет)** (по умолчанию)
Log (Журнальная регистрация)	Выберите функцию журнальной регистрации из предложенных: **None (Никакой)** – Регистрации пакетов в журнале не производится. **Action Matched (Действие при соответствии)** – В журнале регистрируются только пакеты, соответствующие параметрам правила. **Action Not Matched (Действие при несоответствии)** – В журнале	**None** (**Никакая**)

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
	регистрируются только те пакеты, которые не соответствуют параметрам правила. **Both (Все)** – В журнале регистрируются все пакеты.	
Action Matched (Действие при соответствии)	Выберите действие, выполняемое при соответствии пакета правилу. Опциями являются: **Check Next Rule (Проверить следующее правило)**, **Forward (Переслать)** или **Drop (Сбросить)**.	**Check Next Rule** (**Проверить следующее правило**) (по умолчанию)
Action Not Matched (Действие при несоответствии)	Выберите действие, выполняемое при несоответствии пакета правилу. Опциями являются: **Check Next Rule (Проверить следующее правило)**, **Forward (Переслать)** или **Drop (Сбросить)**.	**Check Next Rule** (**Проверить следующее правило**) (по умолчанию)
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.		

32.5 Типы фильтров и трансляция сетевых адресов (NAT)

Существуют два класса правил фильтров: правила общих фильтров для устройств (**Generic Filter** Device rules) и правила фильтра протоколов **(TCP/IP) (**Protocol Filter (**TCP/IP**)). Правила общих фильтров используются по отношению к необработанным данным, входящих/исходящих от локальной вычислительной сети (LAN) или глобальной вычислительной сети (WAN). Правила фильтра протоколов используются по отношению к IP-пакетам.

Когда функция NAT (Трансляция сетевых адресов) включена, то при каждом подключении IP-адрес и номер порта меняются, поэтому невозможно установить точный адрес и порт проводного соединения. Поэтому Prestige устанавливает фильтры протоколов на "родных" IP-адресах и номерах портов для исходящих пакетов до NAT, а для входящих пакетов — после NAT. С другой стороны, общие фильтры (или фильтры устройства) применяются по отношению к исходным пакетам, которые появляются в проводном соединении. Эти фильтры устанавливаются в точке, где Prestige получает или отправляет пакеты данных, например, в интерфейсе. В качестве интерфейса может выступать

порт Ethernet или любой другой порт, относящийся к аппаратному обеспечению. На рисунке ниже это представлено в графическом виде.

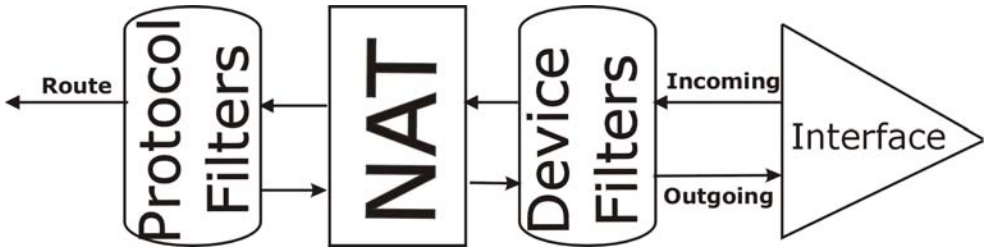


Рис.32-10 Наборы фильтров протоколов и устройств

32.6 Пример фильтра

Давайте рассмотрим пример фильтра, предназначенного для блокирования подключения внешних пользователей к устройству Prestige через сетевой теледоступ.

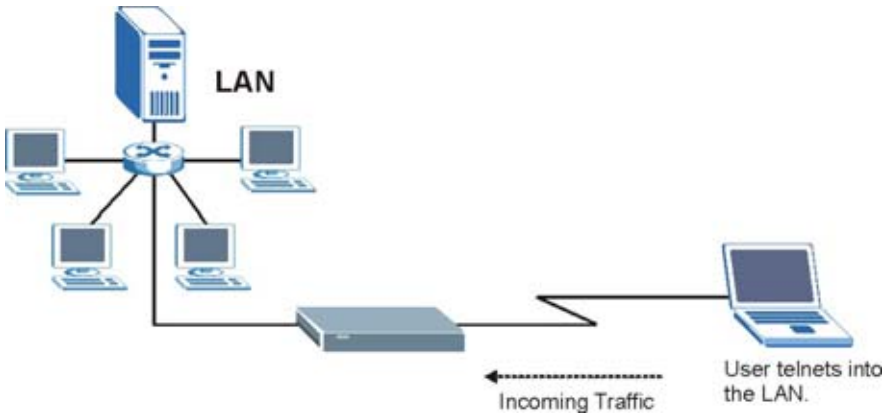


Рис.32-11 Пример фильтра Telnet

Step 1. Откройте **Меню 21.1 — Filter Set Configuration (Настройка наборов фильтров)**. Для этого, в меню 21 наберите цифру 1.

Step 2. Введите индекс набора фильтров, конфигурацию которого Вы намерены установить (в данном случае — номер 6).

Step 3. В поле **Edit Comments (Редактирование комментариев)** введите идентифицирующее имя или комментарий (например, TELNET_WAN) и нажмите клавишу [ENTER].

Step 4. При появлении сообщения "Press [ENTER] to confirm or [ESC] to cancel" нажмите клавишу [ENTER]. При этом откроется **Меню 21.1.6 — Filter Rules Summary (Сводка правил фильтров).**

Step 5. Для установки конфигурации первого правила фильтра, наберите цифру 1. Введите значения в пунктах меню так, как показано ниже.

При нажатии клавиши [ENTER] Вы подтверждаете правильность ввода значений и открываете следующее окно. Напоминаем, что в этом пакете имеется только одно правило фильтра.

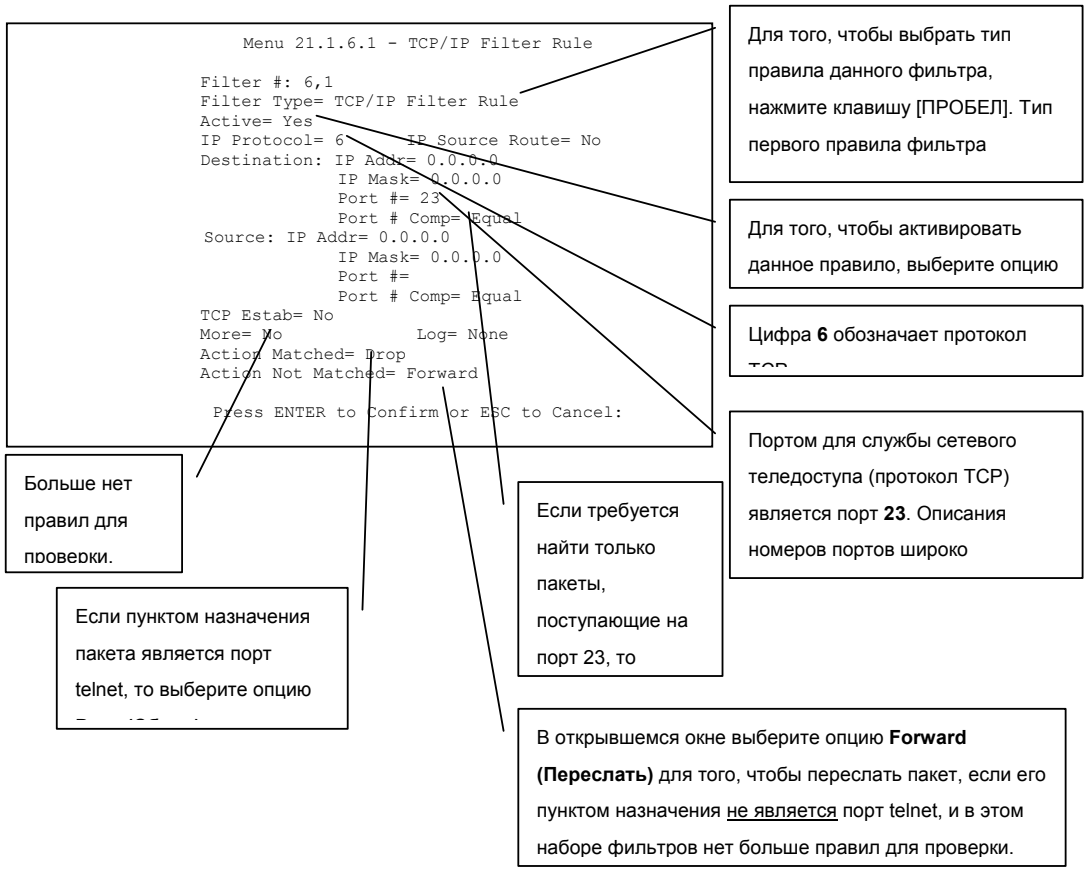


Рис. 32-12 Меню 21.1.6.1 Пример фильтра

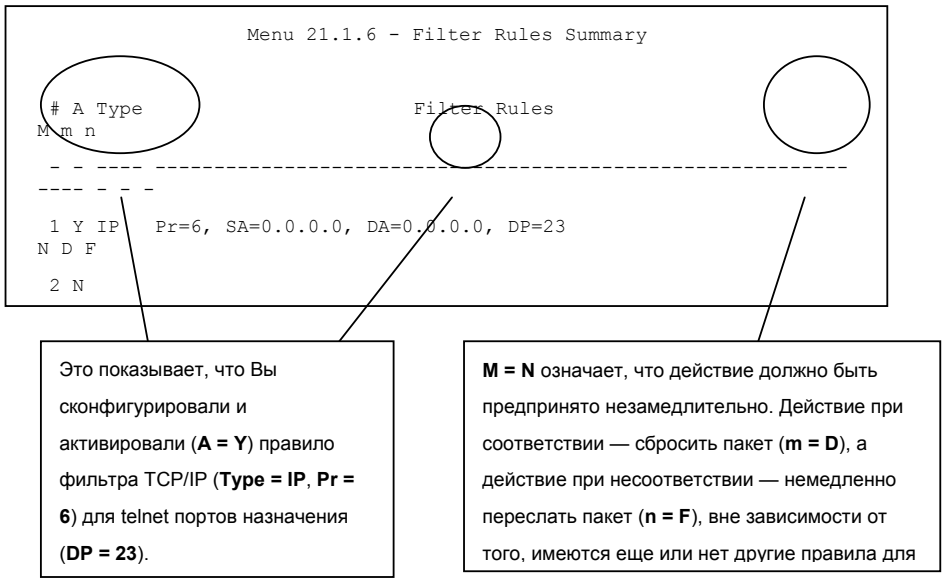


Рис.32-13 Меню 21.1.6.1 Пример сводки правил фильтров

После того, как Вы создали набор фильтров, Вы должны его применить.

Step 1. В главном меню наберите цифру 11. Откроется меню 11, в котором введите номер удаленного узла для редактирования его параметров.

Step 2. В поле **Edit Filter Sets (Редактирование наборов фильтров)** при помощи клавиши [ПРОБЕЛ] выберите опцию **Yes (Да)** и нажмите клавишу [ENTER].

Step 3. При этом откроется меню 11.5. Установите набор фильтров, созданный в качестве примера (например, набор фильтров номер 3), в этом меню так, как описано в следующем разделе.

32.7 Установка фильтров и заводских настроек по умолчанию

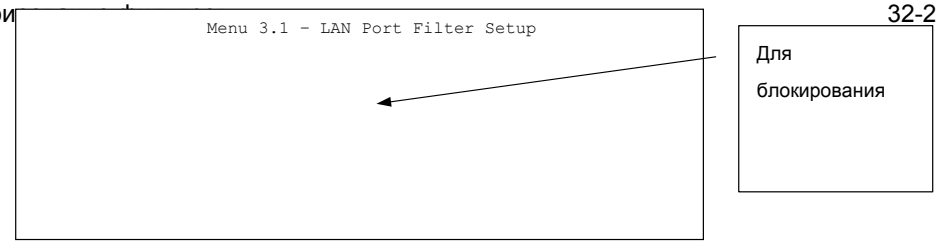
В данном разделе описываются области приложения фильтров после их создания. Наборы правил фильтров, установленные изготовителем по умолчанию и предназначенные для фильтрации трафика, были сконфигурированы в меню 21, но еще не применялись.

Табл.32-5 Таблица наборов фильтров

НАБОРЫ ФИЛЬТРОВ	ОПИСАНИЕ
Наборы входных фильтров:	Применение фильтров для входящего трафика. Допускается использование как правил фильтров для устройства, так и правил фильтров для протокола. Информация о фильтрах представлена выше, в данном разделе.
Наборы выходных фильтров:	Применение фильтров для исходящего трафика устройства Prestige. Допускается использование как правил фильтров для устройства, так и правил фильтров для протокола. Информация о типах фильтров представлена выше в данном разделе.
Наборы фильтров вызовов:	Применение фильтров для разрешения или запрещения пакетам инициировать телефонный вызов.

32.7.1 Трафик Ethernet

Обычно редко возникает необходимость в фильтрации трафика Ethernet, однако, данные наборы фильтров могут использоваться для блокирования определенных пакетов, для уменьшения объемов трафика и для защиты от несанкционированного доступа. Для того, чтобы установить фильтры, откройте меню 3.1 (см. ниже) и наберите номер(а) соответствующих набора(ов) фильтров. Вы можете выбрать не более четырех наборов фильтров из двенадцати. Выбор осуществляется посредством



ввода номеров фильтров, отделяемых запятыми, например: 3, 4, 6, 11. Набор фильтров, установленный изготовителем по умолчанию, NetBIOS_LAN, размещается в поле **protocol filters (фильтры протоколов)** пункта **Input Filter Sets (Наборы входных фильтров)** меню 3.1. Это сделано для того, чтобы локальные сообщения NetBIOS не могли инициировать вызовы на сервер DNS.

Рис. 32-14 Фильтрация трафика Ethernet

32.7.2 Фильтры для удаленных узлов

Откройте меню 11.5 (см. ниже) и введите номер(а) соответствующих набор(ов) фильтра(ов). Можно последовательно задать не более четырех наборов фильтров. Номера наборов фильтров вводятся через запятую. Установленный изготовителем по умолчанию набор фильтров NetBIOS_WAN располагается в поле **protocol filters (фильтры протокола),** в пункте **Call Filter Sets (Наборы фильтров вызовов)** меню 11.5, и предназначен для того, чтобы локальный трафик NetBIOS не мог инициировать вызовы в адрес Интернет-провайдера (ISP).

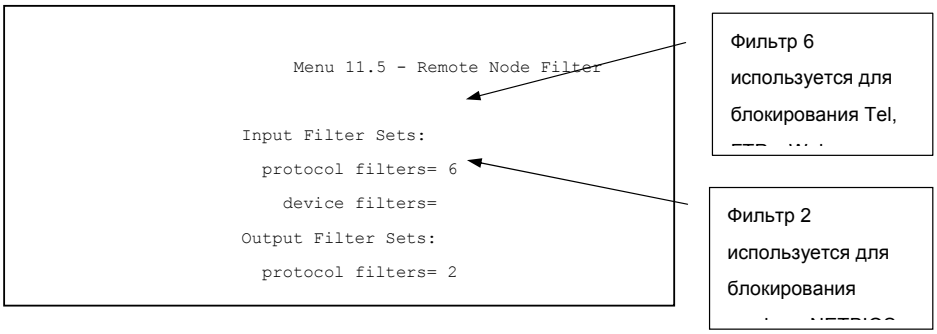


Рис. 32-15 Фильтрование трафика удаленного узла

Следует помнить, что при выборе инкапсуляции PPPoA или PPPoE, наборы фильтров вызовов становятся видимыми.

Раздел 33
Конфигурирование SNMP

В данной главе описывается меню 22 конфигурирования протокола SNMP.

33.1 Что такое SNMP

Протокол SNMP (Простой протокол сетевого управления) используется для обмена управляющей информацией между сетевыми устройствами. SNMP входит в состав набора протоколов TCP/IP. Устройство Prestige поддерживает функциональность агента SNMP, который позволяет через управляющую станцию осуществлять управление и мониторинг устройством Prestige по сети. Prestige поддерживает протокол SNMP версии один (SNMPv1) и версии два (SNMPv2c). Следующий рисунок иллюстрирует функцию управления по протоколу SNMP. SNMP доступен только если выполнено конфигурирование TCP/IP.

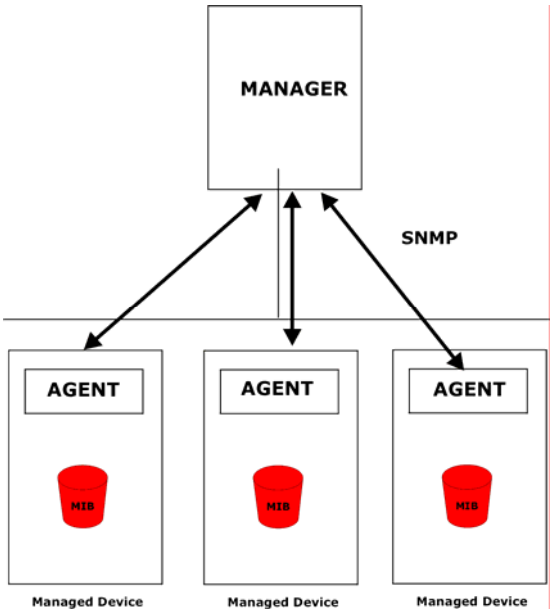


Рис. 33-1 Модель управления по протоколу SNMP

Сеть, управляемая протоколом SNMP, состоит из двух основных компонентов: агентов и программы управления.

Агент представляет собой модуль программы управления, находящийся в управляемом устройстве (Prestige). Агент преобразует информацию о локальную управлении, получаемую от управляемого устройства, в форму, совместимую с протоколом SNMP. В качестве управляющей программы выступает консоль, при помощи которой сетевые администраторы осуществляют управление сетью. Через консоль происходит запуск приложений, предназначенных для контроля и мониторинга над управляемыми устройствами.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют какой вид информации об устройстве необходимо собрать. В качестве примеров переменных можно назвать: количество полученных пакетов, статус порта узла и т.д. База управляющей информации (MIB) представляет собой коллекцию управляемых объектов(MIB). Протокол SNMP позволяет управляющей программе и агентам обмениваться друг с другом информацией, необходимой для доступа к данным объектам.

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

- Get — позволяет управляющей программе извлекать объектную переменную из агента.
- GetNext — позволяет управляющей программе извлекать следующую объектную переменную из таблицы или списка, расположенных внутри агента. В версии 1 протокола SNMP (SNMPv1), при необходимости извлечь все элементы из таблицы, находящейся внутри агента, при помощи управляющей программы, следует сначала инициировать операцию "Get", а затем серию операций "GetNext".
- Set — позволяет управляющей программе устанавливать значения для объектных переменных, находящихся внутри агента.
- Trap — используется агентом для передачи управляющей программе информации о произошедших событиях.

33.2 Поддерживаемые базы управляющей информации (MIB)

Устройство Prestige поддерживает Запросы на комментарии RFC-1215 и Базы управляющей информации MIB II так, как определено в RFC-1213, а также в частных базах управляющей информации корпорации ZyXEL. Базы управляющей информации предназначены для того, чтобы администраторы собирали и размещали в них статистические данные, и осуществляли с их помощью мониторинг статуса и производительности.

33.3 Конфигурирование SNMP

Для конфигурирования протокола SNMP, откройте **Меню 22 — SNMP Configuration (Конфигурирование SNMP)** (см. ниже)**.** Для этого, в главном меню выберите опцию 22. "Паролем" для полей Get (Получить), Set (Установить) и Trap (Прервать) является термин SNMP для пароля.

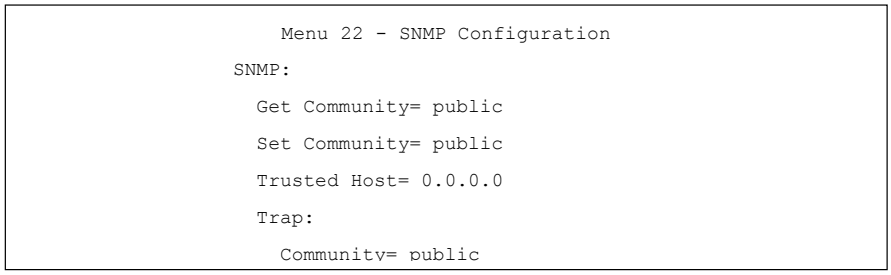


Рис. 33-2 Меню 22 Конфигурирование SNMP

В таблице ниже приводятся описания параметров конфигурации протокола SNMP.

Табл. 33-1 Меню 22 Конфигурирование SNMP

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
SNMP:		
Get Community (Получить пароль)	Наберите в этом поле фразу "**Get Community",** которая является паролем для входящих запросов Get- и GetNext, поступающих от управляющей станции.	public (общий)
Set Community (Установить пароль)	Наберите в этом поле фразу "**Set** community", которая является паролем для входящих Set-запросов, поступающих от управляющей станции.	public (общий)
Trusted Host (Доверенный хост)	Если указать в этом поле доверенный хост, то Prestige будет отвечать только на SNMP сообщения, получаемые с этого адреса. Отсутствие значения в этом поле (устанавливаемое по умолчанию) означает, что Prestige будет отвечать на все получаемые запросы вне зависимости от их источника.	0.0.0.0

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Trap: (Прерывание)		
Community (Пароль)	Наберите в этом поле пароль прерывания, который отправляется с каждым прерыванием в адрес управляющей станции SNMP.	public (общий)
Destination (Пункт назначения)	Укажите в этом поле IP-адрес станции, куда посылаются прерывания SNMP.	0.0.0.0
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.		

33.4 Прерывания SNMP

Устройство Prestige будет отправлять прерывания в адрес управляющей станции SNMP если произойдет любое из перечисленных ниже событий:

Табл. 33-2 Прерывания SNMP

НОМЕР ПРЕРЫВАНИЯ	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
1	coldStart (*определен в RFC-1215*)	Прерывание отправляется после загрузки (после включения питания).
2	warmStart (*определен в RFC-1215*)	Прерывание отправляется после загрузки (после перезагрузки программного обеспечения).
3	linkDown (*определен в RFC-1215*)	Прерывание отправляется с номером порта в случае обрыва любого из каналов связи. См. таблицу ниже.
4	linkUp (*определен в RFC-1215*)	Прерывание отправляется с номером порта.
5	authenticationFailure (*определен*	Прерывание направляется в адрес управляющей

НОМЕР ПРЕРЫВАНИЯ	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
	в RFC-1215)	программы в случае получения требований SNMP "Get" или "Set" с неправильным паролем.
6	whyReboot (определен в ZYXEL-MIB)	Отправка прерывания происходит по причине перезапуска системы, готовившейся к перезапуску, до перезагрузки (теплый запуск).
6a	Для преднамеренной перезагрузки:	Если перезагрузка выполняется преднамеренно, то прерывание отправляется с сообщением "Перезагрузка системы пользователем!" (например, при загрузке новых файлов, выполнение команды CI (командного процессора) "sys reboot", и т. д.).

Номер порта является индексом интерфейса в составе группы интерфейсов.

Табл. 33-3 Порты и постоянные виртуальные каналы

ПОРТ	ПОСТОЯННЫЙ ВИРТУАЛЬНЫЙ КАНАЛ (PVC)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	xDSL

Раздел 34
Защитные функции системы

В данной главе описывается порядок установки параметров конфигурации защитных функций системы устройства Prestige.

34.1 Защитные функции системы

В меню 23 вы можете сконфигурировать системный пароль, внешний сервер RADIUS и IEEE802.1x.

34.1.1 Системный пароль

В главном меню наберите цифру 23 для того, чтобы открыть **Меню 23 – System Security (Защитные функции системы)**.

Вам следует изменить пароль, установленный по умолчанию. Если Вы забыли пароль, то Вам придется восстановить файл конфигурации по умолчанию. О том, как изменить системный пароль, см. раздел, посвященный смене системного пароля, в главе *Введение в SMT,* а также раздел, посвященный перезагрузке устройства Prestige в главе *Введение в Web-конфигуратор*.

```
Menu 23 - System Security

        1. Change Password
```

Рис. 34-1 Меню 23. Защитные функции системы

34.1.2 Конфигурирование внешнего сервера RADIUS

Откройте **Меню 23.2 — System Security-RADIUS Server (Сервер защитных функций системы RADIUS).** Для этого, в Меню 23 — **System Security (Защитные функции системы)** введите цифру 2.

```
Menu 23 - System Security

        1. Change Password
```

Рис. 34-2 Меню 23. Защитные функции системы

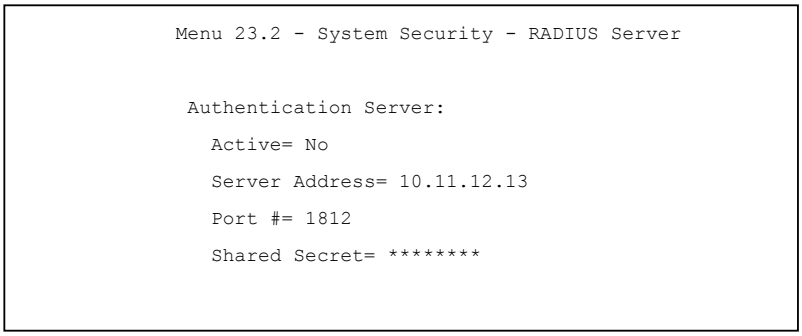


Рис. 34-3 Меню 23.2. Защитные функции системы: Сервер RADIUS

В таблице ниже приводятся описания полей данного меню.

Табл. 34-1 Меню 23.2. Защитные функции системы: Сервер RADIUS

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Authentication Server (Сервер аутентификации)		
Active (Активно)	Клавишей [ПРОБЕЛ] для выберите опцию **Yes (Да)** и нажмите клавишу [ENTER] для того, чтобы включить функцию аутентификации пользователей через внешний сервер аутентификации.	**No (Нет)**
Server Address (Адрес сервера)	Введите в этом поле IP-адрес внешнего сервера аутентификации в десятичном виде с разделительными точками.	10.11.12.13
Port (Порт)	По умолчанию, для сервера аутентификации RADIUS устанавливается порт **1812**. Вам нет необходимости изменять это значение, кроме как по указанию сетевого администратора, и в соответствии с предоставленной им информацией.	**1812**

Табл. 34-1 Меню 23.2. Защитные функции системы: Сервер RADIUS

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Shared Secret (Совместно используемый пароль)	Укажите в этом поле пароль (не более 31 буквенно-цифрового символа) в качестве ключа для совместного использования внешним сервером аутентификации и точками доступа. Этот ключ не передается по сети. Устройство Prestige и сервер аутентификации должны использовать один и тот же ключ.	
Accounting Server (Сервер учета)		
Active (Активно)	Клавишей [ПРОБЕЛ] выберите опцию **Yes (Да)** и нажмите клавишу [ENTER] для того, чтобы включить функцию аутентификации пользователей через внешний сервер учета.	**No (Нет)**
Server Address (Адрес сервера)	Введите в этом поле IP-адрес внешнего сервера учета в десятичном виде с разделительными точками.	10.11.12.13
Port (Порт)	По умолчанию, для сервера учета RADIUS устанавливается порт **1813**. Вам нет необходимости изменять это значение, кроме как по указанию сетевого администратора, и в соответствии с предоставленной им информацией.	**1813**
Shared Secret (Совместно используемый пароль)	Укажите в этом поле пароль (не более 31 буквенно-цифрового символа) в качестве ключа для совместного использования внешним сервером учета и точками доступа. Этот ключ не передается по сети. Устройство Prestige и сервер учета должны использовать один и тот же ключ.	
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо — клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.		

34.1.3 IEEE802.1x

Стандарты IEEE802.1x описывают методы усиленной защиты от несанкционированного доступа как для аутентификации беспроводных станций, так и для управления ключами шифрования.

Для того, чтобы включить на устройстве Prestige функцию расширенного протокола идентификации (EAP), выполните следующие действия:

Step 13. Откройте **Меню 23 — System Security (Защитные функции системы)**. Для этого в главном меню наберите цифру 23.

```
Menu 23 - System Security

1. Change Password
2. RADIUS Server
```

Рис. 34-4 Меню 23. Защитные функции системы

Step 14. Для того, чтобы открыть **Меню 23.4 — System Security (Защитные функции системы) — IEEE802.1x**, наберите цифру 4.

```
Menu 23.4 - System Security - IEEE802.1x

Wireless Port Control= Authentication Required
ReAuthentication Timer (in second)= 1800
Idle Timeout (in second)= 3600


Key Management Protocol= WPA
Dynamic WEP Key Exchange= N/A
```

Рис. 34-5 Меню 23.4 Защитные функции системы: IEEE802.1x

В таблице ниже приводятся описания полей данного меню.

Табл. 34-2 Меню 23.4 Защитные функции системы: IEEE802.1x

ПОЛЕ	ОПИСАНИЕ
Wireless Port Control (Управление беспроводным портом)	Нажатием клавиши [ПРОБЕЛ] выберите режим безопасности для беспроводного доступа к локальной вычислительной сети. Для того, чтобы открыть доступ пользователю любой беспроводной станции к проводной сети без ввода имени пользователя и пароля, выберите опцию **No Authentication Required (Аутентификация не требуется)**. Эта опция устанавливается по умолчанию. Если выбрать опцию **Authentication Required (Требуется аутентификация),** то для получения доступа к проводной сети пользователь беспроводной станции должен будет ввести имя пользователя и пароль. Для того, чтобы заблокировать доступ пользователей всех беспроводных станций к проводной сети, выберите опцию **No Access Allowed (Доступ закрыт)**. Ниже указаны поля, которые недоступны, если выбраны опции **No Authentication Required (Аутентификация не требуется)** или **No Access Allowed (Доступ закрыт)**.
ReAuthentica-tion Timer (in second) (Таймер повторной аутентификации (в секундах))	Укажите в этом поле периодичность, с которой клиент должен повторно вводить имя пользователя и пароль для того, чтобы сохранять подключение к проводной сети. Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводным портом)**. Укажите отрезок времени в диапазоне значений от 10 до 9999 (в секундах). По умолчанию устанавливается значение в **1800** секунд (или 30 минут).
Idle Timeout (in second) (Время простоя (в секундах))	По истечении периода времени бездействия, Prestige автоматически отключает клиента от проводной сети. Для того, чтобы вновь получить доступ к проводной сети, клиент должен заново ввести имея пользователя и пароль. Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводным портом).** По умолчанию устанавливается значение в **3600** секунд (или 1 час).
Key Management Protocol (Протокол управления ключом)	Клавишей [ПРОБЕЛ] выберите **802.1x**, **WPA (Защищенный беспроводной доступ)** или **WPA-PSK (Защищенный беспроводной доступ — предварительно согласованный ключ)** и нажмите клавишу [ENTER].

Табл. 34-2 Меню 23.4 Защитные функции системы: IEEE802.1x

ПОЛЕ	ОПИСАНИЕ
Dynamic WEP Key Exchange (Динамический обмен ключами WEP)	Это поле активируется только в случае, если выбрана опция **Authentication Required (Требуется аутентификация)** в поле **Wireless Port Control (Управление беспроводным портом)**. Также в поле **Authentication Databases (Базы данных аутентификации)** установите опцию **RADIUS Only (Только RADIUS)**. Локальные базы данных пользователей можно не использовать. Для того, чтобы беспроводные станции могли поддерживать связь с точками доступа без использования динамического обмена ключами WEP, выберите опцию **Disable (Отключить)**. Для того, чтобы включить функцию шифрования данных, выберите одну из опций: **64-bit WEP** или **128-bit WEP**. При установленных параметрах конфигурации динамического обмена ключами WEP, доступ к устройству Prestige могут получить до 32 станций. Если на **WPA** или **WPA-PSK** установлен **протокол управления ключами (Key Management Protocol),** то это поле недоступно.
PSK (Предварительно согласованный ключ)	При выборе опции **WPA-PSK** в поле **Key Management Protocol (Протокол управления ключами),** введите предварительно согласованный ключ, содержащий от 8 до 63 ASCII символов с учетом регистра (включая пробелы и символы).
WPA Mixed Mode (Смешанный режим WPA)	Для того, чтобы активировать смешанный режим WPA, выберите опцию **Enable** (**Включить**). В противном случае, выберите опцию **Disable (Отключить)** и установите параметры конфигурации поля **Group Data Privacy (Конфиденциальность групповых данных)**.
Data Privacy for Broadcast/ Multicast packets (Конфиденциальность данных для пакетов широковещательной рассылки/многоадресной рассылки)	Вы можете выбрать в этом поле опции **TKIP** (рекомендуется) или **WEP** для широковещательного или многоадресного (“группового”) трафиков, если **протоколом управления ключом** является **WPA,** а **смешанный режим WPA** отключен. При включении **смешанного режима WPA, WEP** задействуется автоматически. При выборе **протокола управления ключом WPA** или **WPA-PSK, TKIP** автоматически кодирует все одноадресные трафики**.**

Табл. 34-2 Меню 23.4 Защитные функции системы: IEEE802.1x

ПОЛЕ	ОПИСАНИЕ
WPA Broadcast/ Multicast Key Update Timer (Таймер обновления ключа WPA широковещательной/многоадресной рассылки)	**Таймер ключа WPA широковещательной/многоадресной рассылки** показывает скорость, на которой сервер AP (при управлении ключом с помощью **WPA-PSK**) или сервер RADIUS (при управлении ключом с помощью **WPA**) осуществляют передачу нового группового ключа всем клиентам. Процесс повторной настройки по ключу является эквивалентом управления ключом при помощи WPA, при котором автоматически с определенной периодичностью происходит замена WEP ключа для сервера AP и всех станций виртуальной локальной вычислительной сети. Настройка **таймера обновления ключа WPA для широковещательной/многоадресной рассылки** также может осуществляться в режиме WPA-PSK. По умолчанию в Prestige устанавливается значение времени в 1800 секунд (30 минут).

Табл. 34-2 Меню 23.4 Защитные функции системы: IEEE802.1x

ПОЛЕ	ОПИСАНИЕ
Authentication Databases (Базы данных аутентификации)	База данных аутентификации содержит регистрационные сведения о беспроводной станции. Локальная база данных пользователей является встроенной базой данных устройства Prestige. RADIUS является внешним сервером. Укажите в этом поле, какую базу данных Prestige должен использовать (первой) для аутентификации беспроводной станции. Прежде, чем выставить приоритет, убедитесь, что соответствующая база данных установлена надлежащим образом. Если для **WPA (Защищенного беспроводного доступа)** Вы используете **Протокол управления ключами (Key Management Protocol),** то в качестве **Базы данных аутентификации** (**Authentication Databases)** должен использоваться только сервер **RADIUS**. С **Протоколом управления ключами 802.1x** можно использовать только **Локальную базу данных пользователей.** Для того, чтобы Prestige выполнял проверку имени пользователя и пароля беспроводной станции по встроенной базе данных пользователя, выберите опцию **Local User Database Only (Только локальная база данных пользователя)**. Для того, чтобы Prestige выполнял проверку имени пользователя и пароля беспроводной станции по базе данных пользователя, расположенной на указанном сервере RADIUS, выберите опцию **RADIUS Only (Только RADIUS)**. Для того, чтобы Prestige выполнял проверку имени пользователя и пароля беспроводной станции сначала по базе данных пользователя, расположенной в устройстве Prestige, выберите опцию **Local first, then RADIUS (Сначала локальная база, затем RADIUS)**. Если имя пользователя не найдено, то Prestige производит проверку по базе данных пользователей, расположенной на указанном сервере RADIUS. Для того, чтобы Prestige выполнял проверку имени пользователя и пароля беспроводной станции сначала по базе данных пользователя, расположенной на указанном сервере RADIUS, выберите опцию **RADIUS first, then Local (Сначала RADIUS, затем локальная база)**. Если Prestige не может получить доступ к серверу RADIUS, то он производит проверку по локальной базе данных пользователя, расположенной в самом устройстве Prestige. Если имя пользователя не найдено или пароль не соответствует тому, что указано на сервере RADIUS, то Prestige не производит их проверку по локальной базе данных пользователя и аутентификация не проходит.
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.	

Если функция аутентификации пользователей включена, то необходимо указать внешний сервер RADIUS или создать локальные учетные записи пользователей на устройстве Prestige.

34.2 Создание учетных записей пользователей на устройстве Prestige

Если настройки пользователей сохранять локально на устройстве Prestige, то устройство может выполнять аутентификацию пользователей беспроводных станций, не обращаясь к сетевому серверу RADIUS.

Для того, чтобы создать настройки пользователей на устройстве Prestige, выполните указанные ниже операции.

Step 15. Откройте **Меню14 – Dial-in User Setup (Настройка удаленного коммутируемого пользователя)**. Для этого, в главном меню наберите цифру 14.

```
                    Menu 14 - Dial-in User Setup


     1. ________        9.  ________        17. ________        25.
________
     2. ________        10. ________        18. ________        26.
________
     3. ________        11. ________        19. ________        27.
```

Рис. 34-6 Меню 14. Настройка удаленного коммутируемого пользователя

Step 16. Для изменения настроек пользователя, введите соответствующий номер и нажмите клавишу [ENTER] .

```
                Menu 14.1 - Edit Dial-in User


                   User Name= test
                   Active= Yes
```

Рис. 34-7 Меню 14.1 Изменение настроек удаленного коммутируемого пользователя

В таблице ниже приводятся описания полей данного меню.

Табл. 34-3 Меню 14.1 Изменение настроек удаленного коммутируемого пользователя

ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите имя пользователя (не более 31 буквенно-цифрового символа) для данных настроек пользователя. Значения данного поля вводятся с учетом регистра.
Active (Активно)	Для того, чтобы включить настройки пользователя, при помощи клавиши [ПРОБЕЛ] выберите опцию **Yes (Да)** и нажмите клавишу [ENTER].
Пароль	Введите пароль (не более 31 буквенно-цифрового символа) для данных настроек пользователя.
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.	

Раздел 35
Системная информация и диагностика

В данной главе описываются средства диагностики и получения информации, расположенные в меню SMT с цифровыми обозначениями от 24.1 до 24.4.

К данным инструментальным средствам относятся: обновления системного статуса, статуса портов, возможностей журнальной регистрации и трассировки, а также модернизация системного программного обеспечения. В данной главе подробно описывается, как пользоваться этими инструментальными средствами.

Откройте **Меню 24 – System Maintenance (Сопровождение системы)**, см. рисунок ниже**.** Для этого, в главном меню наберите цифру 24.

```
Menu 24 - System Maintenance

 1.  System Status
 2.  System Information and Console Port
Speed
 3.  Log and Trace
 4.  Diagnostic
 5.  Backup Configuration
 6.  Restore Configuration
 7.  Upload Firmware
 8.  Command Interpreter Mode
```

Рис. 35-1 Меню 24. Защитные функции системы

35.1 Статус системы

При первом выборе опции Статус системы на дисплее отображается информация о статусе системы и статистическая информация о портах, см. рисунок ниже. Статус системы является инструментальным средством, используемым для мониторинга устройства Prestige. В частности, с ее помощью можно получить информацию о статусе телефонной линии ADSL, а также о количестве полученных и отправленных пакетов.

Статус системы находится в **Меню 24 — System Maintenance (Сопровождение системы)**. Для того, чтобы открыть это меню, наберите цифру 24.В открывшемся меню, наберите цифру 1**. System Status (Статус системы)**. В **Меню 24.1 — System Maintenance (Сопровождение системы) — Status (Статус)** имеются две команды. При вводе цифры 1 происходит сброс показаний счетчиков, а при нажатии клавиши [ESC] открывается предыдущая экранная форма.

В таблице ниже представлены описания полей **Меню 24.1 — System Maintenance (Сопровождение системы) — Status (Статус),** которые доступны только для чтения и используются в целях диагностики.

```
                    Menu 24.1 - System Maintenance - Status
04:35:40

                                                          Sat. Jan.
01, 2000


Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s
Up Time
 1-1483  N/A              0           0           0       0       0
0:00:00
 2       N/A              0           0           0       0       0
0:00:00
 3       N/A              0           0           0       0       0
0:00:00
```

Рис. 35-2 Меню 24.1. Сопровождение системы: Статус

В таблице ниже даются описания полей **Меню 24.1 — System Maintenance (Сопровождение системы) — Status (Статус)**.

Табл. 35-1 Меню 24.1 Сопровождение системы: Статус

ПОЛЕ	ОПИСАНИЕ
Node-Lnk	В этом поле отображаются индекс удаленного узла и тип связи. Используются следующие типы связи: PPP, ENET и 1483.
Status (Статус)	В этом поле отображается статус удаленного узла.
TxPkts (Передано	В этом поле отображается количество пакетов, переданных на данный

Табл. 35-1 Меню 24.1 Сопровождение системы: Статус

ПОЛЕ	ОПИСАНИЕ
пакетов)	удаленный узел.
RxPkts (Принято пакетов)	В этом поле отображается количество пакетов, принятых от данного удаленного узла.
Errors (Ошибки)	В этом поле отображается количество пакетов с ошибками, обнаруженных во время данного сеанса связи.
Tx B/s (Передача, б/с)	В этом поле отображается скорость передачи данных в байтах в секунду.
Rx B/s (Прием, б/с)	В этом поле отображается скорость приема данных в байтах в секунду.
Up Time (Время соединения)	В этом поле отображается продолжительность текущего сеанса связи с данным удаленным узлом.
My WAN IP (from ISP)	В этом поле отображается IP-адрес удаленного узла Интернет-провайдера.
Ethernet	В этом поле отображается статистическая информация локальной вычислительной сети (LAN).
Status (Статус)	В этом поле отображается статус локальной вычислительной сети (LAN).
Tx Pkts:	В этом поле отображается количество пакетов, переданных на локальную вычислительную сеть(LAN).
Rx Pkts:	В этом поле отображается количество пакетов, полученных от локальной вычислительной сети(LAN).
Collision (Конфликт)	В этом поле отображается количество конфликтов.
WAN (Глобальная вычислительная сеть)	В этом поле отображается статистическая информация глобальной вычислительной сети (WAN).
Line Status (Статус линии)	В этом поле отображается текущий статус линии xDSL line, который может быть либо Up (Вкл), либо Down (Выкл).

Табл. 35-1 Меню 24.1 Сопровождение системы: Статус

ПОЛЕ	ОПИСАНИЕ
Upstream Speed (Скорость исходящего потока)	В этом поле отображается скорость исходящего потока в кбит/с.
Downstream Speed (Скорость входящего потока)	В этом поле отображается скорость входящего потока в кбит/с.
CPU Load (Загрузка CPU)	В этом поле отображается загрузка центрального процессорного устройства в процентах.

35.2 Системная информация

Для того, чтобы вывести на дисплей системную информацию,

Step 17. Для того, чтобы открыть **Меню 24 — System Maintenance (Сопровождение системы)** наберите цифру 24.

Step 18. Для того, чтобы отобразить **Меню 24.2 — System Information and Console Port Speed (Информация о системе и скорость консольного порта),** наберите цифру 2.

Step 19. В этом меню имеются две опции, которые представлены на рисунке ниже:

```
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 скорости консольного порта

Устройство Prestige оснащено внутренним консольным портом, доступ к которому разрешен только специалистам из службы технической поддержки. Не открывайте устройство Prestige, так как это является нарушением условий гарантийных обязательств.

35.2.1 Системная информация

Для того, чтобы открыть окно, изображение которого приводится ниже, в меню 24.2 наберите цифру 1.

```
Menu 24.2.1 - System Maintenance - Information

   Name:
   Routing: IP
   ZyNOS F/W Version: V3.40(PE.0)b1 | 12/18/2003
   ADSL Chipset Vendor: TI AR7 01.01.00.00
   Standard: NORMAL
```

Рис. 35-4 Меню 24.2.1 Сопровождение системы: Информация

В таблице ниже приводятся описания полей данного меню.

Табл. 35-2 Меню 24.2.1 Сопровождение системы: Информация

ПОЛЕ	ОПИСАНИЕ
Name (Имя)	В этом поле отображается системное имя устройства Prestige. Изменение информации в этом поле осуществляется через **Меню 1 – General Setup (Настройка общих параметров)**.
Routing (Маршрутизация)	В этом поле отображается ссылка на используемый маршрутизирующий протокол.
ZyNOS F/W Version	В этом поле отображается ссылка на версию микропрограммного обеспечения ZyNOS (Сетевая операционная система ZyXEL). ZyNOS является зарегистрированной торговой маркой Корпорации ZyXEL Communications.
ADSL Chipset Vendor	В этом поле отображаются производитель микросхем ADSL и версия

Табл. 35-2 Меню 24.2.1 Сопровождение системы: Информация

ПОЛЕ	ОПИСАНИЕ
(Производитель микросхем ADSL)	цифровой абонентской линии (DSL).
Standard (Стандарт)	В этом поле отображается ссылка на операционный протокол, используемый устройством Prestige и DSLAM (Мультиплексором цифровых абонентских линий).
LAN (ЛВС)	
Ethernet Address (Адрес Ethernet)	В этом поле отображается ссылка на Ethernet MAC (Управление доступом к среде) устройства Prestige.
IP Address (IP-адрес)	В этом поле отображается IP-адрес Prestige в десятичном виде с разделительными точками.
IP Mask (Маска IP)	В этом поле отображается маска подсети устройства Prestige.
DHCP (Dynamic Host Configuration Protocol/Протокол динамического выбора конфигурации хост-машины)	В этом поле отображается настройка DHCP (None (Нет), Relay (Передача) или Server (Сервер)) устройства Prestige.

35.2.2 Скорость консольного порта

В **Меню 24.2.2 – System Maintenance (Сопровождение системы) – Console Port Speed (Скорость консольного порта)** можно устанавливать различные значения скорости для консольного порта. Устройство Prestige поддерживает следующие значения скорости в битах в секунду (бит/с): 9600 (по умолчанию), 19200, 38400, 57600 и 115200. Для того, чтобы установить желаемую скорость, в меню 24.2.2. при помощи клавиши [ПРОБЕЛ] выберите нужное значение и нажмите клавишу [ENTER] так, как показано на рисунке ниже.

```
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 устройства Prestige необходимо также установить соответствующий параметр скорости для программного обеспечения, предназначенного для работы в режиме терминала, и используемого для подключения к устройству Prestige.

35.3 Журнальная регистрация и трассировка

Существуют две функциональные возможности регистрации в устройстве Prestige. Первая: журнал регистрации ошибок и регистрационные записи пути, которые хранятся локально. Вторая: функция системного журнала UNIX для регистрации сообщений.

35.3.1 Просмотр журнала регистрации ошибок

При возникновении каких-либо неполадок, в первую очередь необходимо посмотреть записи журнала регистрации ошибок. Для того, чтобы посмотреть записи локального журнала регистрации ошибок/результатов трассировки, выполните указанные ниже действия:

Step 1. В главном меню наберите цифру 24 для того, чтобы открыть **Меню 24 – Сопровождение системы**.

Step 2. Для того, чтобы открыть **Меню 24.3 – System Maintenance (Сопровождение системы) –**

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

    1. View Error Log
    2. UNIX Syslog



            Please enter selection
```

Log and Trace (Журнальная регистрация и трассировка), в меню 24 наберите цифру 3.

Рис. 35-6 Меню 24.3 Сопровождение системы: Журнальная регистрация и трассировка

Step 3. Для того, чтобы отобразить журнал регистрации ошибок в системе, в **Меню 24.3 — System Maintenance (Сопровождение системы) — Log and Trace (Журнальная регистрация и трассировка)**наберите цифру 1.

После того, как устройство Prestige отобразит на экране журнал регистрации ошибок, у вас появится опция, позволяющая очистить содержимое журнала. На рисунке ниже приводятся примеры типичных ошибок и информационных сообщений.

```
59 Thu Jan 01 00:00:03 1970 PP0f  INFO  LAN promiscuous mode <0
60 Thu Jan 01 00:00:03 1970 PP00 -WARN  SNMP TRAP 0: cold start
61 Thu Jan 01 00:00:03 1970 PP00  INFO  main: init completed
```

Рис. 35-7 Примеры сообщений об ошибках и информационных сообщений

35.3.2 Системный журнал и учет

Устройство Prestige использует функцию системного журнала UNIX для регистрации CDR (Журнал регистрации вызовов) и системных сообщений на сервере системного журнала. Параметры конфигурации системного журнала и учета устанавливаются в **Меню 24.3.2 — System Maintenance**

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

        UNIX Syslog (Системный журнал UNIX):
        Active= No
        Syslog IP Address= ?
        Log Facility= Local 1
```

(Сопровождение системы) — UNIX Syslog (Системный журнал UNIX), как показано ниже.

Рис. 35-8 Меню 24.3.2 Сопровождение системы: Системный журнал и учет

Для того, чтобы активировать системный журнал, необходимо установить параметры конфигурации системного журнала UNIX, описание которых приводится в таблице ниже, а затем выбрать то, что Вы хотите 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 и выключения системного журнала, клавишей [ПРОБЕЛ] выберите соответствующую опцию и нажмите клавишу [ENTER].
Syslog IP Address (IP-адрес системного журнала)	Введите IP-адрес сервера системного журнала.
Log Facility (Функция журнальной регистрации)	Клавишей [ПРОБЕЛ] выберите одну из семи опций и нажмите клавишу [ENTER]. Функция журнальной регистрации позволяет регистрировать сообщение в различных файлах сервера. Более подробно см. руководство пользователя по UNIX.

Ниже приводятся примеры системных сообщений четырех типов, отправленных устройством Prestige:

1 — Журнал регистрации вызовов
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 — Инициирующий пакет
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=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=450000282401400001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
3 — Журнал регистрации фильтров
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 — Журнал регистрации PPP

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

35.4 Диагностика

Функция диагностики позволяет проверять различные аспекты функционирования устройства Prestige и определять, работает оно надлежащим образом, или нет. В Меню 24.4, см. рисунок ниже, имеется множество диагностических тестов различных типов, с помощью которых можно проверить качество работы системы.

Для того, чтобы открыть меню диагностики, выполните следующие операции:

Step 1. Откройте **Меню 24 – System Maintenance (Сопровождение системы).** Для этого, в главном меню наберите цифру 24.

Step 2. В открывшемся меню наберите цифру 4, соответствующую пункту Diagnostic

```
            Menu 24.4 - System Maintenance - Diagnostic


xDSL                                System

1.  Reset xDSL                      21. Reboot System

                                    22. Command Mode
```

Formatted: Bullets and Numbering

(Диагностика). При этом откроется **Меню 24.4 – System Maintenance (Сопровождение системы) – Diagnostic (Диагностика)**.

Рис. 35-9 Меню 24.4 Сопровождение системы: Диагностика

В таблице ниже приведены описания диагностических тестов, доступных в меню 24.4, и предназначенных для проверки функционирования каналов связи.

Табл. 35-4 Меню 24.4 Меню сопровождения системы: Диагностика

ПОЛЕ	ОПИСАНИЕ

Табл. 35-4 Меню 24.4 Меню сопровождения системы: Диагностика

ПОЛЕ	ОПИСАНИЕ
Reset xDSL (Сброс xDSL)	Заново устанавливает сеанс связи xDSL с телефонной компанией.
Ping Host (Эхо-тестирование связи с хост-машиной)	Выполняет эхо-тестирование для того, чтобы проверить работоспособность каналов связи и протокола TCP/IP на обеих системах.
Reboot System (Перезагрузить систему)	Перезагрузка устройства Prestige.
Command Mode (Командный режим)	Введите с клавиатуры режим для тестирования и диагностики устройства Prestige при помощи определенного набора команд.
Host IP Address (IP-адрес хоста)	Если вы уже набрали цифру 12 для эхо-тестирования связи с хост-машиной, то теперь наберите адрес компьютера, с которым необходимо установить связь путем эхо-тестирования.

Раздел 36
Управление микропрограммным обеспечением и файлом конфигурации

В этой главе описывается порядок создания резервной копии и восстановления файл конфигурации, а также порядок выгрузки нового микропрограммного обеспечения и файла конфигурации.

36.1 Соглашение по именам файлов

Файл конфигурации (часто называемый также "romfile" или "rom-0") содержит настройки, установленные изготовителем по умолчанию, например: пароль, настройки DHCP, настройки TCP/IP и т. д. Этот файл поставляется корпорацией ZyXEL и имеет расширение “rom”. Если вы изменили настройки устройства Prestige по своему усмотрению, то эти изменения можно сохранить в файле под другим именем, по Вашему выбору.

ZyNOS (Сетевая операционная система корпорации ZyXEL, иногда называемая "ras" файл) представляет собой микропрограммное обеспечение системы, файлы системы имеют расширение "bin". У большинства клиентов FTP и TFTP имена файлов схожи с представленными ниже.

Используйте только то, микропрограммное обеспечение, которое предназначено именно для данной модели устройства Prestige. Оно указано на ярлычке, который находится на нижней панели устройства Prestige.

```
ftp> put firmware.bin ras
```
Это пример сеанса FTP по передаче компьютерного файла "firmware.bin" на устройство Prestige.

```
ftp> get rom-0 config.cfg
```
Это пример сеанса FTP по сохранению текущей конфигурации в компьютерном файле "config.cfg".

Если Ваш (T)FTP клиент не допускает, чтобы имя полученного файла отличалось от имени файла-источника, то Вам потребуется переименовать оба файла, поскольку Prestige распознает только файлы с расширением "rom-0" и "ras". Обязательно сохраните не измененные копии обоих первоначальных файлов, они потребуются в дальнейшем.

Ниже представлена таблица, содержащая сводную информацию. Следует отметить, что имя внутреннего файла обозначает файл, находящийся на устройстве Prestige, а имя внешнего файла

обозначает файл, не находящегося на устройстве Prestige, то есть, находящегося на вашем компьютере, в локальной сети или на FTP сайте. Поэтому имя файла, но не расширение файла, может быть иным. После выгрузки нового микропрограммного обеспечения, откройте поле **ZyNOS F/W Version** в **Меню 24.2.1 – System Maintenance (Сопровождение системы) – Information (Информация)** и подтвердите, что Вы выгрузили правильную версию микропрограммного обеспечения. AT-команда — это команда, которая вводится при нажатии клавиши "y" по запросу меню SMT для входа в режим отладки.

Табл. 36-1 Соглашение по именам файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл конфигурации	Rom-0	Это имя файла конфигурации на устройстве Prestige. При выгрузке файла rom-0 происходит замена всей файловой системы ПЗУ, включая конфигурацию Prestige, данные, относящиеся к системе (в том числе и пароль по умолчанию), журнал регистрации ошибок и журнал регистрации результатов трассировки.	*.rom
Микропрограммное обеспечение	Ras	Это базовое имя для микропрограммного обеспечения ZyNOS на устройстве Prestige.	*.bin

36.2 Создание резервной копии конфигурации

Опция 5 в **Меню 24 – System Maintenance (Сопровождение системы)** позволяет создать резервную копию текущей конфигурации устройства Prestige и сохранить ее на компьютере. Настоятельно рекомендуется создать резервную копию конфигурации устройства Prestige в тот момент когда оно функционирует надлежащим образом. Наиболее предпочтительным способом создания резервной копии является FTP потому, что это наиболее быстрый способ. При этом любые коммуникационные программы должны работать хорошо, однако, для передачи/приема необходимо использовать протокол Xmodem. Переименовывать файлы Вам не придется.

Следует заметить, что термины "загрузка" и "выгрузка" (download/upload) используются с позиции компьютера. "Загрузка (download)" означает получение данных от устройства Prestige на компьютер, а "выгрузка (upload)" — наоборот, передачу данных с компьютера на устройство Prestige.

36.2.1 Создание резервной копии конфигурации

Для создания резервной копии конфигурации, следуйте указаниям, изложенным на рисунке ниже.

```
            Menu 24.5 - System Maintenance - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current Prestige configuration to
   your workstation.

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

Рис. 36-1 Telnet в Меню 24.5

36.2.2 Использование команды FTP из командной строки

Step 1. Запустите клиента FTP на вашем компьютере.

Step 2. Введите команду “open”, а затем — IP-адрес устройства Prestige через пробел.

Step 3. В диалоговом окне введите имя пользователя и нажмите клавишу [ENTER] .

Step 4. В окне запроса введите пароль (по умолчанию "1234").

Step 5. Введите “bin” для того, чтобы установить двоичный режим передачи.

Step 6. Для передачи файлов с устройства Prestige на Ваш компьютер, используйте команду "get", например, "get rom-0 config.rom". Эта команда передает файл конфигурации, находящийся на Prestige, на Ваш компьютер и переименовывает его в "config.rom". Более подробно о соглашении по именам файлов, см. выше в данной главе.

Step 7. Для выхода из режима FTP, введите команду "quit".

36.2.3 Примеры команд FTP, вводимых из командной строки

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
```

Рис. 36-2 Пример сеанса FTP

36.2.4 FTP- клиенты, созданные на основе графического пользовательского интерфейса (GUI)

В таблице ниже приводятся описания некоторых команд, имеющихся у FTP-клиентов, и созданных на основе графического пользовательского интерфейса (GUI).

Табл. 36-2 Общие команды FTP-клиентов, созданных на основе GUI

КОМАНДА	ОПИСАНИЕ
Host Address (Адрес хоста)	Введите адрес хост-сервера.
Login Type (Тип регистрации)	Анонимный. Этот тип регистрации используется в случаях, когда идентификатор пользователя и пароль автоматически передаются серверу для получения анонимного доступа. Анонимная регистрация возможна, только если администратор услуг Интернет-провайдера включил данную опцию. Стандартный. Для регистрации необходимо ввести уникальный идентификатор пользователя и пароль.
Transfer Type (Тип передачи)	Передача файлов либо в режиме ASCII (формат обычного текста), либо в двоичном режиме.
Initial Remote Directory (Исходный удаленный каталог)	Укажите удаленный каталог по умолчанию (путь).
Initial Local Directory (Исходный локальный	Укажите локальный каталог по умолчанию (путь).

каталог)	

36.2.5 Ограничения в управлении протоколами TFTP и FTP через глобальную вычислительную сеть (WAN)

Функционирование протоколов TFTP, FTP и подключение через Telnet по WAN невозможно, если:

1. Услуга подключения через Telnet отключена в меню 24.11.
2. В меню 3.1 (ЛВС) или в меню 11.5 (ГВС) задействован фильтр, блокирующий услугу подключения через Telnet.
3. IP-адрес, указанный в поле **Secured Client IP (IP-адрес защищенного клиента)** меню 24.11, не соответствует IP-адресу клиента. При обнаружении несоответствия адресов, Prestige немедленно прерывает сеанс связи через Telnet.
4. Запущен сеанс связи через консоль SMT.

36.2.6 Создание резервной копии конфигурации при помощи протокола TFTP

Prestige поддерживает функцию загрузки/выгрузки микропрограммного обеспечения и файла конфигурации по ЛВС с использованием протокола TFTP (Упрощенный протокол передачи файлов). Однако использовать протокол TFTP для работы по глобальной вычислительной сети (WAN) не рекомендуется.

Для того, чтобы использовать протокол TFTP, на Вашем компьютере должны быть установлены и клиент Telnet, и TFTP клиент. Для создания резервной копии файла конфигурации, выполните указанные ниже операции.

Step 1. При помощи сетевого теледоступа (Telnet), установленного на Вашем компьютере, подключитесь к устройству Prestige и зарегистрируйтесь. Поскольку протокол TFTP не обладает функциями проверки для защиты информации, Prestige записывает IP-адрес клиента Telnet и принимает запросы TFTP только с этого адреса.

Step 2. Переключите системную консоль (SMT) в режим командного процессора. Для этого, в **Меню 24 – System Maintenance (Сопровождение системы)** введите цифру 8.

Step 3. Для отключения интервала простоя SMT, введите команду "sys stdio 0". При этом, передача данных по протоколу TFTP не прервется. По окончании передачи файла, для восстановления 5-минутного интервала простоя SMT (значение, устанавливаемое по умолчанию), введите команду "sys stdio 5".

Step 4. Запустите на Вашем компьютере клиента TFTP и подключитесь к устройству Prestige. Прежде чем запустить процесс передачи данных, установите двоичный режим передачи.

Step 5. Для передачи файлов между устройством Prestige и компьютером, используйте клиента TFTP (см. пример ниже). Имя файла конфигурации должно быть "rom-0" (rom-нуль, а не заглавная буква O).

Следует помнить, что подключение через Telnet должно быть активно, а системная консоль (SMT) должна находиться в режиме командного процессора (CI mode) как до, так и во время передачи по протоколу TFTP. Более подробно о командах TFTP (см. следующий пример) можно узнать в сопроводительной документации к клиентской программе TFTP. Если Вы работаете в системе UNIX, то команду "get" используйте для передачи файлов с устройства Prestige на компьютер, а команду "binary" — для установки двоичного режима передачи данных.

36.2.7 Пример команды TFTP

Ниже приводится пример команды TFTP:

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

Где "i" указывает на двоичный режим передачи (этот режим используется для передачи двоичных файлов), "host" — IP-адрес устройства Prestige, а "get" — команда передачи файла, находящегося на устройстве Prestige (rom-0 — имя файла конфигурации, находящегося на устройстве Prestige), на компьютер и переименования его в файл config.rom.

36.2.8 TFTP-клиенты, созданные на основе графического пользовательского интерфейса (GUI)

В таблице ниже приводятся описания некоторых полей, имеющихся у TFTP-клиентов и созданных на основе графического пользовательского интерфейса (GUI).

Табл. 36-3 Общие команды TFTP-клиентов, созданных на основе графического пользовательского интерфейса

КОМАНДА	ОПИСАНИЕ
Host (Хост)	Введите IP-адрес устройства Prestige. При поставке, IP-адресом устройства Prestige по умолчанию является: 192.168.1.1.
Send/Fetch (Передать/Принять)	Для того, чтобы выгрузить файл с компьютера на устройство Prestige, используется команда "Send", а для того, чтобы загрузить файл на компьютер с устройства Prestige — команда "Fetch".
Local File (Локальный файл)	Введите путь и имя файла микропрограммного обеспечения (расширение файла: *.bin) или файла конфигурации (расширение файла: *.rom), находящегося на Вашем компьютере.
Remote File (Удаленный	Это имя файла, находящегося на устройстве Prestige. Имя файла микропрограммного обеспечения — "ras", а файла конфигурации — "rom-0".

файл)	
Binary (Двоичный)	Передача файла в двоичном режиме.
Abort (Отмена)	Остановка процесса передачи файла.

В *разделе 36.2.5* указаны параметры конфигурации, при которых работа протоколов TFTP и FTP в глобальной вычислительной сети невозможна.

36.3 Восстановление конфигурации

В данном разделе описывается порядок восстановления предварительно сохраненных параметров конфигурации. Следует иметь в виду, что при выполнении данной функции, прежде, чем резервная конфигурация будет восстановлена, текущая конфигурация — удаляется. Поэтому, прежде чем запустить процесс восстановления, убедитесь, что файл с резервной копией конфигурации сохранен на диске.

Наиболее предпочтительным способом восстановления текущей конфигурации компьютера на устройство Prestige является протокол FTP потому, что он быстрее остальных. Следует помнить, что после завершения процесса загрузки файла, необходимо дождаться автоматической перезагрузки системы.

ПРЕДУПРЕЖДЕНИЕ!
НЕ ПРЕРЫВАЙТЕ ПРОЦЕСС ЗАГРУЗКИ ФАЙЛА, ПОСКОЛЬКУ ЭТО МОЖЕТ ПРИВЕСТИ К ПОЛНОМУ ВЫХОДУ ИЗ СТРОЯ УСТРОЙСТВА PRESTIGE.

36.3.1 Восстановление с использованием протокола FTP

Более подробно о создании резервной копии конфигурации при помощи (T)FTP, см. раздел в данной главе, посвященный выгрузке файлов через FTP и TFTP.

```
              Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation, follow the
procedure below:

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


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

Рис. 36-3 Подключение к Меню 24.6 через Telnet

Step 1. Запустите клиента FTP на вашем компьютере.

Step 2. Введите команду "open", а затем — IP-адрес устройства Prestige через пробел.

Step 3. В диалоговом окне введите имя пользователя и нажмите клавишу [ENTER] .

Step 4. В окне запроса введите пароль (по умолчанию "1234").

Step 5. Введите "bin" для того, чтобы установить двоичный режим передачи.

Step 6. Найдите на вашем компьютере файл "rom", который Вы намерены восстановить на устройстве Prestige.

Step 7. Для передачи файлов с устройства Prestige на Ваш компьютер, используйте команду "put", например, "put config.rom rom-0". Эта команда передает файл конфигурации "config.rom", находящийся на устройстве Prestige на Ваш компьютер. Более подробно о соглашении по именам файлов, см. выше в данной главе.

Step 8. Для выхода из режима FTP, введите команду "quit". После удачного завершения процесса восстановления, устройство Prestige автоматически перезагрузится.

36.3.2 Пример восстановления при помощи 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. 36-4 Пример восстановления при помощи сеанса FTP

В разделе 36.2.5 указаны параметры конфигурации, при которых работа протоколов TFTP и FTP в глобальной вычислительной сети невозможна.

36.4 Выгрузка микропрограммного обеспечения и файлов конфигурации

В данном разделе описывается, как выгрузить файлы микропрограммного обеспечения и файлы конфигурации. Выгрузить файлы конфигурации можно следуя указаниям, изложенным в предыдущем разделе — *Восстановление конфигурации*, либо следуя инструкциям, находящимся в

Меню 24.7.2 – System Maintenance (Сопровождение системы) – Upload System Configuration File (Выгрузка файла конфигурации системы).

ПРЕДУПРЕЖДЕНИЕ!
НЕ ПРЕРЫВАЙТЕ ПРОЦЕСС ПЕРЕДАЧИ ФАЙЛА, ПОСКОЛЬКУ ЭТО МОЖЕТ ПРИВЕСТИ К ПОЛНОМУ ВЫХОДУ ИЗ СТРОЯ УСТРОЙСТВА PRESTIGE.

36.4.1 Выгрузка файла микропрограммного обеспечения

Предпочтительным методом выгрузки файлов микропрограммного обеспечения и файлов конфигурации является FTP. Для того, чтобы им воспользоваться, на Вашем компьютере должен быть установлен FTP-клиент.

При установке связи с устройством Prestige через сетевой теледоступ (telnet), открываются следующие окна, позволяющие выгрузить микропрограммное обеспечение и файлы конфигурации по протоколу FTP.

Рис. 36-5 Сетевой теледоступ к Меню 24.7.1 Выгрузка микропрограммного

```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

 To upload the system firmware, follow the procedure below:

   1. Launch the FTP client on your workstation.
   2. Type "open" and the IP address of your system. Then type "root" and
      SMT password as requested.
   3. Type "put firmware filename ras" where "firmwarefilename" is the name
      of your firmware upgrade file on your workstation and "ras" is the
      remote file name on the system.
   4. The system reboots automatically after a successful firmware upload.

 For details on FTP commands, please consult the documentation of your FTP
```

обеспечения системы

36.4.2 Выгрузка файла конфигурации

При установлении связи с меню 24.7.2. при помощи сетевого теледоступа, открывается следующее

```
      Menu 24.7.2 - System Maintenance - Upload System Configuration File

 To upload the system configuration file, follow the procedure below:

   1. Launch the FTP client on your workstation.
   2. Type "open" and the IP address of your system. Then type "root" and
      SMT password as requested.
   3. Type "put configuration filename rom-0" where "configurationfilename"
      is the name of your system configuration file on your workstation, which
      will be transferred to the "rom-0" file on the system.
   4. The system reboots automatically after the upload system configuration
      file process is complete.
```

окно.

Рис. 36-6 Сетевой теледоступ к Меню 24.7.2 Сопровождение системы

Для выгрузки микропрограммного обеспечения и файлов конфигурации выполните действия, указанные в данных примерах

36.4.3 Пример команды выгрузки файла FTP из подсказки DOS

Step 1. Запустите клиента FTP на вашем компьютере.

Step 2. Введите команду "open", а затем — IP-адрес устройства Prestige через пробел.

Step 3. В диалоговом окне введите имя пользователя и нажмите клавишу [ENTER] .

Step 4. В окне запроса введите пароль (по умолчанию "1234").

Step 5. Введите команду "bin" для того, чтобы установить двоичный режим передачи.

Step 6. Для передачи файлов с Вашего компьютера на устройство Prestige, используйте команду "put", например, "put firmware.bin ras". Эта команда передает микропрограммное обеспечение (firmware.bin) с Вашего компьютера на устройство Prestige и переименовывает его в "ras". Точно также, команда "put config.rom rom-0" передает файл конфигурации (config.rom) с Вашего компьютера на устройство Prestige и переименовывает его в "rom-0". Так же команда "get rom-0 config.rom" передает файл конфигурации с устройства Prestige на Ваш компьютер и переименовывает его в "config.rom." Более подробно о соглашении по именам файлов, см. выше в данной главе.

Step 7. Для выхода из режима FTP, введите команду "quit".

После успешного завершения процесса загрузки файла, устройство Prestige автоматически перезагрузится.

36.4.4 Пример сеанса FTP по выгрузке файла микропрограммного обеспечения

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
```

Рис. 36-7 Пример сеанса FTP по выгрузке файла микропрограммного обеспечения

Другие команды описаны выше в данной главе, в разделе, посвященном клиентам FTP, созданным на основе графического пользовательского интерфейса.

В разделе 36.2.5 указаны параметры конфигурации, при которых работа протоколов TFTP и FTP в глобальной вычислительной сети невозможна.

36.4.5 Выгрузка файлов по протоколу TFTP

Устройство Prestige также поддерживает функцию выгрузки микропрограммного обеспечения по протоколу TFTP (Упрощенный протокол передачи файлов) по локальной вычислительной сети (LAN). Однако использовать протокол TFTP для работы по глобальной вычислительной сети (WAN) не рекомендуется.

Для того, чтобы использовать протокол TFTP, на Вашем компьютере должны быть установлены и клиент Telnet, и TFTP клиент. Для передачи микропрограммного обеспечения и файла конфигурации, выполните описанную ниже процедуру.

Step 1. При помощи сетевого теледоступа (Telnet), установленного на Вашем компьютере, подключитесь к устройству Prestige и зарегистрируйтесь. Поскольку протокол TFTP не обладает функциями проверки для защиты информации, Prestige записывает IP-адрес клиента Telnet и принимает запросы TFTP только с этого адреса.

Step 2. Переключите системную консоль (SMT) в режим командного процессора. Для этого, в **Меню 24 – System Maintenance (Сопровождение системы)** введите цифру 8.

Step 3. Для отключения интервала простоя консоли, введите команду "sys stdio 0". При этом, передача данных по протоколу TFTP не прервется. По окончании передачи файла, для восстановления 5-минутного интервала простоя консоли (значение, устанавливаемое по умолчанию), введите команду "sys stdio 5".

Step 4. Запустите на Вашем компьютере клиента TFTP и подключитесь к устройству Prestige. Прежде чем начать процесс передачи данных, установите двоичный режим передачи.

Step 5. Для передачи файлов между устройством Prestige и компьютером, используйте клиента TFTP (см. пример ниже). Имя файла микропрограммного обеспечения — "ras".

Следует помнить, что подключение через Telnet должно быть активно, а устройство Prestige должно находиться в режиме командного процессора (CI mode) как до, так и во время передачи по протоколу TFTP. Более подробно о командах TFTP (см. следующий пример) можно узнать в сопроводительной документации к клиентской программе TFTP. Если Вы работаете в системе UNIX, то команду "get" используйте для передачи файлов с устройства Prestige на компьютер, команду "put", наоборот, для передачи файлов с компьютера на устройство Prestige, а команду "binary" — для установки двоичного режима передачи данных.

36.4.6 Пример команды выгрузки по протоколу TFTP

Ниже приводится пример команды TFTP:

```
tftp [-i] host put firmware.bin ras
```

Где "i" указывает на двоичный режим передачи (этот режим используется для передачи двоичных файлов), "host" — IP-адрес устройства Prestige, а "put" — команда передачи файла, находящегося на компьютере ("firmware.bin" — имя файла микропрограммного обеспечения, находящегося на компьютере), на удаленный хост ("ras" — имя микропрограммного обеспечения, находящегося на устройстве Prestige).

Перечень команд, которые вы можете увидеть на клиентах TFTP, созданных на основе графического пользовательского интерфейса, представлен выше, в данной главе.

Раздел 37
Сопровождение системы

В этой главе описываются пункты меню SMT от 24.8 до 24.10.

37.1 Режим командного процессора

Командный процессор (CI) является основным микропрограммным обеспечением системы. Командный процессор обеспечивает весь набор функциональных возможностей, что и системная консоль (SMT), а также, дополнительно, некоторые функции настроек нижнего уровня и функции диагностики. Для того, чтобы войти в командный процессор, в системной консоли выберите меню 24.8. Более подробно о командах командного процессора см. прилагаемый диск web-сайта zyxel.com. В **Меню 24 — System Maintenance (Сопровождение системы)** введите цифру 8. Для того, чтобы отобразить (чтобы вернуться в

```
                        Menu 24 - System Maintenance


                        1.  System Status
                        2.  System Information and Console Port
Speed
                        3.  Log and Trace
                        4.  Diagnostic
                        5.  Backup Configuration
                        6.  Restore Configuration
                        7.  Upload Firmware
```

Рис. 37-1 Командный режим в Меню 24

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            ether           wan
```

Рис. 37-2 Доступные команды

37.2 Поддержка управления вызовами

Поддержка управления вызовами может быть использована только, если в меню 4 или в меню 11 установлена **Encapsulation (Инкапсуляция)** на протокол **PPPoE**.

Функция бюджетирования позволяет установить на устройстве Prestige ограничение на общую продолжительность исходящего вызова в определенное время суток. При превышении установленного общего лимита времени исходящих вызовов, текущий вызов сбрасывается, а последующие вызовы блокируются.

Для того, чтобы получить доступ к меню управления вызовами, в меню 24 выберите опцию 9 и войдите в **Меню 24.9 — System Maintenance (Сопровождение системы) — Call Control (Управление вызовами)**, как показано в таблице ниже.

```
                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 отображается бюджетная статистика по исходящим вызовам. В **Меню 24.9 — System Maintenance (Сопровождение системы) — Call Control (Управление вызовами)** введите цифру 1 для того, чтобы открылось следующее меню.

```
                Menu 24.9.1 - System Maintenance - Budget Management

  Remote Node          Connection Time/Total Budget      Elapsed Time/Total Period
 1.MyIsp                        No Budget                        No Budget
 2.--------                        ---                              ---
 3.--------                        ---                              ---
 4.--------                        ---                              ---
 5.--------                        ---                              ---
 6.--------                        ---                              ---
 7.--------                        ---                              ---
 8.--------                        ---                              ---

                        Reset Node (0 to update screen):
```

Рис. 37-4 Меню 24.9.1 Сопровождение системы: Бюджетирование

Общий бюджет представляет собой ограничение по общему количеству времени, отведенного для исходящих вызовов на удаленный узел. Если лимит времени исчерпан, то текущий вызов сбрасывается, а последующие исходящие вызовы на данный удаленный узел будут блокированы. Всякий раз, по прошествии определенного периода времени, общий бюджет открывается вновь. По умолчанию устанавливается общей бюджет равный 0 минутам и период времени равный 0 часам. Это означает, что управление бюджетом не производится. Для того, чтобы сбросить значение суммарного времени соединения, введите в данном меню индекс удаленного узла. Для того, чтобы обновить показания данного окна, введите цифру 0. Установка параметров конфигурации бюджета и периода сброса для удаленного узла производится в меню 11.1, при условии, что выбрана опция инкапсуляции PPPoE.

Табл. 37-1 Меню 24.9.1 Сопровождение системы: Бюджетирование

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Remote Node (Удаленный узел)	Введите в это поле индекс удаленного узла, который Вы хотите сбросить (в данном случае один)	1
Connection Time/Total Budget (Время соединения/Общий бюджет)	В этом поле отображается общая продолжительность времени соединения в рамках бюджета, установленного в меню 11.1.	5/10 означает, что истрачено 5 минут из 10 отведенных.
Elapsed Time/Total Period (Использованное время/Общий период)	Период — это продолжительность цикла в часах, по истечении которого происходит сброс установленного бюджета (см. меню 11.1.) Использованное время — это время, использованное в рамках этого периода.	0,5/1 означает, что 30 минут из отведенного периода в 1 час уже использовано.

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Для того, чтобы обновить информацию в данном окне введите цифру 0, либо нажмите клавишу [ESC] для того, чтобы вернуться к предыдущей экранной форме.		

37.3 Установка времени суток и даты

Устройство Prestige проводит отслеживание даты и времени. Имеется также программный механизм для установки даты и времени суток вручную, либо получения этих данных с внешнего сервера при включении устройства Prestige. Обновление настроек даты и времени Prestige осуществляется в Меню 24.10. После обновления, в журнале регистрации ошибок и в журнале межсетевого экрана устройства Prestige отображается реальное время суток.

Для того, чтобы открыть **Меню 24 System Maintenance (Сопровождение системы)** см. ниже, в главном меню выберите опцию 24.

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information
3.  Log and Trace
4.  Диагностика
5.  Backup Configuration
6.  Restore Configuration
7.  Upload Firmware
8.  Command Interpreter Mode
9.  Call Control
10. Time and Date Setting
11. Дистанционное управление

Enter Menu Selection Number:
```

Рис. 37-5 Меню 24 Сопровождение системы

Затем наберите цифру 10 для того, чтобы перейти в **Меню 24.10 System Maintenance (Сопровождение системы) Time and Date Setting (Установка времени суток и даты).** В этом

```
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
```

меню можно обновить настройки времени суток и даты на устройстве Prestige, как показано на рисунке ниже.

Рис. 37-6 Меню 24.10 Сопровождение системы: Установка времени суток и даты

Табл. 37-2 Меню 24.10 Сопровождение системы: Установка времени суток и даты

ПОЛЕ	ОПИСАНИЕ
Use Time Server when Bootup (При загрузке использовать сервер времени)	Введите сервисный протокол времени, который сервер времени передает при включении устройства Prestige. Не все серверы времени поддерживают все протоколы, поэтому для того, чтобы установить протокол, который действительно работает, Вам, возможно, потребуется консультация Интернет-провайдера или сетевого администратора, либо воспользуйтесь методом проб и ошибок. Основным отличием протоколов является их формат. **Daytime (RFC 867):** день/месяц/год/часовой пояс сервера. **Time (RFC-868):** 4-байтовое целое число, обозначающее общее количество секунд, прошедших с 1970/1/1 с 0:0:0. **NTP (RFC-1305):** формат, схожий с форматом **Time (RFC-868)**. **None (Никакой).** Формат, устанавливаемый по умолчанию, дата и время выставляются вручную.
Time Server Address (Адрес сервера времени)	Введите IP-адрес или имя домена, в котором находится сервер времени. Если Вы не уверены в правильности имеющейся у Вас информации, то уточните ее у Интернет-провайдера или у сетевого администратора.
Current Time (Текущее время)	В этом поле отображается обновленное время суток при каждом повторном открытии данного меню.
New Time (Новое время)	Введите новое время в формате: часы, минуты, секунды.
Current Date (Текущая дата)	В этом поле отображается обновленная дата при каждом повторном открытии данного меню.
New Date (Новая дата)	Введите новую дату в формате: год, месяц, день.
Time Zone (Часовой пояс)	Клавишей [ПРОБЕЛ] установите разницу между Вашим часовым поясом и временем по Гринвичу (GMT) и нажмите клавишу [ENTER].
Daylight Saving (Переход на летний период)	Если в Вашем регионе практикуется переход с зимнего времени на летнее и наоборот, выберите опцию **Yes (ДА)**.
Start Date (Начальная дата)	При использовании перехода на летнее время, введите месяц и день, с которого он начинается.
End Date (Дата окончания)	При использовании перехода на летнее время, введите месяц и день, когда он заканчивается.
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.	

37.3.1 Сброс показаний времени

Устройство Prestige сбрасывает показания времени в трех случаях:

i. При выходе из меню 24.10 после внесения изменений.

ii. При запуске устройства Prestige, если имеется сервер времени, параметры которого указаны в меню 24.10.

iii. По истечение каждых 24 часов после запуска устройства.

Раздел 38
Дистанционное управление

В данной главе описываются функции дистанционного управления (меню SMT 24.11).

38.1 Описание дистанционного управления

При помощи дистанционного управления можно определить, какие службы/протоколы могут иметь доступ, к какому интерфейсу устройства Prestige и через какие компьютеры.

При установке параметров конфигурации дистанционного управления, предназначенного для выполнения функций управления через глобальную вычислительную сеть (WAN), необходимо также установить параметры правила межсетевого экрана для получения доступа. Более подробно о настройках правил межсетевого экрана см. главы, посвященные межсетевому экрану.

38.2 Дистанционное управление

Для того, чтобы отключить функцию дистанционного управления, выберите опцию **Disable (Отключит)** в соответствующем поле **Server Access (Доступ к серверу)**.

Для того, чтобы открыть **Меню 24.11 — Remote Management Control (Управление удаленным доступом),** в меню 24 наберите цифру 11.

38.2.1 Настройка межсетевого экрана

Управление устройством Prestige можно осуществлять через удаленный адрес. Для этого предусмотрены следующие опции:

через Интернет (**WAN only (Только по ГВС)**), **LAN only (Только по ЛВС)**, **All (Все)** (ЛВС и ГВС) и **Disable (Отключить)** (дистанционное управление отключено).

- WAN only (Только через ГВС) (Интернет)
- LAN only (Только по ЛВС)
- ALL (Все)(ГВС и ЛВС)
- Disable (Отключено) (дистанционное

управление отключено)

Если при включенной функции дистанционного управления задействован фильтр, блокирующий данный сервис, то осуществление дистанционного управления становится невозможным.

Для того, чтобы открыть **Меню 24.11 — Remote Management Control (Управление удаленным доступом)** (см. ниже)**,** в меню 24 наберите цифру 11.

```
            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
```

Рис. 38-1 Меню 24.11 Управление удаленным доступом

В таблице ниже приводятся описания полей данного меню.

Табл.38-1 Меню 24.11 Управление удаленным доступом

ПОЛЕ	ОПМСАНИЕ	ПРИМЕР
Telnet Server FTP Server Web Server (Сервер Telnet, сервер FTP, Web-сервер)	Каждая из этих надписей, доступных только для чтения, обозначает соответствующий сервис или протокол.	

Табл.38-1 Меню 24.11 Управление удаленным доступом

ПОЛЕ	ОПМСАНИЕ	ПРИМЕР
Port (Порт)	В этом поле отображается номер порта сервиса или протокола. При необходимости, номер порта можно изменить, но для получения доступа к устройству Prestige, необходимо, что бы номер порта был один и тот же.	23
access (доступ)	При помощи клавиши [ПРОБЕЛ] выберите интерфейс доступа, если таковые имеются. Опциями являются: **LAN only (Только ЛВС)**, **WAN only (Только ГВС)**, **All (Все)** или **Disable (Отключить)**. По умолчанию устанавливается опция **LAN only (Только ЛВС)**.	**LAN only (Только по ЛВС)**
Secured Client IP (IP-адрес защищенного клиента)	По умолчанию устанавливается адрес 0.0.0.0, который позволяет любому клиенту получить доступ к устройству Prestige. Для того, чтобы ограничить доступ к устройству, введите IP-адрес клиента, которому доступ разрешен.	0.0.0.0
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.		

38.2.2 Ограничения дистанционного управления

Дистанционное управление через ЛВС (LAN) или ГВС (WAN) невозможно, если:

6. В меню 3.1 (ЛВС) или в меню 11.5 (ГВС) установлен фильтр, блокирующий подключение через Telnet, FTP или Web.
7. Услуга подключения через Telnet отключена в меню 24.11.
8. IP-адрес, указанный в поле **Secured Client IP (IP-адрес защищенного клиента)** (меню24.11), не соответствует IP-адресу клиента. В этом случае устройство Prestige немедленно прерывает сеанс связи.
9. Запущен другой сеанс связи дистанционного управления, имеющий такой же или более высокий приоритет. Единовременно допускается только один сеанс связи дистанционного управления.
10. Имеется правило межсетевого экрана, блокирующее дистанционное управление.

38.3 Дистанционное управление и трансляция сетевых адресов (NAT)

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

- При конфигурировании через глобальную сеть, используйте IP-адрес устройства Prestige в глобальной сети (WAN).
- При конфигурировании через локальную сеть, используйте IP-адрес устройства Prestige в локальной сети (LAN).

38.4 Системная задержка

По умолчанию время простоя управлением системой равно пяти минутам (триста секунд). Устройство Prestige автоматически отключает Вас от системы, если время простоя сеанса связи по управлению системой превышает указанный период времени. Если периодически обновлять информацию о статусе в меню 24.1. или если `sys stdio` изменить в командной строке, то сеанс связи управления будет поддерживаться постоянно.

Раздел 39
Маршрутизация на базе стратегии IP

В данной главе описываются настройки и применение стратегий маршрутизации IP.

39.1 Обзор маршрутизации на базе стратегии IP

Традиционно, в основе маршрутизации лежит следующее: используется только адрес назначения, а IAD находит кратчайший путь для пересылки пакета. Стратегия маршрутизации IP (IPPR) содержит механизм, позволяющий игнорировать схему маршрутизации, установленную по умолчанию, и изменить способ пересылки пакетов согласно стратегии, установленной сетевым администратором. Маршрутизация на базе стратегии применяется в отношение входящих пакетов для каждого интерфейса и имеет более высокий приоритет, нежели стандартная маршрутизация.

39.2 Преимущества маршрутизации на базе стратегии IP

- Маршрутизация на базе источника – сетевые администраторы могут использовать маршрутизацию на базе стратегии для того, чтобы направлять потоки данных различных пользователей по различным схемам подключения.
- Качество услуги (QoS) – компании могут дифференцировать трафик посредством установления значений очередности или типа услуги (TOS) в заголовке IP на периферии сети. Это позволяет магистрали располагать трафик в соответствии с приоритетом.
- Сокращение расходов – IPPR (маршрутизация на базе стратегии IP) позволяет компаниям распределять интерактивный трафик по каналам с высокой пропускной способностью, по дорогостоящим путям и при этом использовать недорогие пути для пакетного трафика.
- Распределение нагрузки– сетевые администраторы могут использовать маршрутизацию на базе стратегии IP (IPPR) для распределения трафика по нескольким путям.

39.3 Стратегия маршрутизации

Отдельные стратегии маршрутизации используются как часть единого процесса маршрутизации на базе стратегии IP. Стратегия предусматривает наличие определенных критерий соответствия и действия, предпринимаемые при соответствии пакета этим критериям. Предусмотренное действие предпринимается только в том случае, если пакет соответствует всем критериям. К критериям относятся: адрес и порт источника, протокол IP (ICMP, UDP, TCP, и т. д.), адрес и порт назначения,

тип услуги (TOS) и очередность (поля в заголовке IP header), а также длина. Критерий длины используется для разделения интерактивных трафиков и трафиков массивов данных. Интерактивные приложения, например Telnet, обычно имеют короткие пакеты, а трафики массивов данных, например, передача файлов, — длинные пакеты.

К предпринимаемым действиям относятся:

- маршрутизация пакета на другой шлюз (следовательно — на исходящий интерфейс).
- настройка полей типа услуги (TOS) и очередности в заголовке IP.

Маршрутизация на базе стратегии IP (IPPR) выполняется после фильтрации пакетов сервиса удаленного доступа (RAS), как по стилю, таки и по реализации. Стратегии подразделяются на группы, объединяющие родственные стратегии. Пользователь определяет стратегии до того, как применить их на интерфейсе или на удаленном узле, точно также, как это делается с фильтрами. Существует 12 наборов стратегий, каждый из которых содержит по шесть стратегий.

39.4 Настройка стратегии маршрутизации IP

В меню 25 отражены все установленные 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      ________________
```

Рис. 39-1 Меню 25 Настройка стратегии маршрутизации IP

Для того, чтобы настроить стратегию маршрутизации, выполните следующие действия:

Step 1. Откройте **Меню 25 – IP Routing Policy Setup (Настройка стратегии маршрутизации IP).** Для этого, в главном меню наберите цифру 25**.**

Step 2. Откройте **Меню 25.1 – IP Routing Policy Setup (Настройка стратегии маршрутизации IP)**. Для этого, наберите индекс набора стратегий, который Вы намерены сконфигурировать.

В меню 25.1 отображается сводка набора стратегий, включая критерии и действия отдельной стратегии, а также информацию о том, активна данная стратегия или нет. В каждой стратегии имеются две строки. Первая строка представляет собой критерий для входящего пакета, а вторая — действие. Между этими двумя частями располагается разделитель: разделитель "|" означает, что действие предпринимается в случае, когда пакет соответствует критериям, а разделитель "=" означает, что действие предпринимается в случае, когда пакет не соответствует критериям.

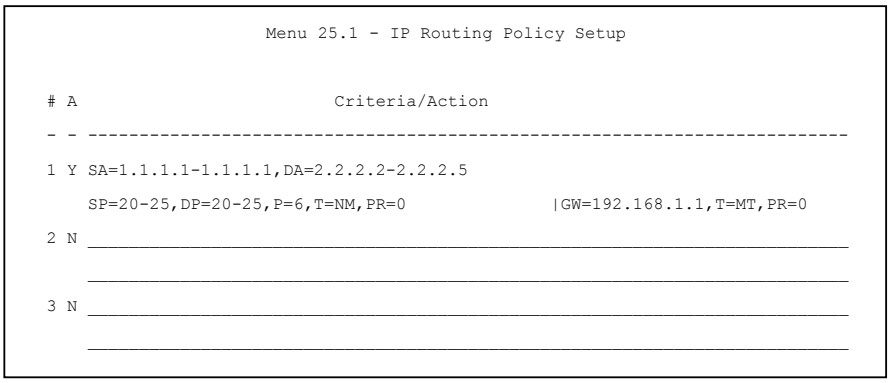


Рис. 39-2 Меню 25.1 Настройка стратегии маршрутизации IP

ТАБЛ. 39-1 МЕНЮ 25.1 НАСТРОЙКА СТРАТЕГИИ МАРШРУТИЗАЦИИ IP

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
Criterion (Критерий) SA	IP-адрес источника
SP	Порт источника
DA	IP-адрес назначения
DP	Порт назначения
P	Уровень IP — 4, номер протокола (TCP=6,

ТАБЛ. 39-1 МЕНЮ 25.1 НАСТРОЙКА СТРАТЕГИИ МАРШРУТИЗАЦИИ IP

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
	UDP=17…)
T	Тип услуги входящего пакета
PR	Очередность входящих пакетов
Action (Действие) GW	IP-адрес шлюза
T	Тип исходящей услуги
P	Очередность исходящих пакетов
Service (Сервис) NM	Стандартный
MD	Минимальная задержка
MT	Максимальная пропускная способность
MR	Максимальная надежность
MC	Минимальная стоимость

Для того, чтобы открыть **Меню 25.1.1 – IP Routing Policy (Стратегия маршрутизации IP)** (см. рисунок ниже), наберите цифру от 1 до 6. В этом меню можно сконфигурировать правило 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:
```

Рис. 39-3 Меню 25.1.1 Стратегия маршрутизации IP

В таблице ниже приводятся описания полей данного меню.

Табл. 39-2 Меню 25.1.1 Стратегия маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
Policy Set Name (Имя набора стратегий)	В этом поле отображается имя набора стратегий, установленное в **Меню 25 – Настройка стратегии маршрутизации IP**.
Active (Активно)	Для того, чтобы активировать или отключить стратегию, клавишей [ПРОБЕЛ] выберите опцию **Yes (Да)** или **No (Нет)** соответственно и нажмите клавишу [ENTER]. Неактивные стратегии в меню SMT 25 обозначены знаком минус"-".
Criteria (Критерии)	
IP Protocol (Протокол IP)	В этом поле отображается протокол 4 уровня IP, например: **UDP**, **TCP**, **ICMP** и т. д.).
Type of Service (Тип услуги)	Установите уровень приоритета для входящего сетевого трафика. Опциями являются: **Don't Care (Не обращать внимание)**, **Normal (Стандартный)**, **Min Delay (Минимальная задержка)**, **Max Thruput (Максимальная пропускная способность), Min Cost (Минимальная стоимость)** или **Max Reliable**

Табл. 39-2 Меню 25.1.1 Стратегия маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
	(Максимальная надежность).
Precedence (Очередность)	В этом поле отображается положение в очереди входящего пакета. Для того, чтобы установить очередность пакета, клавишей [ПРОБЕЛ] выберите значение (цифры от 0 до 7, либо **Don't Care (Не обращать внимание))** и нажмите клавишу [ENTER].
Packet Length (Длина пакета)	Введите в это поле значение длины входящих пакетов (в байтах). Операторы **Len Comp** (см. следующее поле) будут обрабатывать пакеты указанной длины.
Len Comp	Клавишей [ПРОБЕЛ] выберите оператора и нажмите клавишу [ENTER]. Опциями являются: **Equal (Равно)**, **Not Equal (Не равно)**, **Less (Меньше)**, **Greater (Больше)**, **Less or Equal (Меньше или равно)** или **Greater or Equal (Больше или равно)**.
Source (Источник):	
addr start / end	Диапазон IP-адресов источника: от первого до последнего.
port start / end	Диапазон номеров порта источника: от первого до последнего. Применяется только для протоколов TCP/UDP.
Destination (Адрес назначения):	
addr start / end	Диапазон IP-адресов пункта назначения: от первого до последнего.
port start / end	Диапазон номеров порта назначения: от первого до последнего. Применяется только для протоколов TCP/UDP.
Action (Действие)	В этом поле указывается, когда должно предприниматься действие: при **соответствии** критериям или при **несоответствии** критериям.
Gateway addr (Адрес шлюза)	В этом поле указывается адрес исходящего шлюза. Если шлюз находится в локальной сети, то он должен находиться в той же подсети, что и устройство Prestige. В противном случае, в качестве адреса IP-шлюза используется адрес удаленного узла. В качестве шлюза по умолчанию задано 0.0.0.0.
Type of Service (Тип услуги)	Установите новое значение TOS исходящего пакета. Установите уровень приоритета для входящего сетевого трафика. Опциями являются: **No Change (Без изменений)**, **Normal (Стандартный)**, **Min Delay (Минимальная задержка)**, **Max Thruput (Максимальная пропускная способность)**, **Max Reliable (Максимальная надежность)** или **Min Cost (Минимальная стоимость)**.
Precedence (Очередность)	Установите новое значение очередности исходящего пакета. Опциями являются: цифры от 0 до 7 или **No Change (Без изменений)**.

Табл. 39-2 Меню 25.1.1 Стратегия маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
Log (Регистрационный журнал)	Если стратегия активирована, то для внесения записи в регистрационный журнал, клавишей [ПРОБЕЛ] выберите опцию **Yes (Да)** и затем нажмите клавишу [ENTER].
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.	

39.5 Применение стратегии IP

В данном разделе описываются области приложения стратегий IP после их создания.

39.5.1 Стратегии IP Ethernet

Откройте **Меню 3.2 — TCP/IP and DHCP Ethernet Setup (Настройка TCP/IP и DHCP для Ethernet).** Для этого, в **Меню 3 — Ethernet Setup (Настройка Ethernet)**, наберите цифру 2.

Вы можете выбрать до четырех наборов стратегий IP из 12. Для этого, нужно ввести номера стратегий, отделяя их запятыми, например: 2, 4, 7, 9.

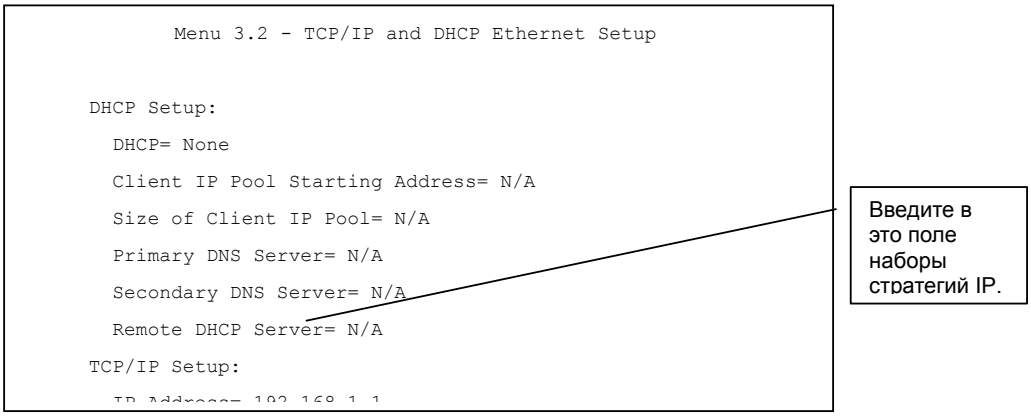


Рис. 39-4 Меню 3.2 Настройка TCP/IP и DHCP для Ethernet

Откройте меню 11.3 (см. ниже) и введите номер(а) соответствующего(их) набора(ов) стратегий маршрутизации IP. Можно последовательно задать не более четырех наборов стратегий. Номера наборов стратегий вводятся через запятую.

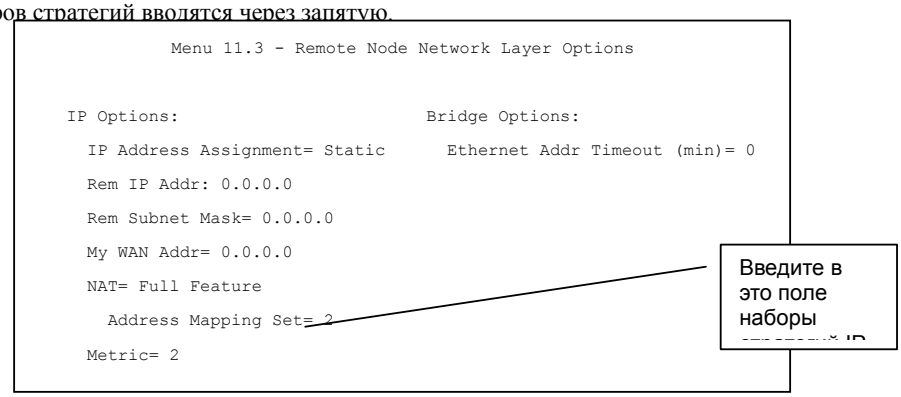


Рис. 39-5 Меню 11.3 Параметры сетевого уровня для удаленного узла

39.6 Пример маршрутизации на базе стратегии IP

Если у есть и подключение к Интернет, и подключение к удаленному узлу, то Вы можете направлять Web-пакеты в Интернет при помощи одной стратегии, а пакеты FTP — на удаленную сеть при помощи другой стратегии. См. рисунок ниже.

Маршрут 1 является установленным по умолчанию IP маршрутом, а маршрут 2 — сконфигурированным IP маршрутом.

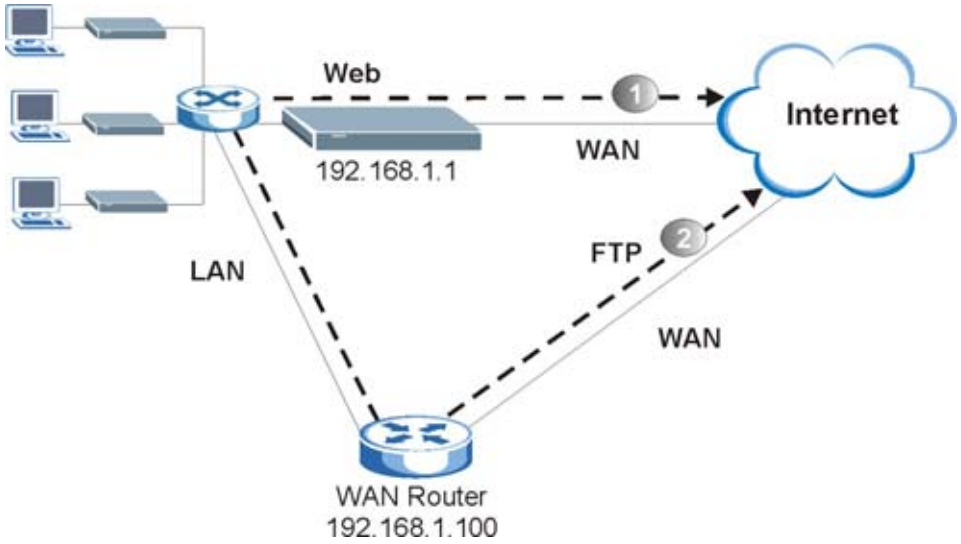


Рис. 39-6 Пример маршрутизации на базе стратегии IP

Для того, чтобы направить Web-пакеты, поступающие от клиентов, имеющих следующие IP-адреса: от 192.168.1.33 до 192.168.1.64, в Интернет через порт WAN устройства Prestige, выполните следующие действия:

Step 1. В меню 25 создайте набор стратегий маршрутизации.

Step 2. В **Меню 25.1.1 — IP Routing Policy (Стратегия маршрутизации IP)** создайте правило для этого набора, как показано ниже.

```
                    Menu 25.1.1 - IP Routing Policy

Policy Set Name= set1
Active= Yes
Criteria:
  IP Protocol    = 6
  Type of Service= Don't Care    Packet length= 10
  Precedence     = Don't Care      Len Comp= N/A
  Source:
    addr start= 192.168.1.33     end= 192.168.1.64
    port start= 0                end= N/A
  Destination:
```

Рис. 39-7 Пример стратегии маршрутизации IP

Step 3. Проверьте в **Меню 25.1 — IP Routing Policy Setup (Настройка стратегии маршрутизации IP),** что правило добавлено правильно.

Step 4. В меню 25 создайте другой набор стратегий маршрутизации.

Step 5. В меню 25.1 создайте правило для данного набора, согласно которому, можно было бы направлять пакеты, поступающие с любого хоста (IP=0.0.0.0 означает любой хост) по протоколу TCP и порт FTP, через другой шлюз (192.168.1.100).

```
                Menu 25.1.1 - IP Routing Policy

Policy Set Name= set2
Active= Yes
Criteria:
  IP Protocol    = 6
  Type of Service= Don't Care      Packet length= 10
  Precedence     = Don't Care        Len Comp= N/A
  Source:
    addr start= 0.0.0.0            end= N/A
    port start= 0                  end= N/A
  Destination:
```

Рис. 39-8 Пример стратегии маршрутизации IP

Step 6. Проверьте в **Меню 25.1 — IP Routing Policy Setup (Настройка стратегии маршрутизации IP),** что правило добавлено правильно**.**

Step 7. Установите оба набора стратегий в меню 3.2 так, 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
```

Рис. 39-9 Применение стратегий IP Пример

Раздел 40
Расписание связи

Расписание связи (применяется только для инкапсуляции PPPoA или PPPoE) позволяет определять, когда следует устанавливать связь с удаленным узлом и на какой период времени.

40.1 Введение

Функция составления расписания связи позволяет устройству Prestige управлять удаленным узлом и определять, когда следует устанавливать связь с удаленным узлом и на какой период времени. Эта функция схожа с функцией расписания, имеющейся у видеомагнитофона, где пользователь может установить период времени, в течение которого видеомагнитофон должен произвести запись. Вы можете установить до 4 наборов расписаний в **Меню11.1 — Remote Node Profile (Настройки**

```
                        Menu 26 - Schedule Setup

Schedule                                  Schedule
 Set #          Name                      Set #          Name
------   ------------------               ------   ------------------
  1       ________________                  7       ________________
  2       ________________                  8       ________________
  3       ________________                  9       ________________
  4       ________________                 10       ________________
  5       ________________                 11       ________________
  6       ________________                 12       ________________


                    Enter Schedule Set Number to Configure=


                    Edit Name=
```

пользователя для удаленного узла). Для того, чтобы открыть **Меню 26 — Schedule Setup (Настройка расписания вызовов)**, в главном меню введите цифру 26, как показано ниже.

Рис. 40-1 Меню 26 Настройка расписания вызовов

Чем ниже цифровое значение набора, тем большим приоритетом он обладает. Это позволяет избежать возникновение конфликтов среди расписаний вызовов. Например: если на удаленном узле установлены наборы 1, 2 ,3 и 4, то набор 1 имеет преимущество перед наборами 2, 3 и 4 потому, что устройство Prestige по умолчанию первым применяет набор, цифровое значение которого является наименьшим. Набор 2 имеет преимущество перед наборами 3 и 4, и так далее.

Вы можете создать до 12 наборов расписаний вызовов, но на одном удаленному узлу Вы можете установить не более четырех.

Для того, чтобы удалить набор расписаний вызовов, в поле Edit Name **(Редактировать имя) введите номер набора и нажмите клавишу [**ПРОБЕЛ**], а затем — клавишу [**ENTER**] (или delete).**

Для установки набора расписаний вызовов, откройте **Меню 26.1 — Schedule Set Setup (Установка набора расписаний вызовов)**, см. ниже. Для этого, в меню 26 (1-12) выберите набор, который вы

```
                        Menu 26.1 - Schedule Set Setup
                Active= Yes
                Start Date(yyyy/mm/dd) = 2000 - 01 - 01
                How Often= Once
                Once:
                  Date(yyyy/mm/dd)= 2000 - 01 - 01
                Weekdays:
                  Sunday= N/A
                  Monday= N/A
                  Tuesday= N/A
                  Wednesday= N/A
                  Thursday= N/A
                  Friday= N/A
                  Saturday= N/A
                Start Time (hh:mm)= 00 : 00
                Duration (hh:mm)= 00 : 00
                Action= Forced On

                          Press ENTER to Confirm or ESC to Cancel:
      Press Space Bar to Toggle
```

намерены установить и нажмите клавишу [ENTER] .

Рис. 40-2 Меню 26.1 Установка набора расписаний вызовов

Если соединение уже установлено, то устройство Prestige его не сбросит. Если соединение сброшено вручную или истекло его время, то инициировать заново удаленный узел можно только после окончания Продолжительности.

Табл. 40-1 Меню 26.1 Установка набора расписаний вызовов

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Active (Активно)	При помощи клавиши [ПРОБЕЛ] выберите одну из двух опций: **Yes (да)** или **No (Нет),** и нажмите клавишу [ENTER]. Опция Yes (Да) активирует набор расписаний, а опция No (Нет) — отключает.	**Yes (Да)**

Табл. 40-1 Меню 26.1 Установка набора расписаний вызовов

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Start Date (Начальная дата)	Введите дату начала реализации набора расписаний в формате год-месяц-день. Правильными датами считаются: с текущей даты до 5 февраля 2036 г.	2000-01-01
How Often (Как часто)	Данный набор расписаний должен повторяться еженедельно или предназначен для однократного использования? Клавишей [ПРОБЕЛ] выберите одну из опций: **Once (Однократно)** или **Weekly (Еженедельно)**, и нажмите клавишу [ENTER]. Обе эти опции являются взаимно исключающими. Если выбрана опция **Once (Однократно)**, то все остальные рабочие дни недели должны быть обозначены как **N/A (недоступно)**. При выборе опции **Once (однократно),** по истечении времени, установленного в расписании, правило расписания автоматически удаляется.	**Once (Однократно)**
Once (Однократно): Date (Дата)	При выборе опции **Once (однократно)** в поле **How Often (Как часто)**, см выше, необходимо указать дату в формате год-месяц-день, с которой активируется набор расписания.	2000-01-01
Weekday (Рабочий день): Day (день)	Если в поле **How Often (Как часто)** выбрана опция **Weekly (Еженедельно),** то необходимо указать день (дни), когда данный набор расписания должен активироваться (и повторяться). Для этого выберите день, затем клавишей [ПРОБЕЛ] выберите опцию **Yes (Да)** и нажмите клавишу [ENTER].	**Yes (Да)** **No (Нет)** **N/A (Недоступно)**
Start Time (Время начала)	Введите время начала реализации набора расписаний в формате часы-минуты.	09:00
Duration (Продолжительность)	Введите максимальную продолжительность, установленную для данного соединения в формате часы-минуты.	08:00

Табл. 40-1 Меню 26.1 Установка набора расписаний вызовов

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Action (Действие)	Опция **Forced On (Включен принудительно)** означает, что соединение сохраняется вне зависимости от того, имеется запрос на установление соединения или нет, и будет поддерживаться в течение всего периода времени, указанного в поле **Duration (Продолжительность)**. Опция **Forced Down (Отключен принудительно)** означает, что соединение блокируется вне зависимости от того, имеется на линии запрос на установление соединения, или нет. Опция **Enable Dial-On-Demand (Включить набор по требованию)** означает, что данное расписание допускает наличие в линии запроса на установление соединения. Опция **Disable Dial-On-Demand (Отключить набор по требованию)** означает, что данное расписание не допускает наличия на линии запроса на установление соединения.	**Forced On (Включен принудительно)**
По окончании заполнения параметров в данном меню, по запросу "Press ENTER to confirm or ESC to cancel" нажмите клавишу [ENTER] для того, чтобы сохранить конфигурацию, либо нажмите клавишу [ESC] для того, чтобы отменить изменения и вернуться к предыдущей экранной форме.		

По окончании конфигурирования наборов расписаний вызовов, их необходимо установить на выбранный удаленный узел (узлы). В главном меню наберите цифру 11, а затем введите индекс выбранного удаленного узла. Для того, чтобы поле наборов расписаний стало доступным, см. ниже, в поле **Encapsulation (Инкапсуляция)** при помощи клавиши [ПРОБЕЛ] выберите **PPPoE** или **PPPoA** и нажмите клавишу [ENTER] .

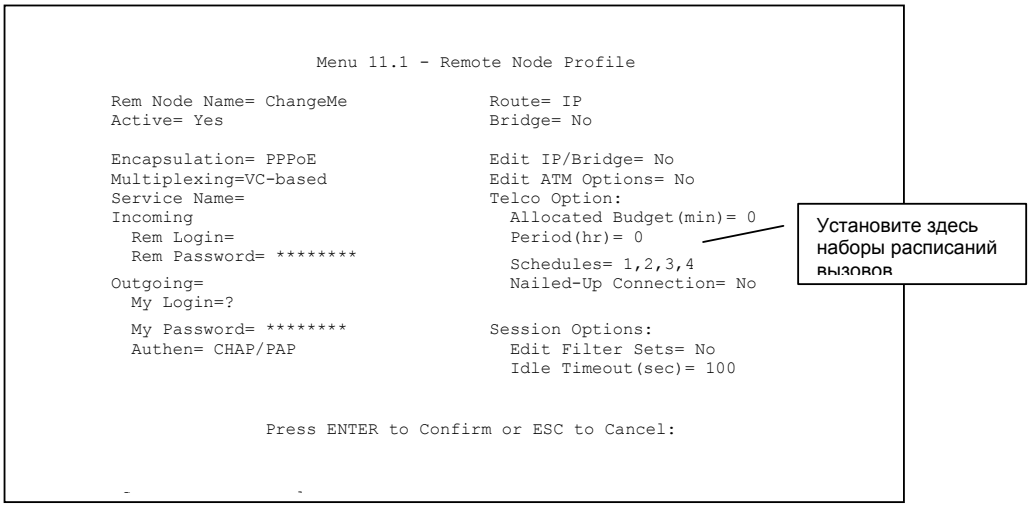


Рис. 40-3 Установка наборов расписаний на удаленном узле (PPPoE)

На одном удаленном узле допускается установка не более четырех наборов расписаний, вводимых через запятую. Измените номера набор расписаний в соответствии со своими предпочтениями.

Раздел 41
Внутренний генератор таблицы системных параметров (SPTGEN)

41.1 Описание внутреннего генератора таблицы системных параметров

Внутренний генератор таблицы системных параметров (SPTGEN) представляет собой текстовый файл конфигурации, используемый для эффективного конфигурирования нескольких устройств Prestiges. Внутренний генератор таблицы системных параметров (SPTGEN) позволяет устанавливать конфигурацию, сохранять и загружать множество меню одновременно при помощи одного текстового файла конфигурации, что исключает необходимость навигации и последовательного конфигурирования множества меню SMT для каждого устройства Prestige.

41.2 Формат текстового файла конфигурации

Все текстовые файлы внутреннего генератора таблицы системных параметров имеют схожий формат, а именно

<идентификационный номер поля = имя поля = допустимые значения параметра = вход>,

где <вход> — это вход, который точно соответствует <допустимым значениям параметра>.

На рисунке ниже приводится пример текстового файла внутреннего генератора таблицы системных параметров.

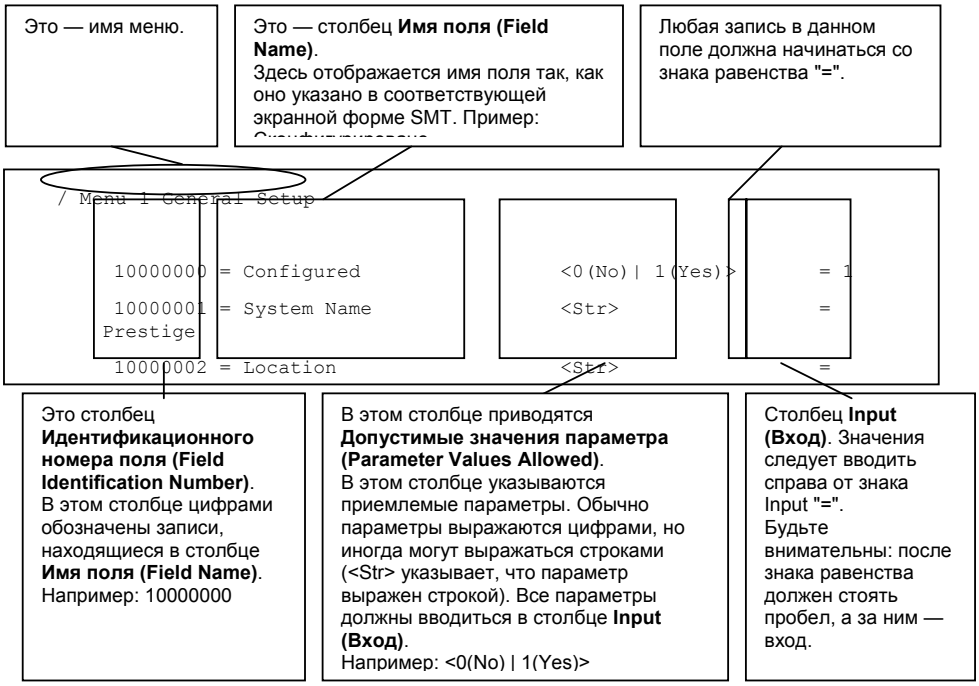


Рис. 41-1 Формат текстового файла конфигурации: Описания столбцов

НЕ ИЗМЕНЯЙТЕ И НЕ УДАЛЯЙТЕ никакие поля, за исключением значений параметров столбца Вход (Input)

Более подробно примеры текстовых файлов представлены в приложении "*Примеры экранных форм внутреннего генератора таблицы системных параметров (SPTGEN)"*.

41.2.1 Изменение файла внутреннего генератора таблицы системных параметров — то, что необходимо помнить

- Каждому вводимому параметру должны предшествовать один знак равенства "=" и один пробел.
- Некоторые параметры зависят от других. Например: если Вы отключаете поле **Configured (Сконфигурировано)** в меню 1 (см. *Рис. 41-1*), то необходимо отключить все поля в данном меню.

- Если в столбце **Input (Вход)** введен неверный параметр, то Prestige не сохранит параметры и в командной строке отобразится **Идентификационный номер поля** (**Field Identification Number)**. На рисунке *Рис. 41-2*, см. ниже, приводится пример того, что отображается на устройстве Prestige, если в столбце **Input (Вход) Идентификационного номера поля (Field Identification Number)** 1000000 вводится значение, отличное от "0" или "1" (см. *Рис. 41-1*).

```
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
```

Рис. 41-2 Введен неверный параметр: Пример командной строки

```
Please wait for the system to write SPT text file(ROM-
t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
```

При вводе верного параметра(ов), устройство Prestige отобразит следующую информацию.

Рис. 41-3 Введен верный параметр: Пример командной строки

41.3 Пример загрузки внутреннего генератора таблицы системных параметров по протоколу FTP

Рис. 41-4Пример загрузки внутреннего генератора таблицы системных параметров по протоколу FTP

Если файл "rom-t" сохранен на Вашем компьютере, то Вы можете его переименовать, но при его выгрузке на устройство Prestige он должен носить имя "rom-t".

41.4 Пример выгрузки внутреннего генератора таблицы системных параметров по протоколу FTP

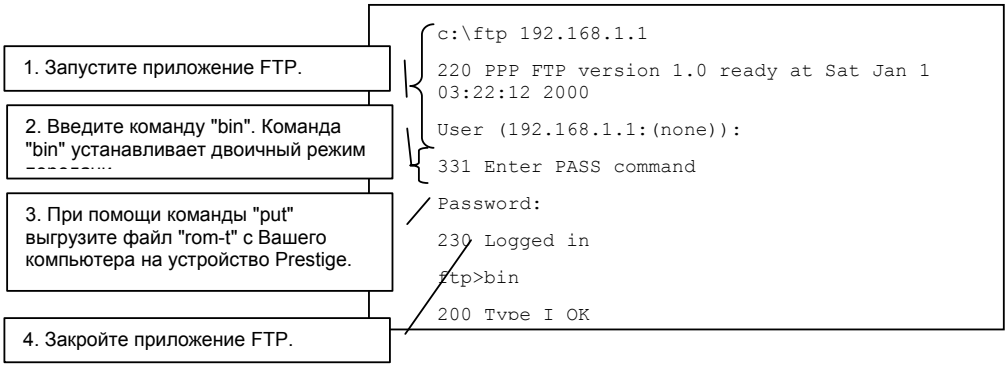


Рис. 41-5 Пример выгрузки внутреннего генератора таблицы системных параметров по протоколу FTP

Глава X:

Приложения и алфавитный указатель

В этой части содержится дополнительная информация и алфавитный указатель ключевых терминов.

Раздел 42
Устранение неисправностей

В данной главе рассматриваются потенциальные проблемы и способы их устранения.

Проблемы с запуском Prestige

Таблица 42-1 Поиск и устранение неисправностей, связанных с запуском Prestige

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
При включении питания ни один из светодиодов Prestige не горит.	Убедитесь, что адаптер питания Prestige подсоединен к Prestige и к соответствующему источнику питания. Проверьте, включен ли Prestige и источник питания. Выключите и снова включите Prestige. Если проблема не исчезла, возможно, имеет место аппаратная неисправность. В этом случае следует связаться с продавцом.

Проблемы со светодиодом LAN

Таблица 42-2 Поиск и устранение неисправностей по светодиоду LAN

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
Светодиоды LAN не включаются.	Проверьте тип и подключение кабеля Ethernet (подробности см. в *Кратком руководстве* или *Ознакомительном курсе*). Проверьте исправность кабеля Ethernet.
	Убедитесь, что Ethernet-карта компьютера функционирует надлежащим образом.

Проблемы со светодиодом DSL

Таблица 42-3 Поиск и устранение неисправностей по светодиоду DSL

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
Светодиод xDSL не горит.	Проверьте телефонный кабель и соединения между портом DSL Prestige и розеткой.
	Телефонная компания должна проверить Вашу телефонную линию и настроить ее для использования сервиса DSL.
	Сбросьте линию ADSL для реинициализации соединения с концентратором DSLAM. Подробности см. в главе *Сопровождение* (Web-конфигуратор) или в главе Информация о системе и диагностика (Системная консоль).

Проблемы с интерфейсом LAN

Таблица 42-4 Поиск и устранение неисправностей интерфейса LAN

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
Отсутствует доступ к Prestige через локальную сеть.	Если оба светодиода 10M/100M на передней панели выключены, см. *Таблица 42-2 Поиск и устранение неисправностей* по светодиоду LAN. Убедитесь, что IP-адрес и маска подсети Prestige принадлежат к одной подсети с компьютерами локальной сети.
Невозможно связаться ни с одним компьютером локальной сети.	Если оба светодиода 10M/100M на передней панели выключены, см. *Таблица 42-2 Поиск и устранение неисправностей* по светодиоду LAN. Убедитесь, что IP-адрес и маска подсети OMNI ADSL принадлежат к одной подсети с компьютерами локальной сети.

Проблемы с интерфейсом WAN

Таблица 42-5 Устранение неисправностей, связанных с интерфейсом глобальной сети

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
Невозможность получения IP-адреса в глобальной сети от Интернет-провайдера.	Интернет-провайдер предоставляет IP-адреса в глобальной сети после аутентификации пользователя. Аутентификация может производиться по имени пользователя и паролю, по MAC-адресу или по имени хоста. Имя пользователя и пароль применимы только к инкапсуляции PPPoE и PPoA. Проверьте правильность введенных параметров **Service Type**, **User Name** и **Password** (убедитесь в правильности установки регистра при вводе). См. главу *Настройка глобальной сети* (Web-конфигуратор) или главу *Доступ в Интернет* (Системная консоль).

Проблемы с доступом в Интернет

Таблица 42-6 Устранение неисправностей, связанных с доступом в Интернет

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
Невозможно получить доступ в Интернет.	Убедитесь, что Prestige включен и подсоединен к сети. Если светодиод DSL выключен, см. *Таблица 42-3 Поиск и устранение неисправностей* по светодиоду DSL. Проверьте настройки глобальной сети. См. главу *Настройка глобальной сети* (Web-конфигуратор) или главу *Доступ в Интернет* (Системная консоль). Убедитесь в правильности введенного имени пользователя и пароля. При использовании сквозного прохода PPPoE, убедитесь, что мост включен. Подробности см. в главе *Меню 1 Настройка общих параметров*. При использовании беспроводных станций убедитесь, что Prestige и беспроводные станции используют одинаковые ESSID, каналы и ключи WEP (если включено шифрование WEP).
Подключение к Интернету разрывается	Проверьте правила планов. См. главу *составление плана вызовов* (Системная консоль). При использовании инкапсуляции PPPoA или PPPoE проверьте настройку допустимого времени простоя. См. главу *Глобальная сеть* (Web-конфигуратор) или главу *Конфигурирование удаленного узла* (Системная консоль). Свяжитесь с Интернет-провайдером.

Проблемы с паролем

Таблица 42-7 Устранение неисправностей, связанных с паролем

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
Невозможно получить доступ к Prestige.	Имя пользователя - “admin”. По умолчанию установлен пароль "1234". Поля **Password (Пароль)** и **Username (Имя пользователя)** чувствительны к регистру. Убедитесь, что Вы вводите правильный пароль и имя пользователя в нужном регистре. Если Вы изменили пароль и забыли его, Вам придется загрузить файл конфигурации по умолчанию (См. раздел *Сброс настроек Prestige* в главе *Знакомство с Web-конфигуратором*). Это восстановит все заводские настройки по умолчанию, включая пароль.

Проблемы с Web-конфигуратором

Таблица 42-8 Устранение неисправностей, связанных с Web-конфигуратором

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
Нет доступа к Web-конфигуратору.	См. *Таблица 42-7 Устранение неисправностей, связанных* с паролем. Убедитесь, что не идет сеанс связи через системную консоль. Убедитесь, что доступ к услугам Web разрешен. Если Вы сконфигурировали IP-адрес защищенного клиента, IP-адрес Вашего компьютера должен совпадать с ним. Более подробная информация приведена в главе по дистанционному управлению. Для получения доступа из глобальной сети необходимо сконфигурировать дистанционное управление, разрешающее доступ серверам глобальной сети (или всем). Следует также сконфигурировать правило межсетевого экрана, разрешающее доступ из глобальной сети. Подробности см. в главах по дистанционному управлению и межсетевым экранам. Для доступа из локальной сети IP-адреса Вашего компьютера и Prestige должны находиться в одной и той же подсети. Если Вы изменили IP-адрес Prestige в локальной сети, введите новый в поле адреса. Удалите все фильтры в меню 3.1 (локальная сеть) и меню 11.5 (глобальная сеть), которые блокируют услуги Web. См. также раздел *Проблемы дистанционного управления*

Проблемы дистанционного управления

Таблица 42-9 Устранение неисправностей, связанных с дистанционным управлением

ПРОБЛЕМА	СПОСОБ УСТРАНЕНИЯ
Невозможно дистанционное управление Prestige через локальную или глобальную сеть.	См. сценарии, при которых дистанционное управление может быть невозможно, в разделе *дистанционного управления Ограничения* главы *Управление микропрограммным обеспечением и файлами конфигурации* (Системная консоль).
	При конфигурировании через глобальную сеть следует использовать IP-адрес Prestige в глобальной сети. При конфигурировании через локальную сеть следует использовать IP-адрес Prestige в локальной сети.
	См. инструкции по проверке соединений с локальной сетью в *Таблица 42-4 Поиск и устранение неисправностей* интерфейса LAN.
	См. инструкции по проверке подключения к глобальной сети в разделе *Проблемы с интерфейсом глобальной сети*.
	См. также раздел *Проблемы с Web-конфигуратором*.

Раздел 43
Организация IP-подсетей

IP-адресация

Маршрутизаторы “прокладывают маршруты” на основе сетевых номеров. Маршрутизатор, доставляющий пакет данных на хост адресата, использует идентификатор хоста.

Классы IP-адресов

IP-адрес состоит из четырех октетов (по восемь битов), записанных в десятичном виде с разделительными точками, например, 192.168.1.1. IP-адреса разделяются на несколько классов. Класс адреса зависит от величины его первого октета.

- У адресов класса “A” в самом левом бите содержится 0. В адресе класса “A” первый октет обозначает номер сети, а остальные три октета определяют идентификатор хоста.
- У адресов класса “B” в самом левом бите содержится 1, а в следующем слева бите - 0. В адресе класса “B” первые два октета определяют номер сети, а остальные два октета - идентификатор хоста.
- Адреса класса “C” начинаются (слева направо) с последовательности 1 1 0. В адресе класса “C” первые три октета определяют номер сети, а последний октет - идентификатор хоста.
- Адреса класса “D” начинаются с последовательности 1 1 1 0. Адреса класса “D” используются для многоадресной рассылки. (Существует также адрес класса “E”. Он зарезервирован для использования в будущем.)

Таблица 43-1 Классы IP-адресов

IP-АДРЕС:		ОКТЕТ 1	ОКТЕТ 2	ОКТЕТ 3	ОКТЕТ 4
Класс A	0	Номер сети	Идентификатор хоста	Идентификатор хоста	Идентификатор хоста
Класс B	10	Номер сети	Номер сети	Идентификатор хоста	Идентификатор хоста
Класс C	110	Номер сети	Номер сети	Номер сети	Идентификатор хоста

Идентификаторы хостов, состоящие только из нулей или только из единиц, не допускаются.

Следовательно:

- Сеть класса “C” (8 битов для нумерации хостов) может включать до $(2^8 – 2)$, т. е. 254 хостов.
- Сеть класса “B” (16 битов для нумерации хостов) может включать до $(2^{16} – 2)$, т. е. 65534 хостов.

Сеть класса “A” (24 бита для нумерации хостов) может включать до (2^{24} – 2) хостов (около 16 миллионов хостов).

Поскольку первый октет IP-адреса класса “A” должен содержать “0”, первый октет адреса класса “A” может иметь значение от 0 до 127.

Аналогично, первый октет адреса класса “B” должен начинаться с “10”, поэтому первый октет адреса класса “B” имеет допустимый диапазон значений от 128 до 191. Первый октет адреса класса “C” начинается с “110” и, следовательно, принимает значения от 192 до 223.

Таблица 43-2 Допустимые диапазоны IP-адресов разных классов

КЛАСС	ДОПУСТИМЫЕ ЗНАЧЕНИЯ ПЕРВОГО ОКТЕТА (ДВОИЧНЫЕ)	ДОПУСТИМЫЕ ЗНАЧЕНИЯ ПЕРВОГО ОКТЕТА (ДЕСЯТИЧНЫЕ)
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

Маску подсети используют, чтобы определить, какие биты являются частью сетевого номера, а какие - частью идентификатора хоста (при помощи операции логического умножения "И"). Маска подсети содержит 32 бита; каждый бит маски соответствует биту IP-адреса. Если бит маски подсети имеет значение “1”, то соответствующий бит IP-адреса является частью сетевого номера. Если бит маски подсети имеет значение “0”, то соответствующий бит IP-адреса является частью идентификатора хоста.

Маски подсети записываются в десятичном виде с разделительными точками, как и IP-адреса. “Естественные” маски для IP-адресов классов A, B и C выглядят следующим образом.

Таблица 43-3 “Естественные” маски

КЛАСС	ЕСТЕСТВЕННАЯ МАСКА
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Организация подсетей

При организации подсетей распределение IP-адресов по классам не учитывается. Например, адрес класса C уже не должен иметь номер сети из 24 битов и идентификатор хоста из 8 битов. При организации подсетей некоторые из битов идентификатора хоста преобразуются в биты сетевого номера. По существующей договоренности маски подсети всегда состоят из непрерывной

последовательности единиц, начинающейся с самого левого бита маски, за которой следует непрерывная последовательность нулей, а полное число битов равно 32.

Поскольку маска всегда состоит из начинающейся слева непрерывной последовательности единиц, за которой следует непрерывная последовательность нулей, а полное число битов маски равно 32, то вместо записи значения каждого можно просто указать количество единиц. Для этого обычно после адреса пишут символ “/” и число битов в маске.

Например, запись 192.1.1.0 /25 означает адрес 192.1.1.0 с маской 255.255.255.128.

В следующей таблице показаны в обоих форматах все возможные маски подсети для адреса класса “C”.

Таблица 43-4 Альтернативный формат записи масок подсети

IP-АДРЕС МАСКИ ПОДСЕТИ	"ЕДИНИЧНЫЕ" БИТЫ МАСКИ ПОДСЕТИ	ЗНАЧЕНИЯ БИТОВ 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 из приведенных масок - это естественная маска класса “C”. Обычно, если маска не указана, подразумевается, что используется естественная маска.

Пример: Две подсети

Рассмотрим, например, адрес класса “C” 192.168.1.0 с маской подсети, равной 255.255.255.0.

	НОМЕР СЕТИ	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 составляют номер сети (класс “C”). Мы хотим получить две отдельные сети.

Разделим сеть 192.168.1.0 на две отдельные подсети, преобразовав один из битов идентификатора хоста IP-адреса в бит сетевого номера. “Позаимствованный” бит идентификатора хоста может иметь

значение “0” or “1”, что дает две подсети; 192.168.1.0 с маской 255.255.255.128 и 192.168.1.128 с маской 255.255.255.128.

В следующих таблицах выделенные фоном или жирным шрифтом значения последних битов октетов обозначают биты идентификатора хоста, “позаимствованные” для использования в качестве битов идентификатора сети. Количество “позаимствованных” битов идентификатора хоста определяет возможное количество подсетей. Оставшееся (после “заимствования”) число битов идентификатора хоста определяет возможное количество хостов в каждой подсети.

Таблица 43-5 Подсеть 1

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ 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	Наименьший идентификатор хоста: 192.168.1.1	
Broadcast-адрес: 192.168.1.127	Наибольший идентификатор хоста: 192.168.1.126	

Таблица 43-6 Подсеть 2

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ 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	Наименьший идентификатор хоста: 192.168.1.129	
Broadcast-адрес: 192.168.1.255	Наибольший идентификатор хоста: 192.168.1.254	

Оставшиеся 7 битов определяют возможное число хостов в каждой подсети. Идентификаторы хостов из одних нулей соответствуют самой подсети, а идентификаторы хостов из одних единиц определяют широковещательный адрес этой подсети, так что реальное число возможных хостов в каждой подсети в этом примере равно $(2^7 – 2)$, т. е. по 126 хост на каждую подсеть.

Адрес 192.168.1.0 с маской 255.255.255.128 соответствует самой подсети, а адрес 192.168.1.127 с маской 255.255.255.128 - это направленный широковещательный адрес для первой подсети. Следовательно, наименьший IP-адрес, который может быть назначен реальному хосту первой подсети, - это 192.168.1.1, а наибольший - 192.168.1.126. Аналогично, возможные ID-адреса хостов второй подсети находятся между 192.168.1.129 и 192.168.1.254.

Пример: Четыре подсети

В предыдущем примере было показано, как использовать 25-битную маску подсети для разделения адресного пространства класса “C” на две подсети. Аналогично, чтобы разделить адрес класса “C” на четыре подсети, нужно “позаимствовать” два бита идентификатора хоста, дающие четыре возможные комбинации: 00, 01, 10 и 11. Маска подсети содержит 26 битов (11111111.11111111.11111111.**11**000000) или равна 255.255.255.192. Каждая подсеть содержит 6 битов идентификатора хоста, что дает (2^6 - 2) или 62 хоста для каждой подсети (одни нули соответствуют самой подсети, одни единицы - широковещательному адресу подсети).

Таблица 43-7 Подсеть 1

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ 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	Наименьший идентификатор хоста: 192.168.1.1	
Broadcast-адрес: 192.168.1.63	Наибольший идентификатор хоста: 192.168.1.62	

Таблица 43-8 Подсеть 2

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ 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	Наименьший идентификатор хоста: 192.168.1.65	
Broadcast-адрес: 192.168.1.127	Наибольший идентификатор хоста: 192.168.1.126	

Таблица 43-9 Подсеть 3

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ 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	Наименьший идентификатор хоста: 192.168.1.129	
Broadcast-адрес: 192.168.1.191	Наибольший идентификатор хоста: 192.168.1.190	

Таблица 43-10 Подсеть 4

	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ 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	Наименьший идентификатор хоста: 192.168.1.193	
Broadcast-адрес: 192.168.1.255	Наибольший идентификатор хоста: 192.168.1.254	

Пример восьми подсетей

Аналогично можно использовать 27-битную маску для создания 8 подсетей (001, 010, 011, 100, 101, 110).

В следующей таблице показаны значения последних октетов IP-адресов класса C для каждой подсети.

Таблица 43-11 Восемь подсетей

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

В следующей таблице дается сводка по планированию подсетей класса “C”.

Таблица 43-12 Планирование подсетей класса Class C

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

Организация подсетей в сетях классов A и B.

В адресах классов “A” и “B” маска подсети также определяет, какие биты являются частью сетевого номера, а какие - частью идентификатора хоста.

Адрес класса “B” имеет два октета идентификатора хоста, которые могут быть использованы в организации подсетей, а адрес класса “A” имеет три октета идентификатора хоста (см. *Таблица 43-1*), которые могут быть использованы в организации подсетей.

В следующей таблице дается сводка по планированию подсетей класса “B”.

Таблица 43-13 Планирование подсетей класса Class B

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

Раздел 44
Беспроводная сеть и IEEE 802.11

Беспроводная сеть (WLAN) позволяет создать гибкую систему передачи данных, которую можно использовать для доступа к различным услугам (Интернет-навигации, электронной почте, службам печати и т. д.) без организации дорогостоящей кабельной инфраструктуры. В сущности, среда беспроводной сети позволяет свободно подключаться к сети в любой точке своей зоны охвата.

Преимущества беспроводной сети

- Доступ к сетевым службам в местах, где прокладка кабелей затруднена или невыгодна - например, в исторических зданиях, зданиях с асбестосодержащими материалами, учебных классах.
- Врачи и медперсонал получают доступ ко всем записям о пациенте при помощи портативного компьютера прямо на дому у пациента.
- Гибкие рабочие группы могут понизить полную стоимость владения сетями, конфигурация которых часто изменяется.
- Пользователи конференц-залов получают доступ к сети, не ограниченный их перемещениями между разными заседаниями - и доступ к самой последней информации, облегчающий оперативный обмен решениями.
- Эта система обеспечивает сетевое покрытие промышленных комплексов, дает предприятиям возможности роуминга и создания простых в использовании беспроводных сетей, охватывающих целые комплексы.

IEEE 802.11

Создание в 1997 г. стандарта IEEE 802.11 для беспроводных сетей (WLAN) стало первым важным шагом в эволюционном развитии технологий беспроводных сетей . Этот стандарт был разработан для повышения уровня взаимодействия между беспроводными сетями разных изготовителей, а также в целях внедрения разнообразных средств повышения производительности и других преимуществ.

Стандарт IEEE 802.11 определяет три различных передачи метода для PHY, уровня, отвечающего за передачу данных между узлами. Два из этих методов используют радиочастотные сигналы со спектральной модуляцией, Direct Sequence Spread Spectrum (DSSS, Прямая модуляция спектра последовательностями) и Frequency-Hopping Spread Spectrum (FHSS, Псевдослучайный выбор частот спектра), в нелицензированном диапазоне ISM (Industrial, Scientific and Medical - Промышленность, наука и медицина) от 2.4 до 2.4825 ГГц. Третий используемый метод - это инфракрасная технология,

использующая для транспортировки данных сигналы крайне высоких частот, находящиеся в электромагнитном спектре чуть ниже видимого света.

Конфигурация независимой беспроводной сети

Простейшая конфигурация WLAN - это независимая (Ad-hoc) сеть, соединяющая компьютеры с беспроводными узлами или станциями (STA), которая называется Базовый набор услуг (BSS). В самом примитивном варианте беспроводная сеть соединяет несколько компьютеров с беспроводными адаптерами. Если два или более беспроводных адаптеров находятся в зонах действия друг друга, они могут установить независимую сеть, которую обычно называют сеть Ad-hoc, или Независимый базовый набор услуг (IBSS). На следующей схеме приведен пример сети из настольных и переносных компьютеров, использующих беспроводлные адаптеры для созданипя беспроводной сети.

Схема 44-1 Соединение равноправных узлов в независимую сеть

Инфраструктурная конфигурация беспроводной сети

В инфраструктурной беспроводной сети многочисленные точки доступа (AP) связывают WLAN с проводной сетью и позволяют пользователям эффективно распределять сетевые ресурсы. Точки доступа не только обеспечивают связь с проводной сетью, но и организуют управление трафиком беспроводной сети в непосредственном окружении. Несколько точек доступа могут обеспечить беспроводное покрытие целого здания или комплекса зданий. Все взаимодействие между станциями или между станцией и клиентом проводной сети происходит через точку доступа.

Расширенный набор услуг (ESS), изображенный на следующем рисунке, состоит из нескольких перекрывающихся BSS (каждый из которых содержит точку доступа), связанных при помощи Системы распределения (DS). Хотя в качестве DS может использоваться сеть любого типа, это почти

всегда бывает локальная сеть Ethernet. Портативные узлы могут перемещаться от одной точки доступа к другой в условиях непрерывного покрытия всего комплекса.

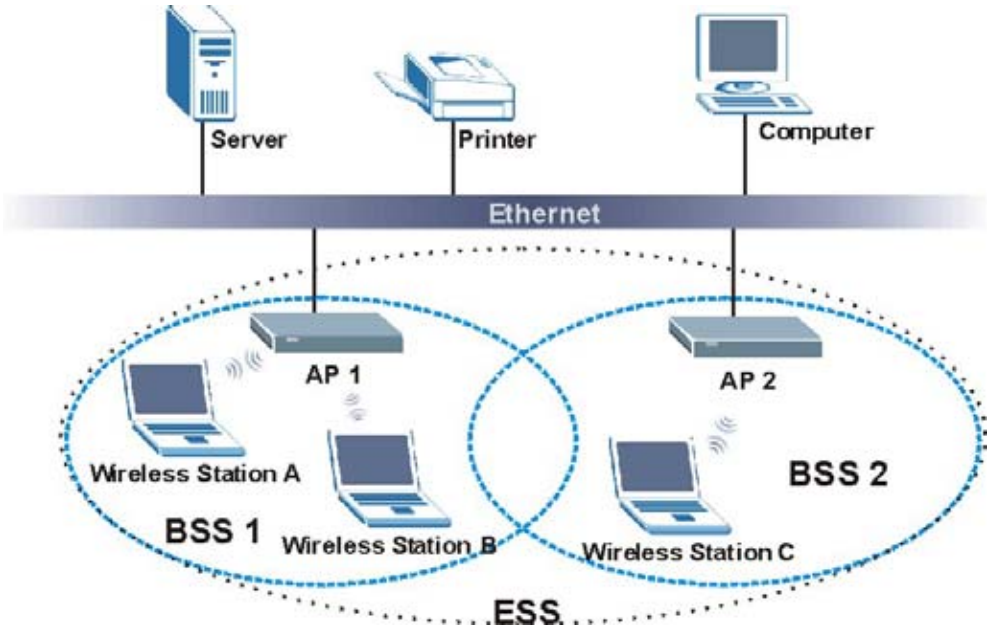


Схема 44-2 Покрытие комплекса зданий при помощи ESS

Раздел 45
PPPoE

PPPoE в действии

Модем ADSL образует мост для сеанса связи PPP поверх Ethernet (PPP поверх Ethernet, RFC 2516) с Вашего ПК на постоянный виртуальный канал ATM (Permanent Virtual Circuit (PVC)), соединенный с концентратором доступа xDSL, являющимся другим концом моста сеанса связи PPP (см. следующий рисунок). Один постоянный виртуальный канал может поддерживать любое количество сеансов PPP Вашей локальной сети. PPPoE предоставляет управление доступом и составление счетов, аналогично службам коммутации, использующим PPP.

Преимущества PPPoE

PPPoE дает следующие преимущества:

- Предоставляет хорошо знакомый пользовательский интерфейс для доступа в сеть по коммутируемой линии (DUN).
- Уменьшает нагрузку на линии связи, предоставляя виртуальные соединения на всем пути к Интернет-провайдеру для тысяч пользователей. Для GSTN (PTSN и ISDN) разводка коммутации осуществляется на местах.
- 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.

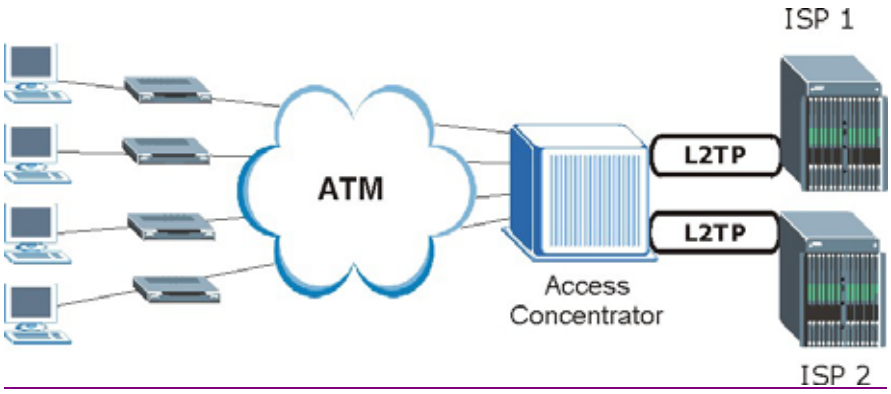


Схема 45-1 Конфигурация аппаратного обеспечения "Один ПК на маршрутизатор"

Как функционирует PPPoE

Драйвер PPPoE представляет Ethernet как последовательный канал связи с ПК; через него ПК запускает PPP, в то время как модем передает кадры Ethernet в концентратор доступа (Access Concentrator (AC)). Между концентратором доступа и Интернет-провайдером, концентратор доступа выступает в качестве L2TP (Layer 2 Tunneling Protocol - Протокол туннелирования 2 уровня) LAC (L2TP Access Concentrator - концентратор доступа L2TP) и туннеллирует кадры PPP Интернет-провайдеру. Туннель L2TP способен работать с несколькими сеансами PPP.

При использовании PPPoE, виртуальный канал (VC - Virtual Circuit) является аналогом коммутируемого соединения и проходит между модемом и концентратором доступа, в противоположность другим каналам к Интернет-провайдеру. Однако сеанс PPP устанавливается между персональным компьютером и Интернет-провайдером.

Prestige в качестве клиента PPPoE

При использовании Prestige в качестве клиента PPPoE, персональные компьютеры локальной сети видят только Ethernet и не знают о PPPoE. Это облегчает работу администратора, избавляя его от необходимости настройки клиентов PPPoE на отдельных персональных компьютерах.

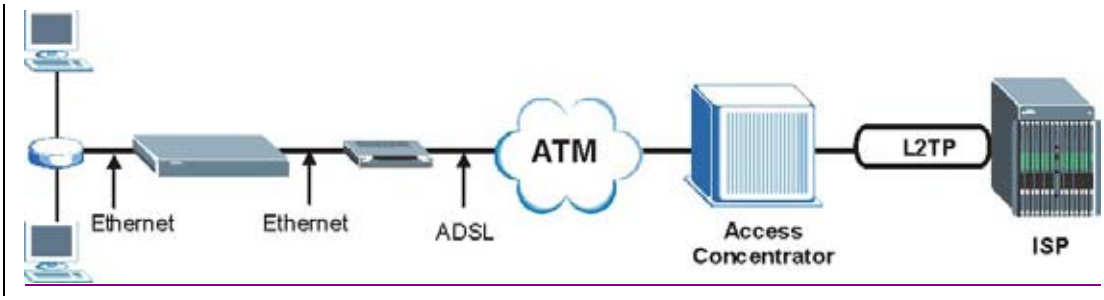


Схема 45-2 Prestige в качестве клиента PPPoE

Раздел 46
Топология виртуального соединения

ATM представляет собой технологию, ориентированную на соединение, что означает создание виртуальных соединений, по которым осуществляется связь между оконечными системами. Для обозначения виртуальных цепей используются следующие термины:

- Виртуальный канал (VC - Virtual Channel) Логические соединения между коммутаторами ATM
- Виртуальный путь "Жгут" виртуальных каналов
- Виртуальное соединение Совокупность виртуальных путей между конечными точками соединения

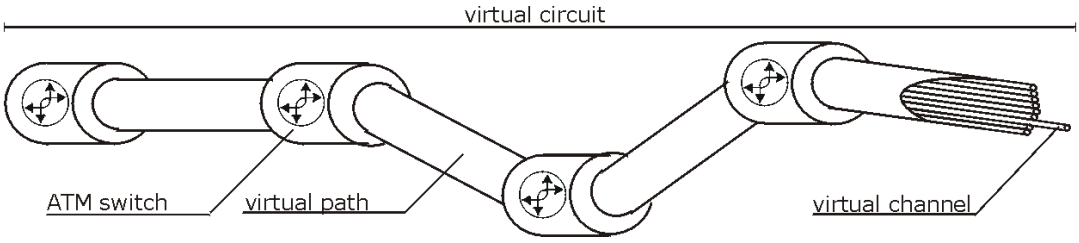


Схема 46-1Топология виртуальной цепи

Представьте, что виртуальный путь - это кабель, состоящий из нескольких проводов. Кабель соединяет две точки, при этом провода внутри кабеля образуют отдельные электропроводящие цепи 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.

Раздел 47
Примеры окон Внутреннего SPTGEN

В этом приложении описываются окна Внутреннего SPTGEN Prestige.

Сокращения, используемые в таблице примеров окон Внутреннего SPTGEN

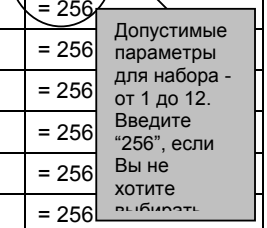
СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
FIN	Идентификационный номер поля (в окнах SMT не виден)
FN	Имя поля
PVA	Допустимые значения параметров
INPUT	Пример возможного ввода
*	Относится к модели P652H/HW.

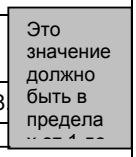
Ниже представлены окна Внутреннего SPTGEN, связанные с окнами SMT Prestige.

Таблица примеров окон Внутреннего SPTGEN

/ МЕНЮ 1 НАСТРОЙКА ОБЩИХ ПАРАМЕТРОВ (МЕНЮ SMT 1)			
FIN	**FN**	**PVA**	**INPUT**
10000000 =	Configured	<0(Нет) | 1(Да)>	= 0
10000001 =	System Name	<Str>	= Prestige
10000002 =	Location	<Str>	=
10000003 =	Contact Person's Name	<Str>	=
10000004 =	Route IP	<0(Нет) | 1(Да)>	= 1
10000006 =	Bridge	<0(Нет) | 1(Да)>	= 0

/ МЕНЮ 3.1 НАСТРОЙКА ОБЩИХ ПАРАМЕТРОВ ETHERNET (МЕНЮ SMT 3.1)			
FIN	**FN**	**PVA**	**INPUT**
30100001 =	Input Protocol filters Set 1		= 2
30100002 =	Input Protocol filters Set 2		= 256
30100003 =	Input Protocol filters Set 3		= 256
30100004 =	Input Protocol filters Set 4		= 256
30100005 =	Input device filters Set 1		= 256
30100006 =	Input device filters Set 2		= 256
30100007 =	Input device filters Set 3		= 256
30100008 =	Input device filters Set 4		= 256
30100009 =	Output protocol filters Set 1		= 256
30100010 =	Output protocol filters Set 2		= 256
30100011 =	Output protocol filters Set 3		= 256
30100012 =	Output protocol filters Set 4		= 256
30100013 =	Output device filters Set 1		= 256
30100014 =	Output device filters Set 2		= 256
30100015 =	Output device filters Set 3		= 256
30100016 =	Output device filters Set 4		= 256
МЕНЮ 3.2 НАСТРОЙКА TCP/IP И DHCP ДЛЯ ETHERNET (МЕНЮ SMT 3.2)			
FIN	**FN**	**PVA**	**INPUT**
30200001 =	DHCP	<0(нет) | 1(Сервер) | 2(Ретранслятор)>	= 0
30200002 =	Client IP Pool Starting Address		= 192.168
30200003 =	Size of Client IP Pool		= 32
30200004 =	Primary DNS Server		= 0.0.0.0
30200005 =	Secondary DNS Server		= 0.0.0.0
30200006 =	Remote DHCP Server		= 0.0.0.0





30200008 =	IP Address		= 172.21.2.200
30200009 =	IP Subnet Mask		= 16
30200010 =	RIP Direction	<0(нет) | 1(Все) | 2(Только вх.) | 3(Только исх.)>	= 0
30200011 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30200012 =	Multicast	<0(IGMP-v2) | 1(IGMP-v1) | 2(нет)>	= 2
30200013 =	IP Policies Set 1 (1~12)		= 256
30200014 =	IP Policies Set 2 (1~12)		= 256
30200015 =	IP Policies Set 3 (1~12)		= 256
30200016 =	IP Policies Set 4 (1~12)		= 256
/ МЕНЮ 3.2.1 НАСТРОЙКА ПСЕВДОНИМА IP (МЕНЮ SMT 3.2.1)			
FIN	**FN**	**PVA**	**INPUT**
30201001 =	IP Alias 1	<0(Нет) | 1(Да)>	= 0
30201002 =	IP Address		= 0.0.0.0
30201003 =	IP Subnet Mask		= 0
30201004 =	RIP Direction	<0(нет) | 1(Все) | 2(Только вх.) | 3(Только исх.)>	= 0
30201005 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2		= 256
30201008 =	IP Alias #1 Incoming protocol filters Set 3		= 256
30201009 =	IP Alias #1 Incoming protocol filters Set 4		= 256
30201010 =	IP Alias #1 Outgoing protocol filters Set 1		= 256

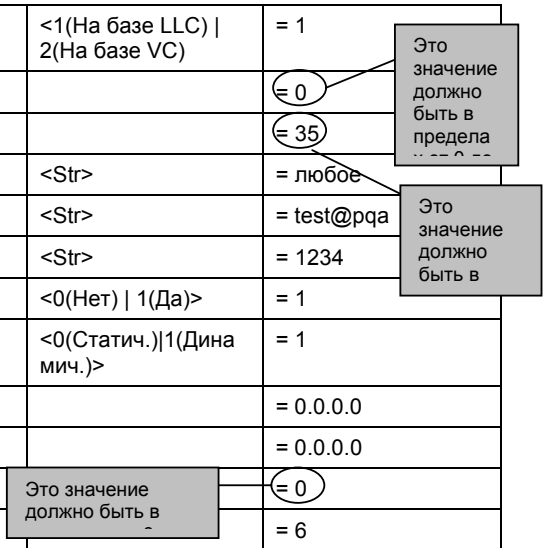
Это значение должно быть в предела

Это значение должно быть в предела

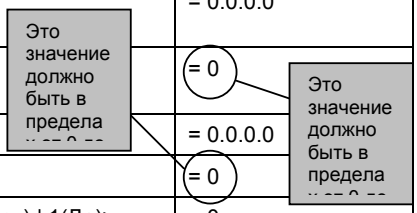
30201011 =	IP Alias #1 Outgoing protocol filters Set 2		= 256
30201012 =	IP Alias #1 Outgoing protocol filters Set 3		= 256
30201013 =	IP Alias #1 Outgoing protocol filters Set 4		= 256
30201014 =	IP Alias 2 <0(Нет) | 1(Да)>		= 0
30201015 =	IP Address		= 0.0.0.0
30201016 =	IP Subnet Mask		= 0
30201017 =	RIP Direction	<0(нет) | 1(Все) | 2(Только вх.) | 3(Только исх.)>	= 0
30201018 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201019 =	IP Alias #2 Incoming protocol filters Set 1		= 256
30201020 =	IP Alias #2 Incoming protocol filters Set 2		= 256
30201021 =	IP Alias #2 Incoming protocol filters Set 3		= 256
30201022 =	IP Alias #2 Incoming protocol filters Set 4		= 256
30201023 =	IP Alias #2 Outgoing protocol filters Set 1		= 256
30201024 =	IP Alias #2 Outgoing protocol filters Set 2		= 256
30201025 =	IP Alias #2 Outgoing protocol filters Set 3		= 256
30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256
***/ МЕНЮ 3.5 НАСТРОЙКА БЕСПРОВОДНОЙ СЕТИ (МЕНЮ SMT 3.5)**			
30500001 =	ESSID		Wireless
30500002 =	Hide ESSID	<0(Нет) | 1(Да)>	= 0

30500003 =	Channel ID	<1|2|3|4|5|6|7|8|9|10|11|12|13>	= 1
30500004 =	RTS Threshold	<0 ~ 2432>	= 2432
30500005 =	FRAG. Threshold	<256 ~ 2432>	= 2432
30500006 =	WEP	<0(ОТКЛЮЧИТЬ) | 1(WEP 64 бита) | 2(WEP 128 битов)>	= 0
30500007 =	Default Key	<1|2|3|4>	= 0
30500008 =	WEP Key1		=
30500009 =	WEP Key2		=
30500010 =	WEP Key3		=
30500011 =	WEP Key4		=
***/ МЕНЮ 3.5.1 ФИЛЬТР MAC-АДРЕСОВ WLAN (МЕНЮ SMT 3.5.1)**			
30501001 =	Mac Filter Active	<0(Нет) | 1(Да)>	= 0
30501002 =	Filter Action	<0(Разрешить) | 1(Запретить)>	= 0
30501003 =	Address 1		= 00:00:00:00:00:00
30501004 =	Address 2		= 00:00:00:00:00:00
30501005 =	Address 3		= 00:00:00:00:00:00
И т. д.	…		…
30501034 =	Address 32		= 00:00:00:00:00:00
***/ МЕНЮ 4 НАСТРОЙКА ДОСТУПА В ИНТЕРНЕТ (МЕНЮ SMT 4)**			
FIN	**FN**	**PVA**	**INPUT**
40000000 =	Configured	<0(Нет) | 1(Да)>	= 1
40000001 =	ISP	<0(Нет) | 1(Да)>	= 1
40000002 =	Active	<0(Нет) | 1(Да)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2(PPPOE) | 3(RFC 1483)| 4(PPPoA)| 5(ENET ENCAP)>	= 2

40000005 =	Multiplexing	<1(На базе LLC) | 2(На базе VC)	= 1
40000006 =	VPI #		= 0
40000007 =	VCI #		= 35
40000008 =	Service Name	<Str>	= любое
40000009 =	My Login	<Str>	= test@pqa
40000010 =	My Password	<Str>	= 1234
40000011 =	Single User Account	<0(Нет) | 1(Да)>	= 1
40000012 =	IP Address Assignment	<0(Статич.)|1(Динамич.)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0(Нет) | 1(Да)>	= 1
40000026 =	Bridge	<0(Нет) | 1(Да)>	= 0
40000027 =	ATM QoS Type	<0(CBR) | (1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR)		= 0
40000029 =	Sustain Cell Rate (SCR)		= 0
40000030 =	Maximum Burst Size(MBS)		= 0



40000031=	RIP Direction	<0(нет) | 1(Все) | 2(Только вх.) | 3(Только исх.)>	= 0
40000032=	RIP Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.1 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.1)**			
FIN	**FN**	**PVA**	**INPUT**
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0(Нет) | 1(Да)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.2 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.2)**			
FIN	**FN**	**PVA**	**INPUT**
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0(Нет) | 1(Да)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask		= 0
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		= 0
120102007 =	IP Static Route set #2, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.3 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.3)**			
FIN	**FN**	**PVA**	**INPUT**
120103001 =	IP Static Route set #3, Name	<Str>	=

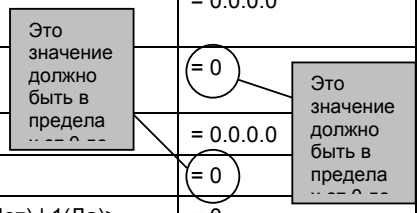


120103002 =	IP Static Route set #3, Active	<0(Нет) | 1(Да)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.4 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.4)**			
FIN	**FN**	**PVA**	**INPUT**
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0(Нет) | 1(Да)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0
120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.5 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.5)**			
FIN	**FN**	**PVA**	**INPUT**
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0(Нет) | 1(Да)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0
120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0(Нет) | 1(Да)>	= 0

*/ МЕНЮ 12.1.6 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.6)			
FIN	**FN**	**PVA**	**INPUT**
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0(Нет) | 1(Да)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0(Нет) | 1(Да)>	= 0
*/ МЕНЮ 12.1.7 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.7)			
FIN	**FN**	**PVA**	**INPUT**
120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0(Нет) | 1(Да)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0
120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(Нет) | 1(Да)>	= 0
*/ МЕНЮ 12.1.8 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.8)			
FIN	**FN**	**PVA**	**INPUT**
120108001 =	IP Static Route set #8, Name	<Str>	=
120108002 =	IP Static Route set #8, Active	<0(Нет) | 1(Да)>	= 0
120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0

120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0(Нет) | 1(Да)>	= 0

***/ МЕНЮ 12.1.9 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.9)**			
FIN	**FN**	**PVA**	**INPUT**
120109001 =	IP Static Route set #9, Name	<Str>	=
120109002 =	IP Static Route set #9, Active	<0(Нет) | 1(Да)>	= 0
120109003 =	IP Static Route set #9, Destination IP address		= 0.0.0.0
120109004 =	IP Static Route set #9, Destination IP subnetmask		= 0
120109005 =	IP Static Route set #9, Gateway		= 0.0.0.0
120109006 =	IP Static Route set #9, Metric		= 0
120109007 =	IP Static Route set #9, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.10 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.10)**			
FIN	**FN**	**PVA**	**INPUT**
120110001 =	IP Static Route set #10, Name		=
120110002 =	IP Static Route set #10, Active	<0(Нет) | 1(Да)>	= 0
120110003 =	IP Static Route set #10, Destination IP address		= 0.0.0.0
120110004 =	IP Static Route set #10, Destination IP subnetmask		= 0
120110005 =	IP Static Route set #10, Gateway		= 0.0.0.0
120110006 =	IP Static Route set #10, Metric		= 0
120110007 =	IP Static Route set #10, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.11 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.11)**			
FIN	**FN**	**PVA**	**INPUT**
120111001 =	IP Static Route set #11, Name	<Str>	=
120111002 =	IP Static Route set #11, Active	<0(Нет) | 1(Да)>	= 0



120111003 =	IP Static Route set #11, Destination IP address		= 0.0.0.0
120111004 =	IP Static Route set #11, Destination IP subnetmask		= 0
120111005 =	IP Static Route set #11, Gateway		= 0.0.0.0
120111006 =	IP Static Route set #11, Metric		= 0
120111007 =	IP Static Route set #11, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.12 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.12)**			
FIN	**FN**	**PVA**	**INPUT**
120112001 =	IP Static Route set #12, Name	<Str>	=
120112002 =	IP Static Route set #12, Active	<0(Нет) | 1(Да)>	= 0
120112003 =	IP Static Route set #12, Destination IP address		= 0.0.0.0
120112004 =	IP Static Route set #12, Destination IP subnetmask		= 0
120112005 =	IP Static Route set #12, Gateway		= 0.0.0.0
120112006 =	IP Static Route set #12, Metric		= 0
120112007 =	IP Static Route set #12, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.13 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1.13)**			
FIN	**FN**	**PVA**	**INPUT**
120113001 =	IP Static Route set #13, Name	<Str>	=
120113002 =	IP Static Route set #13, Active	<0(Нет) | 1(Да)>	= 0
120113003 =	IP Static Route set #13, Destination IP address		= 0.0.0.0
120113004 =	IP Static Route set #13, Destination IP subnetmask		= 0
120113005 =	IP Static Route set #13, Gateway		= 0.0.0.0
120113006 =	IP Static Route set #13, Metric		= 0
120113007 =	IP Static Route set #13, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.14 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1. 14)**			

FIN	FN	PVA	INPUT
120114001 =	IP Static Route set #14, Name	<Str>	=
120114002 =	IP Static Route set #14, Active	<0(Нет) | 1(Да)>	= 0
120114003 =	IP Static Route set #14, Destination IP address		= 0.0.0.0
120114004 =	IP Static Route set #14, Destination IP subnetmask		= 0
120114005 =	IP Static Route set #14, Gateway		= 0.0.0.0
120114006 =	IP Static Route set #14, Metric		= 0
120114007 =	IP Static Route set #14, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.15 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1. 15)**			
FIN	**FN**	**PVA**	**INPUT**
120115001 =	IP Static Route set #15, Name	<Str>	=
120115002 =	IP Static Route set #15, Active	<0(Нет) | 1(Да)>	= 0
120115003 =	IP Static Route set #15, Destination IP address		= 0.0.0.0
120115004 =	IP Static Route set #15, Destination IP subnetmask		= 0
120115005 =	IP Static Route set #15, Gateway		= 0.0.0.0
120115006 =	IP Static Route set #15, Metric		= 0
120115007 =	IP Static Route set #15, Private	<0(Нет) | 1(Да)>	= 0
***/ МЕНЮ 12.1.16 НАСТРОЙКА СТАТИЧЕСКОГО МАРШРУТА IP (МЕНЮ SMT 12.1. 16)**			
FIN	**FN**	**PVA**	**INPUT**
120116001 =	IP Static Route set #16, Name	<Str>	=
120116002 =	IP Static Route set #16, Active	<0(Нет) | 1(Да)>	= 0
120116003 =	IP Static Route set #16, Destination IP address		= 0.0.0.0
120116004 =	IP Static Route set #16, Destination IP subnetmask		= 0
120116005 =	IP Static Route set #16, Gateway		= 0.0.0.0

120116006 =	IP Static Route set #16, Metric		= 0
120116007 =	IP Static Route set #16, Private	<0(Нет) | 1(Да)>	= 0

/ **МЕНЮ 15 НАСТРОЙКА СЕРВЕРА SUA (МЕНЮ SMT 15)**			
FIN	**FN**	**PVA**	**INPUT**
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Active	<0(Нет) | 1(Да)>	= 0
150000003 =	SUA Server #2 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000004 =	SUA Server #2 Port Start		= 0
150000005 =	SUA Server #2 Port End		= 0
150000006 =	SUA Server #2 Local IP address		= 0.0.0.0
150000007 =	SUA Server #3 Active	<0(Нет) | 1(Да)>	= 0
150000008 =	SUA Server #3 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000009 =	SUA Server #3 Port Start		= 0
150000010 =	SUA Server #3 Port End		= 0
150000011 =	SUA Server #3 Local IP address		= 0.0.0.0
150000012 =	SUA Server #4 Active	<0(Нет) | 1(Да)>	= 0
150000013 =	SUA Server #4 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0(Нет) | 1(Да)>	= 0
150000018 =	SUA Server #5 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000019 =	SUA Server #5 Port Start		= 0
150000020 =	SUA Server #5 Port End		= 0

150000021 =	SUA Server #5 Local IP address		= 0.0.0.0
150000022 =	SUA Server #6 Active	<0(Нет) | 1(Да)> = 0	= 0
150000023 =	SUA Server #6 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000024 =	SUA Server #6 Port Start		= 0
150000025 =	SUA Server #6 Port End		= 0
150000026 =	SUA Server #6 Local IP address		= 0.0.0.0
150000027 =	SUA Server #7 Active	<0(Нет) | 1(Да)>	= 0
150000028 =	SUA Server #7 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0
150000031 =	SUA Server #7 Local IP address		= 0.0.0.0
150000032 =	SUA Server #8 Active	<0(Нет) | 1(Да)>	= 0
150000033 =	SUA Server #8 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000034 =	SUA Server #8 Port Start		= 0
150000035 =	SUA Server #8 Port End		= 0
150000036 =	SUA Server #8 Local IP address		= 0.0.0.0
150000037 =	SUA Server #9 Active	<0(Нет) | 1(Да)>	= 0
150000038 =	SUA Server #9 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000039 =	SUA Server #9 Port Start		= 0
150000040 =	SUA Server #9 Port End		= 0
150000041 =	SUA Server #9 Local IP address		= 0.0.0.0
150000042	= SUA Server #10 Active	<0(Нет) | 1(Да)>	= 0
150000043 =	SUA Server #10 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000044 =	SUA Server #10 Port Start		= 0
150000045 =	SUA Server #10 Port End		= 0

150000046 =	SUA Server #10 Local IP address		= 0.0.0.0
150000047 =	SUA Server #11 Active	<0(Нет) | 1(Да)>	= 0
150000048 =	SUA Server #11 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000049 =	SUA Server #11 Port Start		= 0
150000050 =	SUA Server #11 Port End		= 0
150000051 =	SUA Server #11 Local IP address		= 0.0.0.0
150000052 =	SUA Server #12 Active	<0(Нет) | 1(Да)>	= 0
150000053 =	SUA Server #12 Protocol	<0(Все)|6(TCP)|17(UDP)>	= 0
150000054 =	SUA Server #12 Port Start		= 0
150000055 =	SUA Server #12 Port End		= 0
150000056 =	SUA Server #12 Local IP address		= 0.0.0.0

/ МЕНЮ 21 НАБОР ФИЛЬТРОВ 1 (МЕНЮ SMT 21)

FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=

В меню SMT можно сконфигурировать до 12 наборов фильтров; во

/ МЕНЮ 21.1.1.1 НАБОР ФИЛЬТРОВ 1, ПРАВИЛО 1 (МЕНЮ SMT 21.1.1.1)

FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1,Rule 1 Type	<2(TCP/IP)>	=2
210101002 =	IP Filter Set 1,Rule 1 Active	<0(Нет) | 1(Да)>	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address		= 0.0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask		= 0
210101006 =	IP Filter Set 1,Rule 1 Dest Port		= 137
210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1

Изменить этот тип можно только в меню SMT.

Это значение должно быть в

Это значение должно быть в

210101008 =	IP Filter Set 1,Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 1
/ МЕНЮ 21.1.1.2 НАБОР ФИЛЬТРОВ 1, ПРАВИЛО 2 (МЕНЮ SMT 21.1.1.2)			
FIN	**FN**	**PVA**	**INPUT**
210102001 =	IP Filter Set 1,Rule 2 Type	<2(TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0(Нет) | 1(Да)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210102008 =	IP Filter Set 1,Rule 2 Src IP address		= 0.0.0.0
210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port		= 0

210102011 =	IP Filter Set 1,Rule 2 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 1
/ МЕНЮ 21.1.1.3 НАБОР ФИЛЬТРОВ 1, ПРАВИЛО 3 (МЕНЮ SMT 21.1.1.3)			
FIN	**FN**	**PVA**	**INPUT**
210103001 =	IP Filter Set 1,Rule 3 Type	<2(TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active	<0(Нет) | 1(Да)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port		= 139
210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address		= 0.0.0.0
210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210103013 =	IP Filter Set 1,Rule 3 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)	= 3

210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)	= 1
/ МЕНЮ 21.1.1.4 НАБОР ФИЛЬТРОВ 1, ПРАВИЛО 4 (МЕНЮ SMT 21.1.1.4)			
FIN	**FN**	**PVA**	**INPUT**
210104001 =	IP Filter Set 1,Rule 4 Type	<2(TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0(Нет) | 1(Да)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)	= 1
/ МЕНЮ 21.1.1.5 НАБОР ФИЛЬТРОВ 1, ПРАВИЛО 5 (МЕНЮ SMT 21.1.1.5)			
FIN	**FN**	**PVA**	**INPUT**
210105001 =	IP Filter Set 1,Rule 5 Type	<2(TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active	<0(Нет) | 1(Да)>	= 1

210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0
210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 1
/ МЕНЮ 21.1.1.6 НАБОР ФИЛЬТРОВ 1, ПРАВИЛО 6 (МЕНЮ SMT 21.1.1.6)			
FIN	**FN**	**PVA**	**INPUT**
210106001 =	IP Filter Set 1,Rule 6 Type	<2(TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0(Нет) | 1(Да)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139

210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210106013 =	IP Filter Set 1,Rule 6 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 2

/ МЕНЮ 21.1 НАБОР ФИЛЬТРОВ 2 (МЕНЮ SMT 21.1)			
FIN	**FN**	**PVA**	**INPUT**
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN

/ МЕНЮ 21.1.2.1 НАБОР ФИЛЬТРОВ 2, ПРАВИЛО 1 (МЕНЮ SMT 21.1.2.1)			
FIN	**FN**	**PVA**	**INPUT**
210201001 =	IP Filter Set 2, Rule 1 Type	<0(нет)|2(TCP/IP)>	= 2
210201002 =	IP Filter Set 2, Rule 1 Active	<0(Нет) | 1(Да)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port		= 137
210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210201008 =	IP Filter Set 2, Rule 1 Src IP address		= 0.0.0.0

210201009 =	IP Filter Set 2, Rule 1 Src Subnet Mask		= 0
210201010 =	IP Filter Set 2, Rule 1 Src Port		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210201014 =	IP Filter Set 2, Rule 1 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 1
/ МЕНЮ 21.1.2.2 НАБОР ФИЛЬТРОВ 2, ПРАВИЛО 2 (МЕНЮ SMT 21.1.2.2)			
FIN	**FN**	**PVA**	**INPUT**
210202001 =	IP Filter Set 2, Rule 2 Type	<0(нет)|2(TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active	<0(Нет) | 1(Да)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address		= 0.0.0.0
210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask		= 0
210202010 =	IP Filter Set 2,Rule 2 Src Port		= 0
210202011 =	IP Filter Set 2, Rule 2 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3

210202014 =	IP Filter Set 2, Rule 2 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 1
/ МЕНЮ 21.1.2.3 НАБОР ФИЛЬТРОВ 2, ПРАВИЛО 3 (МЕНЮ SMT 21.1.2.3)			
FIN	**FN**	**PVA**	**INPUT**
210203001 =	IP Filter Set 2, Rule 3 Type	<0(нет)|2(TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active	<0(Нет) | 1(Да)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask		= 0
210203006 =	IP Filter Set 2, Rule 3 Dest Port		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address		= 0.0.0.0
210203009 =	IP Filter Set 2,Rule 3 Src Subnet Mask		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port		= 0
210203011 =	IP Filter Set 2, Rule 3 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210203013 =	IP Filter Set 2, Rule 3 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210203014 =	IP Filter Set 2,Rule 3 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 1
/ МЕНЮ 21.1.2.4 НАБОР ФИЛЬТРОВ 2, ПРАВИЛО 4 (МЕНЮ SMT 21.1.2.4)			
FIN	**FN**	**PVA**	**INPUT**
210204001 =	IP Filter Set 2, Rule 4 Type	<0(нет)|2(TCP/IP)>	= 2
210204002 =	IP Filter Set 2, Rule 4 Active		<0(Нет)|1(Да)> = 1 ???
210204003 =	IP Filter Set 2, Rule 4 Protocol		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address		= 0.0.0.0

210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port		= 137
210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210204013 =	IP Filter Set 2, Rule 4 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210204014 =	IP Filter Set 2, Rule 4 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 1
/ МЕНЮ 21.1.2.5 НАБОР ФИЛЬТРОВ 2, ПРАВИЛО 5 (МЕНЮ SMT 21.1.2.5)			
FIN	**FN**	**PVA**	**INPUT**
210205001 =	IP Filter Set 2, Rule 5 Type	<0(нет)|2(TCP/IP)>	= 2
210205002 =	IP Filter Set 2, Rule 5 Active	<0(Нет) | 1(Да)>	= 1
210205003 =	IP Filter Set 2,Rule 5 Protocol		= 17
210205004 =	IP Filter Set 2, Rule 5 Dest IP address		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port		= 0

210205011 =	IP Filter Set 2, Rule 5 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210205014 =	IP Filter Set 2, Rule 5 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 1
/ МЕНЮ 21.1.2.6 НАБОР ФИЛЬТРОВ 2, ПРАВИЛО 6 (МЕНЮ SMT 21.1.2.5)			
FIN	**FN**	**PVA**	**INPUT**
210206001 =	IP Filter Set 2, Rule 6 Type	<0(нет)|2(TCP/IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active	<0(Нет) | 1(Да)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol		= 17
210206004 =	IP Filter Set 2, Rule 6 Dest IP address		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp	<0(нет)|1(равно)|2(не равно)| 3(меньше)| 4(больше)>	= 0
210206013 =	IP Filter Set 2,Rule 6 Act Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 3
210206014 =	IP Filter Set 2,Rule 6 Act Not Match	<1(проверить след.)|2(переслать)| 3(сбросить)>	= 2
***/ МЕНЮ 23.1 НАСТРОЙКА СИСТЕМНОГО ПАРОЛЯ (МЕНЮ SMT 23.1)**			

FIN	FN	PVA	INPUT
230000000 =	System Password		= 1234
***/ МЕНЮ 23.2 ЗАЩИТНЫЕ ФУНКЦИИ СИСТЕМЫ: СЕРВЕР RADIUS (МЕНЮ SMT 23.2)**			
FIN	**FN**	**PVA**	**INPUT**
230200001 =	Authentication Server Configured	<0(Нет) | 1(Да)>	= 1
230200002 =	Authentication Server Active	<0(Нет) | 1(Да)>	= 1
230200003 =	Authentication Server IP Address		= 192.168.1.32
230200004 =	Authentication Server Port		= 1822
230200005 =	Authentication Server Shared Secret		= 111111111111111 1111111111111111
230200006 =	Accounting Server Configured	<0(Нет) | 1(Да)>	= 1
230200007 =	Accounting Server Active	<0(Нет) | 1(Да)>	= 1
230200008 =	Accounting Server IP Address		= 192.168.1.44
230200009 =	Accounting Server Port		= 1823
230200010 =	Accounting Server Shared Secret		= 1234
***/ МЕНЮ 23.4 ЗАЩИТНЫЕ ФУНКЦИИ СИСТЕМЫ: IEEE802.1X (МЕНЮ SMT 23.4)**			
FIN	**FN**	**PVA**	**INPUT**
230400002 =	ReAuthentication Timer (in second)		= 555
230400003 =	Idle Timeout (in second)		= 999
230400004 =	Authentication Databases	<0(Только локальные базы данных пользователей) |1(Только RADIUS) |2(Локальные,RADIUS) |3(RADIUS,Локальные)>	= 1
/ МЕНЮ 24.11 ДИСТАНЦИОННОЕ УПРАВЛЕНИЕ (МЕНЮ SMT 24.11)			
FIN	**FN**	**PVA**	**INPUT**
241100001 =	TELNET Server Port		= 23
241100002 =	TELNET Server Access	<0(все)|1(нет)|2(Lan)|3(Wan)>	= 0
241100003 =	TELNET Server Secured IP address		= 0.0.0.0
241100004 =	FTP Server Port		= 21
241100005 =	FTP Server Access	<0(все)|1(нет)|2(Lan)|3(Wan)>	= 0

Эти значения должны быть в предела

241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0(все)|1(нет)|2(Lan)|3(Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

Это значение должно быть в предела

Примеры команд

Ниже представлены примеры окон Внутреннего SPTGEN, связанных с командами интерпретатора команд SMT Prestige.

/КОМАНДА ИНТЕРПРЕТАТОРА КОМАНД (ДЛЯ ПРИЛОЖЕНИЯ A): WAN ADSL OPENCMD			
FIN	**FN**	**PVA**	**INPUT**
990000001 =	ADSL OPMD	<0(glite)|1(t1.413)|2(gdmt)|3(мульти)>	= 3
/КОМАНДА ИНТЕРПРЕТАТОРА КОМАНД (ДЛЯ ПРИЛОЖЕНИЯ B): WAN ADSL OPENCMD			
FIN	**FN**	**PVA**	**INPUT**
990000001 =	ADSL OPMD	<0(etsi)|1(нормальный)|2(gdmt)|3(мульти)>	= 3

Раздел 48
Настройка IP-адреса компьютера

На всех компьютерах должна быть установлена адаптерная плата Ethernet 10M или 100M и настроен протокол 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.

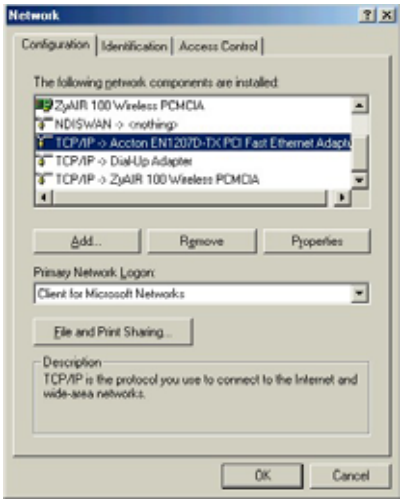
TCP/IP уже должен быть инсталлирован на компьютерах с системами Windows NT/2000/XP, Macintosh OS 7 или более поздними операционными системами.

После инсталляции соответствующих компонентов TCP/IP сконфигурируйте параметры TCP/IP, чтобы иметь возможность коммуникации с сетью.

При назначении IP-параметров вручную, а не при помощи динамического назначения, следует убедиться, что все компьютеры имеют IP-адреса в той же подсети, что и порт локальной сети Prestige.

Windows 95/98/Me

Щелкните на **Start**, **Settings**, **Control Panel** и дважды щелкните на иконке **Network**, чтобы открыть окно **Network**.



Установка компонентов

На закладке **Configuration** в окне **Network** показан список установленных компонентов. Следует выбрать сетевой адаптер, протокол TCP/IP и клиента для сетей Microsoft.

Для выбора сетевого адаптера:

a. Щелкните на **Add** в окне **Network**.

b. Выберите **Adapter** и щелкните на **Add**.

c. Выберите производителя и модель сетевого адаптера и щелкните на **OK**

Для выбора TCP/IP:

a. Щелкните на **Add** в окне **Network**.

b. Выберите **Protocol** и щелкните на **Add**.

c. Выберите **Microsoft** из списка **производителей**.

d. Выберите **TCP/IP** из списка сетевых протоколов и щелкните на **OK**.

Для выбора клиента для сетей Microsoft:

a. Щелкните на **Add**.

b. Выберите **Client** и щелкните на **Add**.

c. Выберите **Microsoft** из списка производителей.

d. Выберите из списка сетевых клиентов **Client for Microsoft Networks** и щелкните на **OK**.

e. Перезапустите компьютер для применения изменений.

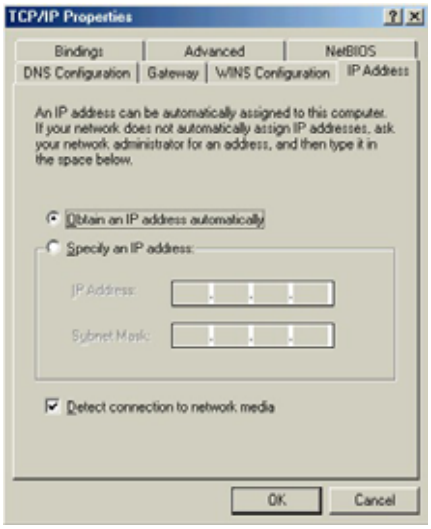
Конфигурирование

1. В окне **Network** щелкните на закладке **Configuration**, выберите пункт TCP/IP и щелкните на **Properties**.

2. Щелкните на закладке **IP Address**.

   - Если используется динамический IP-адрес, выберите **Obtain an IP address automatically**.

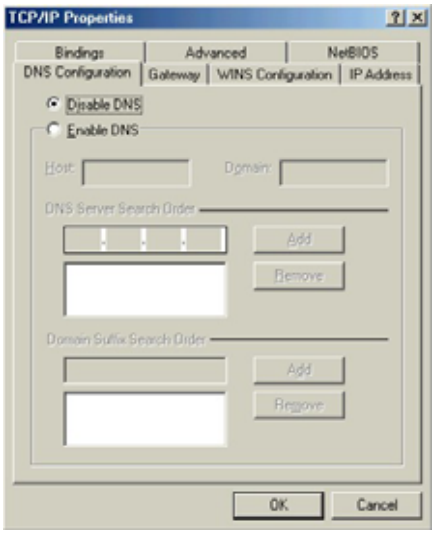
   - Если используется статический IP-адрес, выберите **Specify an IP address** и введите соответствующую информацию в полях **IP Address** и **Subnet Mask**.



3. Щелкните на закладке **DNS Configuration**.

   - Если Вы не располагаете информацией о DNS, выберите **Disable DNS**.

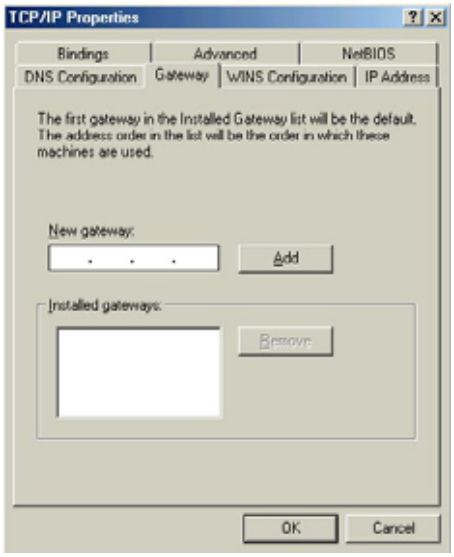
   - Если Вы располагаете информацией о DNS, выберите **Enable DNS** и введите соответствующую информацию в указанных ниже полях (в заполнении всех полей может не быть необходимости).



4. Щелкните на закладке **Gateway**.

   - Если Вы не знаете IP-адрес шлюза, удалите ранее установленные шлюзы.

   - Если Вы знаете IP-адрес шлюза, введите его в поле **New gateway** и щелкните на **Add**.



5. Щелкните на кнопке **OK** для сохранения, а затем закройте окно **TCP/IP Properties**.

6. Щелкните на кнопке **OK**, чтобы закрыть окно **Network**. При появлении соответствующей подсказки вставьте компакт-диск с Windows.

7. Включите Prestige и перезапустите компьютер (при появлении соответствующей подсказки)

Проверка настроек

1. Щелкните **Start**, а затем на **Run**.

2. В окне **Run** введите "winipcfg", а затем щелкните на **OK** для перехода к окну **IP Configuration**.

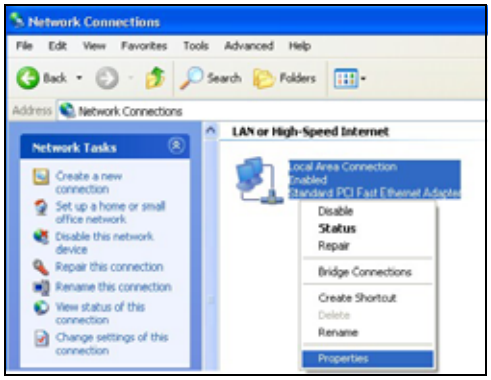
3. Выберите сетевой адаптер. При этом должен быть выведен IP-адрес и маска подсети Вашего компьютера, а также шлюз по умолчанию.

Windows 2000/NT/XP

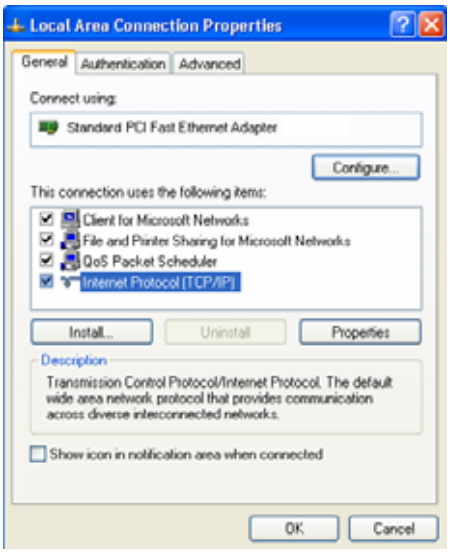
1. В Windows XP щелкните на **start**, **Control Panel**. В Windows 2000/NT щелкните **Start**, **Settings**, **Control Panel**.

2. В Windows XP щелкните на **Network Connections**. В Windows 2000/NT щелкните на **Network and Dial-up Connections**.

3. Щелкните правой кнопкой мыши на **Local Area Connection**, затем щелкните на **Properties**.



4. Выберите **Internet Protocol (TCP/IP) (Протокол Интернета (TCP/IP))** (на закладке **General (Общие)** в WinXP) и щелкните **Properties (Свойства)**.



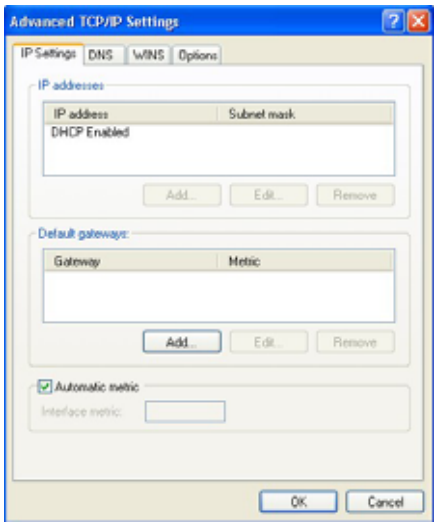
5. При этом откроется окно **Internet Protocol TCP/IP Properties** (в WinXP - закладка **General**).

   - Если используется динамический IP-адрес, щелкните на **Obtain an IP address automatically**.

   - Если используется статический IP-адрес, щелкните на **Use the following IP Address** и заполните поля **IP address**, **Subnet mask** и **Default gateway**.

   Щелкните на **Advanced**.

6. - Если Вы не знаете IP-адрес шлюза, удалите все предварительно установленные шлюзы под закладкой **IP Settings** и щелкните на **OK**.



Для конфигурирования дополнительных IP-адресов выполните одну или несколько из следующих операций:

- Под закладкой **IP Settings** в IP addresses щелкните на **Add**.

- Под закладкой **TCP/IP Address** введите IP-адрес в поле **IP address** и маску подсети в поле **Subnet mask**, а затем щелкните на **Add**.

- Повторите описанные выше действия для всех IP-адресов, которые Вы хотите добавить.

- Сконфигурируйте дополнительные шлюзы по умолчанию под закладкой **IP Settings**, щелкнув на **Add** в **Default gateways**.

- В **TCP/IP Gateway Address** введите IP-адрес шлюза по умолчанию в **Gateway**. Для конфигурирования в ручном режиме метрики (количество транзитных пунктов при передаче данных) отключите **Automatic metric** и введите метрику в **Metric**.

- Щелкните на **Add**.

- Повторите описанные выше действия для всех шлюзов, которые Вы хотите добавить.

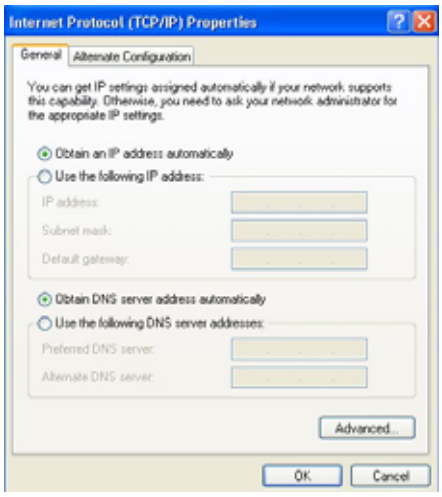
- В завершение щелкните на **OK**.

7. В окне **Internet Protocol TCP/IP Properties** (в WinXP - на закладке **General**):

   - Щелкните на **Obtain DNS server automatically**, если Вы не знаете IP-адрес(-а) сервера(-ов) DNS.

   - Если Вы знаете IP-адрес(-а) сервера(-ов) DNS, щелкните на **Use the following DNS server addresses** и введите их в полях **Preferred DNS server** и **Alternate DNS server**.

   Если серверы DNS уже предварительно сконфигурированы, щелкните на **Advanced**, а затем на закладке **DNS** для их упорядочения.



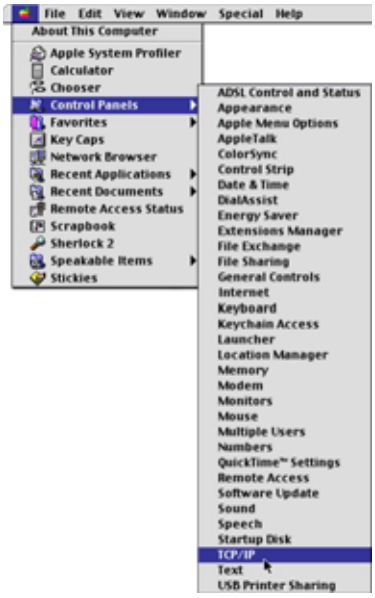
8. Щелкните на **OK** и закройте окно **Internet Protocol (TCP/IP) Properties**.
9. Щелкните на **OK**, чтобы закрыть окно **Local Area Connection Properties**.
10. Включите Prestige и перезапустите компьютер (при появлении соответствующей подсказки).

Проверка настроек

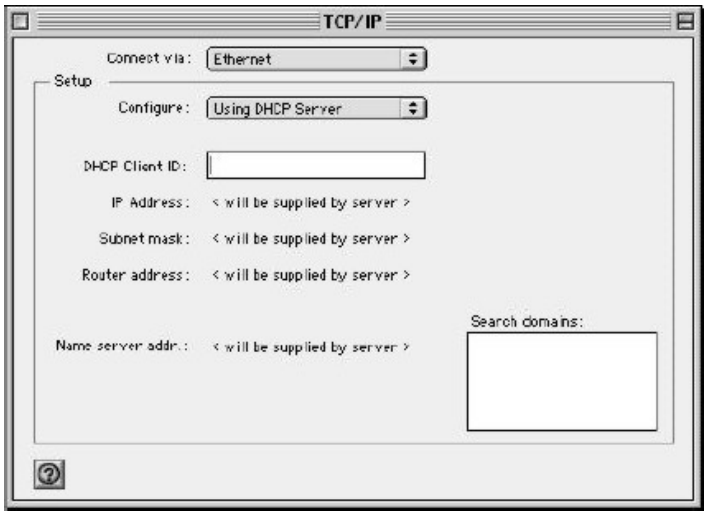
1. Щелкните на **Start**, **All Programs**, **Accessories** и **Command Prompt**.
2. В окне **Command Prompt** введите "ipconfig", а затем нажмите клавишу [ENTER]. Можно также открыть окно **Network Connections**, щелкнуть правой кнопкой мыши на ярлыке сетевого соединения, щелкнуть на **Status**, а затем щелкнуть на закладке **Support**.

Macintosh OS 8/9

1. Щелкните на Меню **Apple**, **Control Panel**, а затем дважды щелкните на **TCP/IP**, чтобы открыть **TCP/IP Control Panel**.



2. Выберите из списка **Connect via** пункт **Ethernet built-in**.



3. При динамически назначаемых параметрах выберите из списка **Configure:** опцию **Using DHCP Server**.
4. При статически назначаемых параметрах выполните следующее:

   - В окне **Configure** выберите **Manually**.

   - Введите Ваш IP-адрес в окне **IP Address**.

   - Введите Вашу маску подсети в окне **Subnet mask**.

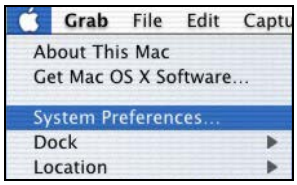
   - Введите IP-адрес Prestige в окне **Router**.
5. Закройте **TCP/IP Control Panel**.
6. При появлении соответствующей подсказки щелкните на **Save** для сохранения изменений в конфигурации.
7. Включите Prestige и перезапустите компьютер (при появлении соответствующей подсказки).

Проверка настроек

Проверьте свойства TCP/IP в окне **TCP/IP Control Panel**.

Macintosh OS X

1. Щелкните на меню **Apple**, затем щелкните на **System Preferences** , чтобы открыть окно **System Preferences**.

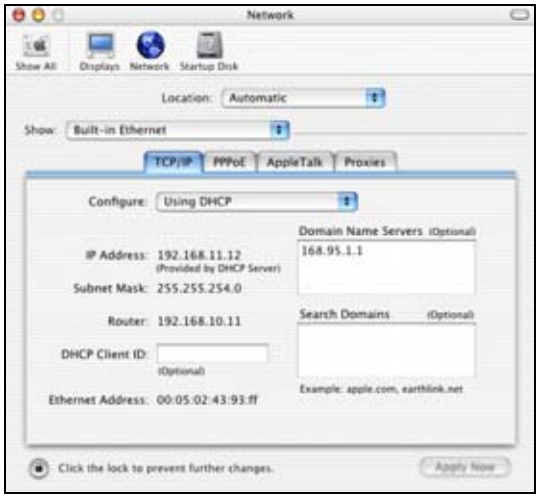


2. Щелкните на **Network** в панели иконок.

   - Выберите из списка **Location** опцию **Automatic**.

   - Выберите из списка **Show** опцию **Ethernet built-in**.

   - Щелкните на закладке **TCP/IP**.



3. При динамически назначаемых параметрах выберите из списка **Configure** опцию **Using DHCP.**

4. При статически назначаемых параметрах выполните следующее:

   - В окне **Configure** выберите **Manually**.

   - Введите Ваш IP-адрес в окне **IP Address**.

   - Введите Вашу маску подсети в окне **Subnet mask**.

   - Введите IP-адрес Prestige в окне **Router**.

5. Щелкните на **Apply Now** и закройте окно.

6. Включите Prestige и перезапустите компьютер (при появлении соответствующей подсказки).

Проверка настроек

Проверьте свойства TCP/IP в окне **Network**.

Раздел 49
Разделители частот и микрофильтры

В этом приложении описывается установка разделителя частот POTS или телефонного микрофильтра.

Подключение разделителя частот POTS

При использовании стандарта ADSL Full Rate (G.dmt) Вы можете использовать разделитель POTS (Обычной телефонной сети) для разделения сигналов телефона и сигналов ADSL. Это позволяет одновременно осуществлять на одной и той же линии телефонные вызовы и доступ в Интернет. Кроме того, разделители частот устраняют разрушающие помехи, создаваемые телефонными аппаратами.

Установите разделитель частот POTS в точке входа телефонной линии в дом, как показано на следующем рисунке.

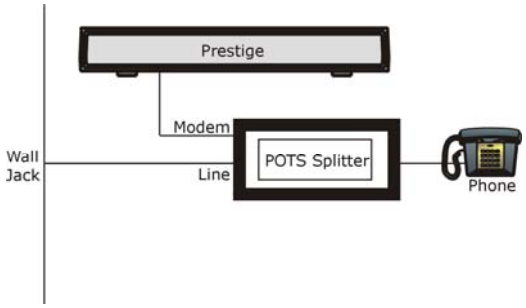


Схема 49-1 Подключение разделителя частот POTS

Шаг 1. Подключить сторону с обозначением "Phone" к телефону.
Шаг 2. Подключить сторону с обозначением "Modem" к Prestige.
Шаг 3. Подключить сторону с обозначением "Line" к стенной розетке телефона.

Телефонные микрофильтры

Передача голосовых сигналов телефона осуществляется в низком частотном диапазоне (0 - 4 кГц), а передача сигналов ADSL происходит на более высоких частотах - свыше 4 кГц. Микрофильтр выступает в качестве фильтр низких частот Вашего телефона, исключающего взаимное влияние сигналов ADSL и голосовых сигналов телефона. Телефонные микрофильтры используются по усмотрению пользователя.

Шаг 1. Подключить телефонный провод, идущий от стенной розетки, к концу Y-образного разъема с одним выводом.

Шаг 2. Подключить провод, идущий от конца Y-образного разъема с двумя выводами, к стороне стены микрофильтра.

Шаг 3. Подключить другой провод, идущий от конца Y-образного разъема с двумя выводами, к Prestige.

Шаг 4. Подключить сторону телефона микрофильтра к телефону, как показано на следующем рисунке.

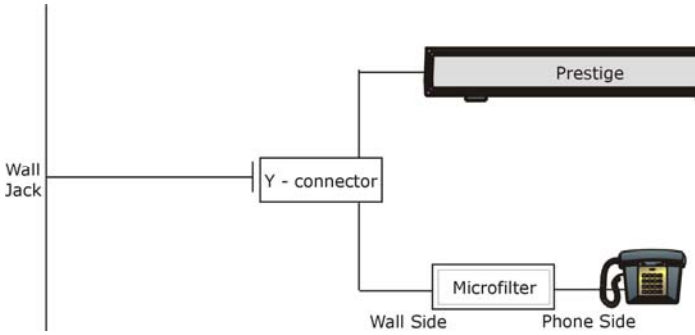


Схема 49-2 Подключение микрофильтра

Prestige с ISDN

Этот раздел предназначен только для пользователей, использующих Prestige с ADSL в сети ISDN (с цифровыми телефонными услугами). Ниже приведен пример установки Prestige с ISDN.

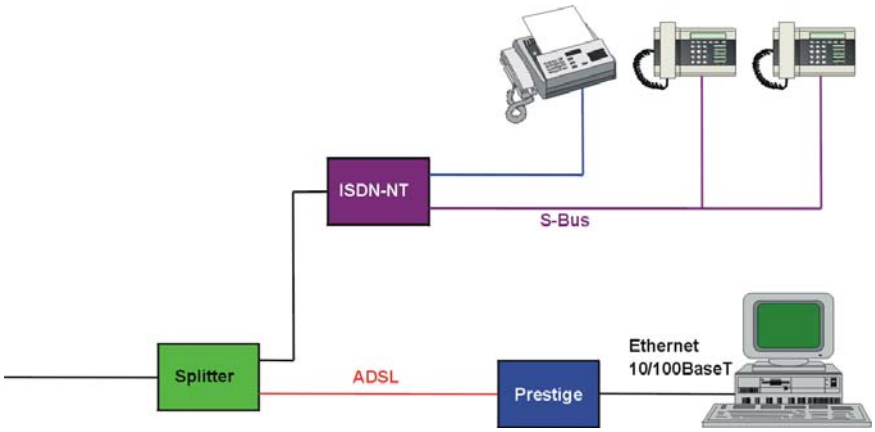


Схема 49-3 Prestige с ISDN

Раздел 50
Описание журнальных записей

В этом приложении приводятся описания примеров журнальных сообщений[1].

Таблица 50-1 Сообщения сопровождения системы

СООБЩЕНИЕ	ОПИСАНИЕ
`Time calibration is successful`	Маршрутизатор установил время по 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`	Истек срок действия IP-адреса клиента DHCP.
`DHCP server assigns %s`	Сервер DHCP назначил клиенту IP-адрес.
`SMT Login Successfully`	Успешное подключение к интерфейсу SMT маршрутизатора.
`SMT Login Fail`	Безуспешная попытка подключения к интерфейсу SMT маршрутизатора.
`WEB Login Successfully`	Успешное подключение к интерфейсу Web-конфигуратора маршрутизатора.
`WEB Login Fail`	Безуспешная попытка подключения к интерфейсу Web-конфигуратора маршрутизатора.
`TELNET Login Successfully`	Успешное подключение к маршрутизатору через telnet.
`TELNET Login Fail`	Безуспешная попытка подключения к маршрутизатору через telnet.
`FTP Login Successfully`	Успешное подключение к маршрутизатору через ftp.
`FTP Login Fail`	Безуспешная попытка подключения к маршрутизатору через ftp.

[1] На момент написания этого документа Prestige не поддерживал выдачу всех описанных здесь сообщений.

Таблица 50-2 Сообщения UPnP

СООБЩЕНИЕ	ОПИСАНИЕ
UPnP pass through Firewall	Пакеты UPnP могут проходить сквозь межсетевой экран.

В сообщениях о фильтрации содержимого “(Destination)” означает IP-адрес или имя домена назначения.

Таблица 50-3 Сообщения о фильтрации содержимого

СООБЩЕНИЕ	ПРИМЕЧАНИЕ	ОПИСАНИЕ
(Destination) Keyword Blocking	Web-блокировка	Prestige заблокировал доступ к адресу или имени домена, содержащим запрещенное ключевое слово.
(Destination) Contains ActiveX	Web-блокировка	Prestige заблокировал доступ к IP-адресу или имени домена, содержащим ActiveX, т. к. фильтр содержимого настроен на запрет ActiveX.
(Destination) Contains Java applet	Web-блокировка	Prestige заблокировал доступ к IP-адресу или имени домена, содержащим апплеты Java, т. к. фильтр содержимого настроен на запрет апплетов Java.
(Destination) Contains cookie	Web-блокировка	Prestige заблокировал доступ к IP-адресу или имени домена, содержащим cookie, т. к. фильтр содержимого настроен на запрет cookies.
(Destination) Proxy mode detected	Web-блокировка	Prestige заблокировал доступ к IP-адресу или имени домена, присвоенного прокси-серверу, т. к. фильтр содержимого настроен на запрет прокси-серверов.
(Destination)	Web-пересылка	Prestige разрешил доступ к адресу или имени домена после запланированного отключения фильтра содержимого.

В сообщениях об атаках может быть указан протокол (Protocol) пакета (например, TCP или UDP), вызвавшего появление сообщения.

Таблица 50-4 Сообщения об атаках

СООБЩЕНИЕ	ОПИСАНИЕ
`attack (Protocol)`	Межсетевой экран обнаружил атаку. В сообщении также может быть указан протокол (например, TCP или UDP).
`land Protocol)`	Межсетевой экран обнаружил атаку типа land. В сообщении также может быть указан протокол (например, TCP или UDP).
`icmp echo ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку типа ICMP echo. См. описание типа и кода в разделе по сообщениям ICMP.
`syn flood TCP`	Межсетевой экран обнаружил атаку типа TCP syn flood.
`ports scan TCP`	Межсетевой экран обнаружил атаку типа TCP port scan.
`teardrop (Protocol)`	Межсетевой экран обнаружил атаку типа teardrop.
`illegal command TCP`	Межсетевой экран обнаружил атаку некорректной командой TCP SMTP.
`NetBIOS TCP`	Межсетевой экран обнаружил атаку TCP NetBIOS.
`ip spoofing - no routing entry (Protocol)`	Межсетевой экран обнаружил атаку подменой IP-адреса при отсутствии у Prestige маршрута по умолчанию. В сообщении также может быть указан протокол (например, TCP или UDP).
`vulnerability ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку уязвимости ICMP. См. описание типа и кода в разделе по сообщениям ICMP.
`traceroute ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку трассировки ICMP. См. описание типа и кода в разделе по сообщениям ICMP.

Сообщения о доступе могут содержать следующую информацию:

- (Protocol) - протокол пакета (например, TCP или UDP), вызвавшего появление сообщения.
- (Direction) - направление, в котором перемещался пакет (например, от LAN к WAN или от WAN к LAN)
- (Rule) - номер правила межсетевого экрана, вызвавшего появление сообщения.

Таблица 50-5 Сообщения о доступе

СООБЩЕНИЕ	ОПИСАНИЕ
Firewall default policy (Protocol, Direction)	Доступ соответствовал стратегии по умолчанию, и Prestige заблокировал или переслал данные в соответствии с конфигурацией стратегии по умолчанию межсетевого экрана .
Firewall rule match (Protocol, Direction, Rule)	Доступ соответствовал правилу межсетевого экрана, и Prestige заблокировал или переслал его в соответствии с конфигурации правила .
Firewall rule NOT match: (Protocol, Direction, Rule)	Доступ не соответствовал правилу межсетевого экрана, и Prestige зарегистрировал его в журнале.
dest port (Protocol, Direction)	Доступ не соответствовал порту назначения, указанному в правиле межсетевого экрана, и Prestige зарегистрировал его в журнале.
src port (Protocol, Direction)	Доступ не соответствовал порту источника, указанному в правиле межсетевого экрана, и Prestige зарегистрировал его в журнале.
dest IP (Protocol, Direction)	Доступ не соответствовал IP-адресу назначения, указанному в правиле межсетевого экрана, и Prestige зарегистрировал его в журнале.
src IP (Protocol, Direction)	Доступ не соответствовал IP-адресу источника, указанному в правиле межсетевого экрана, и Prestige зарегистрировал его в журнале.
protocol (Protocol, Direction)	Доступ не соответствовал протоколу, указанному в правиле межсетевого экрана, и Prestige зарегистрировал его в журнале.
Triangle route packet forwarded (Protocol)	Межсетевой экран разрешил сеанс связи по треугольному маршруту.
ICMP Source Quench	Prestige отправил или принял пакет ICMP source quench, сообщающий хосту о необходимости снизить скорость передачи данных.
ICMP Time Exceed	Prestige отправил или принял пакет ICMP Time Exceed, т. к. пакет с нулевым временем жизни (TTL) был сброшен.
ICMP Destination Unreachable	Prestige отправил или принял пакет ICMP Destination Unreachable, когда пакет был сброшен из-за закрытого порта назначения.

Таблица 50-5 Сообщения о доступе

СООБЩЕНИЕ	ОПИСАНИЕ
Packet without a NAT table entry blocked (Protocol)	Маршрутизатор заблокировал пакет, не имеющий соответствующей записи в таблице NAT.
Out of order TCP handshake packet blocked (Protocol)	Маршрутизатор заблокировал пакет TCP-квитирования, пришедший вне очереди
Unsupported/out-of-order ICMP (Protocol)	Prestige выдает это сообщение после сброса пакета ICMP по одной из двух следующих причин: 1. Prestige не поддерживает протокол пакетов ICMP. 2. Данный пакет ICMP является эхо-ответом, для которого не было соответствующего эхо-запроса.
Router reply ICMP packet	Маршрутизатор отправил ответный пакет ICMP. Этот пакет автоматически проходит через межсетевой экран.
Remote access denied	Маршрутизатор заблокировал попытку удаленного доступа.

Таблица 50-6 Сообщения о сбросе TCP

СООБЩЕНИЕ	ОПИСАНИЕ
Firewall sent TCP reset packets	Межсетевой экран отправил пакеты сброса TCP.

Таблица 50-7 Примечания ICMP

ТИП	КОД	ОПИСАНИЕ
0		Эхо-ответ
	0	Сообщение эхо-ответа
3		Адресат недоступен
	0	Сеть недоступна
	1	Хост недоступен
	2	Протокол недоступен
	3	Порт недоступен

Таблица 50-7 Примечания ICMP

ТИП	КОД	ОПИСАНИЕ
	4	Пакет, нуждавшийся во фрагментации, был сброшен, т. к. для него был установлен режим Don't Fragment (DF)
	5	Некорректный маршрут от источника
4		Обрыв источника
	0	Шлюз может сбрасывать Интернет-датаграммы, если он не располагает необходимой буферной памятью для постановки датаграмм в очередь на вывод в следующую сеть на пути к сети назначения.
5		Перенаправление
	0	Перенаправление датаграмм для сети
	1	Перенаправление датаграмм для хоста
	2	Перенаправление датаграмм для типа услуги и сети
	3	Перенаправление датаграмм для типа услуги и хоста
8		Эхо
	0	Эхо-сообщение
11		Превышение времени
	0	Превышение времени жизни при передаче
	1	Превышение времени включения фрагмента в сборку
12		Проблемы с параметрами
	0	Указатель свидетельствует об ошибке
13		Временная метка
	0	Сообщение запроса временной метки
14		Ответ на запрос временной метки
	0	Сообщение ответа на запрос временной метки
15		Запрос информации
	0	Сообщение запроса информации
16		Ответ на запрос информации
	0	Сообщение ответа на запрос информации

Раздел 51
Алфавитный указатель

П

Р

С

Т